МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

На правах рукописи

Джура Георгий Сергеевич

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Специальность 08.00.05 – Экономика и управление народным хозяйством
(по отраслям сферы деятельности, в т.ч.: менеджмент)

Диссертация
на соискание ученой степени
кандидата экономических наук

Экземпляр диссертации идентичен по содержанию другим экземплярам, которые были представлены в диссертационный совет
Ученый секретарь диссертационного совета Д 01.001.01
канд. гос. упр., доцент
Кретова А.В.

Научный руководитель:
кандидат наук по государственному управлению, доцент
Шумаева Елена Александровна

Донецк – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Использование информационных технологий на современном этапе способствует повышению эффективности всех сфер государственного управления и приводит к развитию всех отраслей. Однако преимущества от внедрения информационных технологий сопровождаются рядом рисков и угроз безопасности, минимизация и предотвращение которых в существующих условиях может быть обеспечена только на общегосударственном уровне, т.к. именно органы публичного управления выступают субъектами, в полномочия которых входит регулирование, контроль и надзор за сложными и разветвленными процессами информационно-технологического пространства.

Важность обеспечения информационной безопасности в настоящее время очевидна не только на уровне государств и бизнеса, но и для отдельно взятого гражданина, с учетом переориентации различных видов его жизнедеятельности на инфокоммуникационные платформы при непрерывном росте угроз безопасности информации во всем мире, необходимость защиты персональных данных и другой конфиденциальной информации в информационном пространстве выходит на новый уровень.

Современные социально-экономические условия обуславливают необходимость проведения глубоких стратегических преобразований в информационной сфере, которые должны быть реализованы за счет как системных реформ (на общегосударственном уровне), так и процессных (внутри органов государственной власти). В этой связи актуализируются задачи поиска и комплексного исследования научно-методических и практических подходов к совершенствованию системы обеспечения информационной безопасности в органах государственной власти.

Степень разработанности темы исследования. Современные исследования проблем совершенствования системы обеспечения

информационной безопасности опираются на многочисленные научные труды как зарубежных ученых таких, как И.И. Лившиц, А.Н. Люльченко, В.В. Сагитова и др., так и отечественных – Т.В. Гончарова, Т.О. Загорная, Р.В. Ободец, Е.А. Шумаева и др. Научные исследования общих теоретических и методологических основ информационной безопасности нашли отражение в работах М.Е. Агафоновой, М.В. Арсентьева, В.Я. Богачева, Т.В. Владимировой, Г.Р. Ганибаева, А.П. Данилова, С.И. Макаренко, А.А. Нежельского, Н.Р. Шевко, А.В. Шободоевой и др. Исследованиям прикладных аспектов совершенствования процессов информационной безопасности посвящены работы В.В. Арутюнова, А.Н. Благовещенского, С.В. Захарова, С.И. Козьминых, А.И. Кураленко, И.В. Машкиной, Н.В. Мамушкиной, В.Н. Шамкина, Д.Р. Хлестовой и др. Проблемам обеспечения информационной безопасности в органах государственной власти посвящены труды Л.Н. Алексеевой, А.А. Мурашкиной, Д.В. Соколова, Л.К. Терещенко и др.

Вместе с тем фрагментарность исследований и отсутствие обобщенного осмысления теоретических и методических основ обеспечения информационной безопасности в органах государственной власти обусловили необходимость исследования и развития концептуальных подходов к ее совершенствованию на современном этапе становления Донецкой Народной Республики, а также определили актуальность темы, цель и задачи диссертации.

Цель и задачи исследования. Целью исследования является развитие научно-методических основ и разработка рекомендаций по совершенствованию системы обеспечения информационной безопасности в органах государственной власти на основе формирования архитектуры единого информационного пространства органов государственной власти, разработки концепции совершенствования данной системы и методического подхода к ее комплексной диагностике.

Достижение поставленной цели обусловило необходимость решения следующих задач:

раскрыть сущность процесса обеспечения информационной безопасности в органах государственной власти;

исследовать теоретико-методические подходы к формированию и развитию систем обеспечения информационной безопасности в органах государственной власти, а также зарубежный опыт функционирования систем с учетом возможности его применения в отечественной практике;

проанализировать тенденции развития системы обеспечения информационной безопасности в Донецкой Народной Республике и провести диагностику системы обеспечения информационной безопасности органа государственной власти с использованием разработанного методического подхода к оценке рисков информационной безопасности;

разработать концепцию совершенствования системы обеспечения информационной безопасности в органах государственной власти;

сформировать архитектуру единого информационного пространства органов государственной власти;

разработать методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти.

Объектом исследования является процесс обеспечения информационной безопасности.

Предмет исследования – совершенствование системы обеспечения информационной безопасности в органах государственной власти.

Диссертация выполнена в соответствии с паспортом специальности 08.00.05 – Экономика и управление народным хозяйством (по отраслям сферы деятельности, в т.ч.: менеджмент), в частности: п. 10.8 «Информационное обеспечение системы публичного управления. «Электронная демократия», «электронное государство», «электронное правительство» и технологии электронного администрирования» и п. 10.11 «Проектирование систем управления организациями. Новые формы функционирования и развития систем управления организациями. Информационные системы в управлении организациями. Качество управления организацией. Методология развития

бизнес-процессов. Развитие методологии и методов управления корпоративной инновационной системой».

Научная новизна полученных результатов. К числу основных результатов, характеризующих научную новизну исследования, относятся следующие:

усовершенствованы:

теоретико-методический подход к совершенствованию системы обеспечения информационной безопасности в органах государственной власти за счет разработки концепции совершенствования системы, которая, в отличие от существующих, базируется на системных процессно-ориентированных принципах управления, повышении эффективности применения комплексного подхода к обеспечению информационной безопасности в органах государственной власти, инструментарии оценки рисков и диагностики, объектной модели регулирования и оптимизации механизмов государственного управления в исследуемой сфере;

организационные подходы к формированию архитектуры единого информационного пространства органов государственной власти за счет создания системы управления информационной безопасностью в органах государственной власти, что, в отличие от существующей структуры управления, позволит стандартизировать, унифицировать и обеспечить единство механизмов развития системы обеспечения информационной безопасности в публичном управлении, а также оптимизировать процессы взаимодействия органов государственной власти в сфере обеспечения информационной безопасности;

методический подход к оценке рисков информационной безопасности в органах государственной власти, который отличается от существующих тем, что реализуется посредством моделирования угроз безопасности информации и оценки уязвимостей информационных активов в органе государственной власти, что дает возможность выделить ключевые риски и приоритизировать последовательность их обработки;

получили дальнейшее развитие:

понятийно-категориальный аппарат исследования сущности процесса обеспечения информационной безопасности, а именно, конкретизировано понятие «информационная безопасность» в органах государственной власти, которое, в отличие от существующих, определяет информационную безопасность как защищенность информационных активов органа от любых случайных или преднамеренных воздействий, результатом которых может явиться нанесение ущерба любым свойствам информации и (или) средствам ее обработки, обеспечивающим удовлетворение информационных потребностей граждан, органов государственной власти и других субъектов информационных отношений за счет внедрения мер, средств и процессов защиты информации, достаточных для нейтрализации существующих угроз безопасности информации в условиях непрерывного совершенствования методов и способов их реализации; под понятием «информационный актив» в органах государственной власти предложено понимать информацию и (или) средство ее обработки, определенные и управляемые как единое целое; с реквизитами, позволяющими их идентифицировать; имеющие ценность для органов государственной власти и находящиеся в их распоряжении; представленные на любом материальном носителе или в его виде в пригодной форме для выполнения присущих им задач; необходимые для реализации социальных, политических, экономических и других функций и полномочий;

модель процессов системы обеспечения информационной безопасности за счет формирования дополнительного набора процессов подсистем и структурно-логических связей между ними, что позволило оптимизировать структуру системы обеспечения информационной безопасности и сформировать современное видение применения комплексного подхода к обеспечению информационной безопасности;

методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти, основанный на использовании международных и российских стандартов и «лучших практик», посредством формирования обобщенной схемы реализации подхода и

декомпозиции ключевого этапа оценки соответствия требованиям стандарта, что дает возможность выбрать и обосновать эталонные значения критериев состояния системы обеспечения информационной безопасности и осуществить объективную оценку ее уровня, а также определить и классифицировать основные процессные составляющие системы, отличающиеся от существующих тем, что имеют более полную структуру и являются адаптированными под специфику органов государственной власти.

Теоретическая и практическая значимость работы. Теоретическое значение полученных результатов определяется достигнутым уровнем разработанности исследуемой проблемы, научной новизной и заключается в совершенствовании системы обеспечения информационной безопасности в органах государственной власти Донецкой Народной Республики.

Практическое значение исследования заключается в доведении разработанных и предложенных теоретико-методических и практических рекомендаций, обоснованных в ходе исследования, до уровня практических разработок по совершенствованию системы обеспечения информационной безопасности в органах государственной власти.

Диссертация выполнена в соответствии с тематикой научно-исследовательской работы кафедры менеджмента и хозяйственного права ГОУ ВПО «Донецкий национальный технический университет» Министерства образования и науки Донецкой Народной Республики в рамках темы Н6-18 «Стратегия интеграционного антикризисного развития социально-экономических систем региона: методология, проблемы, перспективы», где лично автором предложена концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти.

Рекомендации и предложения, изложенные в диссертации, внедрены в практическую деятельность: Министерства связи Донецкой Народной Республики – методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти, который используется при принятии решений по оптимизации существующей системы

обеспечения информационной безопасности (справка от 24.02.2021 № 98); Государственного унитарного предприятия Донецкой Народной Республики «Углетелеком» – методический подход к оценке рисков информационной безопасности в органах государственной власти, который используется в процессе диагностики систем обеспечения информационной безопасности в органах государственной власти (справка от 19.02.2021 № 370/02).

Полученные научные результаты используются в учебном процессе Государственного образовательного учреждения высшего профессионального образования «Донецкий национальный технический университет» при разработке и изложении учебных дисциплин «Информационно-аналитическое обеспечение государственного и муниципального управления», «Электронная коммерция», «Управление изменениями» (справка от 15.02.21 № 39.2/1189-1).

Справки о внедрении результатов исследования размещены в Приложении А.

Методология и методы исследования. Теоретической основой диссертации являются фундаментальные положения экономической науки, теории государственного управления, труды отечественных и зарубежных ученых в сфере обеспечения информационной безопасности.

Для достижения поставленной цели в диссертации использован процессный и системный подходы (при структурировании процессов системы обеспечения информационной безопасности в органах государственной власти); комплекс теоретических и эмпирических методов научного познания, включающий методы: анализа и синтеза, логического анализа (для уточнения понятий «информационная безопасность» и «информационный актив» в органах государственной власти); сравнения и обобщения, абстрагирования (при выделении отдельных процессов в системе обеспечения информационной безопасности в органах государственной власти), сравнений и аналогий (при исследовании зарубежного опыта функционирования систем обеспечения информационной безопасности в органах государственной власти); статистический (для выявления современных тенденций и особенностей развития сферы обеспечения информационной безопасности в органах государственной

власти Донецкой Народной Республики); экспертный (при анализе и оценке показателей, характеризующих общегосударственные подходы к обеспечению информационной безопасности; проведении оценки рисков информационной безопасности и диагностики системы обеспечения информационной безопасности органа государственной власти); сравнительно-правовой метод анализа (при разработке концепции совершенствования системы обеспечения информационной безопасности в органах государственной власти); индукции и дедукции, логического обобщения (для теоретического обобщения и формулирования выводов), а также использованы табличные и графические приемы иллюстрации результатов исследования.

Для обработки экономической информации, построения диаграмм, графиков, схем, рисунков применялись пакеты прикладных программ, в частности Microsoft Excel, Draw.io.

В качестве информационной базы исследования послужили законодательные и нормативные правовые акты и документы Донецкой Народной Республики и Российской Федерации по организационно-техническим и правовым вопросам в сфере обеспечения информационной безопасности, материалы монографических исследований, научно-практических конференций и периодических изданий, результаты авторского исследования.

Положения, выносимые на защиту:

понятийно-категориальный аппарат исследования в части конкретизации понятий «информационная безопасность» и «информационный актив» в органах государственной власти;

модель процессов системы обеспечения информационной безопасности, оптимизирующая ее структуру;

методический подход к оценке рисков информационной безопасности в органах государственной власти;

концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти;

организационные подходы к формированию архитектуры единого информационного пространства органов государственной власти;

методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти.

Степень достоверности результатов исследования. Достоверность полученных результатов подтверждается широким охватом теоретической и эмпирической базы исследования, посвященной вопросам совершенствования системы обеспечения информационной безопасности в органах государственной власти, использованием данных официальной статистики, корректностью применения методов научных исследований с использованием экономико-математического моделирования.

Диссертация является самостоятельной научной работой в области экономики и управления, в которой изложен авторский подход к решению важной задачи научно обоснованного совершенствования системы информационной безопасности в органах государственной власти. Из научных трудов, опубликованных в соавторстве, использованы только те идеи, положения и расчеты, которые являются результатом личных исследований соискателя. Вклад автора в коллективно опубликованные работы конкретизирован в списке трудов, опубликованных по теме диссертации.

Основные положения и результаты исследования докладывались и получили одобрение на научно-практических и научно-технических конференциях различного уровня: «Государственное управление инновациями: проблемы, технологии, перспективы» (г. Донецк, 2016 г.); «Завалишинские чтения’17» (г. Санкт-Петербург, 2017 г.); «Современное государственное и муниципальное управление: проблемы, технологии, перспективы» (г. Донецк, 2017, 2019 гг.); «Программная инженерия: методы и технологии разработки информационно-вычислительных систем (ПИИВС-2018)» (г. Донецк, 2018 г.); «Стратегия устойчивого развития в антикризисном управлении экономическими системами» (г. Донецк, 2019, 2020 гг.); «Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ –

2019"» (г. Севастополь, 2019 г.); «Бизнес-инжиниринг сложных систем: модели, технологии, инновации» (г. Донецк-Екатеринбург, 2019 г.); «Инновационные перспективы Донбасса» (г. Донецк, 2020 г.); «Актуальные проблемы обеспечения национальной безопасности» (г. Донецк, 2020 г.).

Публикации. По теме диссертации опубликовано 19 научных работ, в том числе: 1 коллективная монография, 6 статей в рецензируемых научных изданиях, 1 статья в других изданиях, 11 работ апробационного характера. Общий объем научных работ составляет 20,7 п.л., из них 6,33 п.л. принадлежит лично автору.

Из научных трудов, опубликованных в соавторстве, в диссертации используются только самостоятельно полученные научные результаты и практические рекомендации.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ И МЕТОДИЧЕСКИЕ ОСНОВЫ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

1.1. Сущность процесса обеспечения информационной безопасности в органах государственной власти

Развитие и интеграция отрасли информационных технологий (далее – ИТ) со всеми сферами государственного управления и жизнедеятельности человека в настоящее время свидетельствует о том, что их использование способствует совершенствованию направлений деятельности государства в целом и отдельно взятой организации, в частности, и, в конечном счете, приводит к существенному прогрессу в любой отрасли. Сервисы, предоставляемые информационными системами и ресурсами, способствуют существенному улучшению качества осуществляемых с их помощью процессов.

Возникновение пандемии COVID-19 также придало импульс переходу на инфокоммуникационные платформы не только взаимодействий между людьми, но и практически всех сфер государственного управления и общественных процессов от производственной деятельности до образовательной. Стоит отметить, что переводимые в автоматизированный вид процессы становятся прозрачными, быстрыми, отлаженными, безотказными, четкими и предсказуемыми, что играет существенную роль в совершенствования благосостояния граждан.

Однако, все эти преимущества сопровождаются рядом рисков и угроз, минимизация и предотвращение которых в существующих условиях должна быть обеспечена как на общегосударственном, так и на межгосударственном уровне,

т.к. именно государство выступает единственно эффективным субъектом, в полномочия которого входит регулирование сложных и разветвленных процессов в информационно-технологическом пространстве [1].

Обладание ценными данными предоставляет ощутимые преимущества как в частном секторе, так и в государственном, и при этом возлагает высокую степень ответственности за защищенность этих данных на их владельца. Поэтому обеспечение информационной безопасности (далее – ИБ) в органах государственной власти (далее – ОГВ) на современном этапе является интегрированной частью общей системы управления, необходимой для развития организаций и государств [2].

Важность обеспечения ИБ очевидна не только на уровне государств и бизнеса. Для отдельно взятого гражданина, с учетом переориентации так или иначе всех видов его жизнедеятельности на ИТ-платформы, а также роста рисков и угроз безопасности информации, важность защиты данных в глобальном информационном пространстве выходит на новый уровень.

В рамках концепции А. Маслоу понятие «безопасность» рассматривается в качестве одной из жизненно важных потребностей человека. Ученый расположил безопасность на втором уровне пирамиды потребностей после базовых потребностей в пище и воде. Поэтому с ростом влияния информационной составляющей на безопасность человека, все более важными становятся такие направления обеспечения ИБ, как: защита личных данных, неприкосновенность частной жизни и другие фундаментальные конституционные права [3; 4].

Так, О.Н. Дроботенко отмечает, что в современных условиях все ключевые сферы жизнедеятельности людей оказываются всё более интегрированными в информационное пространство, ввиду чего, влияние, оказываемое на систему безопасности данного пространства, может существенно изменять состояние общегосударственной системы в целом. Поэтому несмотря на то, что информационный компонент на современном этапе выступает ключевым фактором развития, угрозы и риски, сопутствующие развитию данного

компонента, приобретают все большую степень влияния на безопасность личности, общества и государства.

Усложнение и все большая интеграция различных сфер и отраслей с информационными системами обусловливает возникновение новых угроз безопасности. В свою очередь, трудность принятия конкретных мер, которые бы снижали возникающие при этом риски ИБ, связана с неисчерпаемым арсеналом средств и методов враждебного воздействия как на техническую, так и на информационную составляющую [4].

На современном этапе качество процессов ИБ становится важнейшим фактором успешного осуществления политической стратегии государства как на макро-, так и на микро- уровне, обеспечивающим защиту государства от внешних и внутренних угроз, трансформируя привычные критерии оценки роли и соотношения военной мощи и политических возможностей в реализации геополитических интересов, столкновение которых превращает информационное противоборство за лидерство в информационную войну [5].

В таких сложных внутренне- и внешнеполитических условиях сложно переоценить важность процесса обеспечения ИБ для ОГВ как системообразующих субъектов, формирующих систему управления информационным полем государства. Стоит отметить, что актуальность вопросов обеспечения ИБ для ОГВ обусловлена такими ключевыми тенденциями, как:

– высокие темпы роста цифровизации в различных сферах деятельности;

– резкое увеличение вычислительной мощности современных цифровых устройств при одновременном упрощении их эксплуатации;

– резкое увеличение объемов накапливаемых, хранимых и обрабатываемых данных;

– сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

– резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;

– бурное развитие программных и аппаратных средств, не удовлетворяющих минимальным требованиям информационной безопасности;

– повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;

– развитие сети интернет, сопровождающееся ростом поддерживающих и зависимых от ее функционирования систем [227].

Данные тенденции говорят о важности обеспечения ИБ для большинства отраслей и сфер деятельности. Стоит также отметить разветвленность и интегрированность сферы обеспечения ИБ с другими сферами и областями. ИБ влияет на все другие виды национальной безопасности (экологическую, научно-техническую, политическую, оборонную и др.) (рисунок 1.1) [6-8].

Данный факт подтверждается в Стратегии национальной безопасности Российской Федерации (далее – РФ), утвержденной Указом Президента РФ от 2 июля 2021 г. № 400, в которой информационная безопасность отнесена к стратегическим национальным приоритетам [9, ст. 3 п. 4].

В современных условиях для достижения необходимого уровня национальной безопасности необходимо предвидеть все реальные и потенциальные угрозы жизненно важным интересам личности, общества и государства. Особую актуальность на современном этапе приобретает непрерывное получение достоверной и полной информации не только об угрозах и степени их опасности, но и о возможностях воздействия на них с целью устранения, нейтрализации или снижения рисков, возникающих от данных угроз. Такое положение дел может быть достигнуто только в рамках эффективной, технологичной и системной поддержки информационного обеспечения государства и общества [10].

С учетом указанного влияния необходимо отметить, что по мере развития и усложнения средств, методов и форм цифровизации процессов обработки данных повышается зависимость общества от уровня обеспечения безопасности используемых информационных технологий, от которых во многом зависит благополучие, а зачастую, и жизнь многих людей.

Рисунок 1.1 – Влияние информационной безопасности на национальную безопасность [составлено автором на основе [9]]

Явным примером этому является беспрецедентный уровень перемещения в информационную плоскость государственных информационных систем, обеспечивающих функционирование таких отраслей как медицинская, образовательная, финансовая, промышленная и другие. Поэтому интегрированность информационной компоненты в жизнедеятельность государства и общества обуславливает необходимость формирования целостного и непротиворечивого понятийного аппарата, позволяющего четко детализировать процесс обеспечения ИБ в ОГВ [11-14; 228].

При исследовании сущности процесса обеспечения ИБ в ОГВ, важно рассмотреть сущность ключевых понятий, т.к. по мнению Томаса Рейда, ничто так не мешает прогрессу знания, как расплывчатость терминологии [15]. Таблица 1.1 иллюстрирует, что сущность понятия «информационная безопасность» в разных трактовках может быть отличной за счет отраслевых аспектов рассматриваемых вопросов.

Таблица 1.1 – Сущность понятия «информационная безопасность» [составлено автором на основе [16-24]]

Автор/источник	Содержание
Доктрина информационной безопасности Российской Федерации	состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства
ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности	защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность
В.Н. Лопатин	состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз
А. Н. Асаул	защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры
А. Д. Урсул	состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям
М. В. Арсентьев	снятие информационной неопределенности относительно объективно и субъективно существующих потенциальных и реальных угроз за счет контроля над мировым пространством и наличия возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта
Т. В. Владимирова	обеспечение безопасности социальных практик информационной среды в условиях роста интенсивности информационных потоков и устаревания информации
Р. М. Юсупов	состояние, в котором ему (субъекту) не может быть нанесен существенный ущерб путем воздействия на его информационную сферу
В. Ф. Пилипенко	состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфер

Так, А.В. Шободоева отмечает, что терминологическая база, связанная с вопросами ИБ, включает достаточно много разрозненных актов, обладающих противоречивым и несовершенным понятийным аппаратом. По этой причине при формировании терминологического базиса понятия «информационная безопасность» необходимо начинать с отраслевой фокусировки [25].

В свою очередь, Л.А. Сергиенко отмечает, что понятие «информационная безопасность» приобрело государственную трактовку в 1989 г., когда по решению Президиума Верховного Совета СССР была создана рабочая комиссия по совершенствованию системы национальной безопасности, возглавляемая профессором В.Н. Лопатиным, который предлагал выделить 3 подгруппы защиты информационных активов: 1 – защита информации и прав на нее (включая право на доступ, на тайну, на объекты интеллектуальной собственности); 2 – защита человека и общества от воздействия «вредной» информации; 3 – защита информационных систем и прав на них (в том числе прав и интересов государства по сохранению единого информационного пространства) [26].

Однако, как отмечают А.П. Данилов и А.А. Данилов данная трактовка главным образом относилась к защите компьютерных данных (информационных систем, сетей и др.) и в дальнейшем расширялась как с учетом специфики отраслей, так и с учетом охвата все больших аспектов, связанных с обеспечением ИБ [27]. В свою очередь, Г.Р. Ганибаев отмечает, что трактовка ИБ как состояния защищенности основана на статическом подходе, наряду с которым в научной литературе используется динамический (к примеру, в трактовке М.В. Арсентьева или Т.В. Владимировой) (рисунок 1.2) [28, с. 194].

В соответствии с динамическим подходом к трактовке ИБ предполагается признание в качестве свойств современного общества следующих характеристик: возможности доступа к информации; наличия собственного высокого информационного потенциала (ресурсов); независимости в использовании собственного информационного потенциала; средств защиты этой части потенциала (технических, организационных, правовых и др.); определения защищаемой части собственного информационного потенциала за счет

соотнесения с информационным потенциалом других субъектов; создания возможностей и условий для обогащения своего собственного информационного потенциала за счет потенциала других субъектов, в том числе, и находящегося под защитой, что определяется существующей конкуренцией, соперничеством и противоборством [35, с. 15].

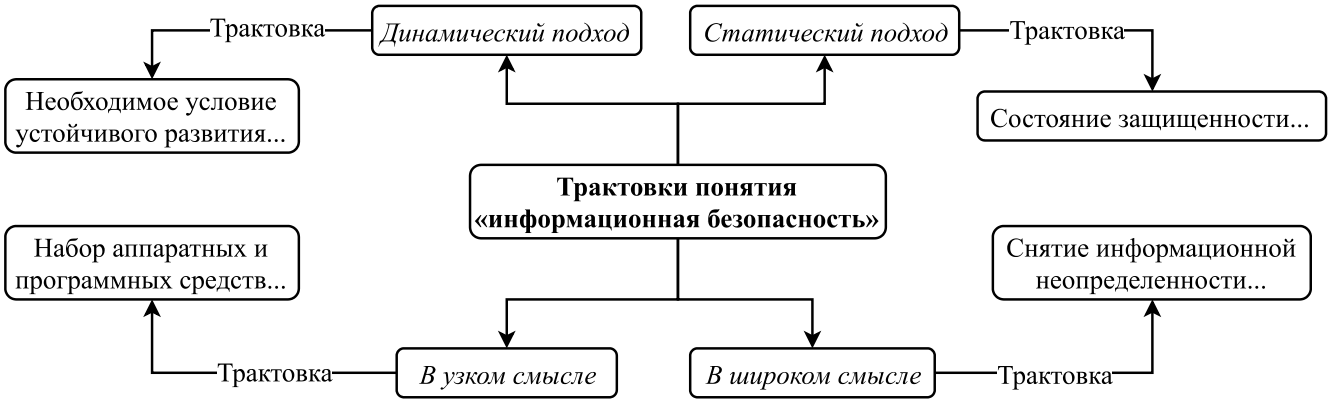

Рисунок 1.2 – Трактовки информационной безопасности [составлено автором на основе [25-28; 35]]

В динамической трактовке информационная безопасность определяется как необходимое условие устойчивого развития системы при растущей неопределенности внешней среды, вызванной повышением уровня вариативности, интенсивности и частоты коммуникационных взаимодействий, отражающихся в изменении характеристик информационных потоков и предполагает наличие в различных системах механизмов контроля за информационными потоками, а также инструментов предупреждения (предотвращения, нейтрализации) угроз [28].

А.В. Шободоева, в свою очередь, разделяет подходы к трактовке термина «информационная безопасность» в «узком» и в «широком» смысле. Данный подход можно интерпретировать следующим образом: в «узком» смысле (для организации) «информационная безопасность» – это набор программных и аппаратных средств обеспечения свойств информации в автоматизированных информационных системах, «широкий» же подход (для государства) был

использован в Доктрине информационной безопасности РФ и используется в общенациональном масштабе [16].

В «широком» смысле в информационной сфере формируются стратегические и тактические задачи внутренней и внешней государственной политики по обеспечению ИБ, т.е. здесь ИБ – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства. Также А.В. Шободоева отмечает, что, основная формула как нормативных, так и научных трактовок ИБ – это состояние защищенности и объясняет это тем, что такой подход свойственен российской научной мысли к пониманию категории «безопасность» [25].

Интересен и подход Н.Р. Шевко, мысль которой можно интерпретировать как понимание под исследуемым термином защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений [29].

Таким образом, можно сделать вывод, что для ОГВ, с учетом их специфики, наиболее актуальной является динамическая трактовка в широком смысле, формирующая циклично развивающуюся систему, охватывающая все, участвующие в процессе обеспечения ИБ объекты и субъекты, а также предполагающая определенный баланс интересов личности, общества и государства.

Стоит отметить, что при формировании терминологического базиса, устанавливающего рамки в процессах обеспечения безопасности информационных активов ОГВ, важно понимать разницу между нижеприведенными терминами, которые зачастую смешиваются (таблица 1.2). Из определения понятий «защита информации» и «безопасность информации» прослеживается взаимоствязь между ними: «защита информации» направлена на обеспечение «информационной безопасности», или, иными словами, «безопасность информации» обеспечивается с помощью ее защиты. Понятие «информационная безопасность» в научной литературе сначала отождествлялось

с понятием «безопасность информации», затем к нему прибавилась защищенность субъектов информационных отношений от негативных информационных воздействий [33].

Таблица 1.2 – Основные определения, относящиеся к термину «информационная безопасность» [составлено автором на основе [30-32]]

Термин	Определение
Информационная безопасность	сохранение конфиденциальности, целостности, доступности, подлинности, подотчетности, недоказуемости, достоверности и других свойств информации
Безопасность информации	состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, целостность и доступность
Защита информации	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Кибербезопасность	сохранение свойств информации в киберпространстве (сложной среде, не существующей ни в какой физической форме, возникающей в результате взаимодействия людей, программного обеспечения и интернет-сервисов посредством технологий, устройств и сетей)

Основным различием между «информационной безопасностью» и «безопасностью информации» является то, что первое понятие отражает процесс, а второе – состояние. Как отмечает Г.Р. Ганибаев, содержание понятия «информационная безопасность» шире понятия «безопасность информации», т.к. наряду с информационным процессом включает широкий спектр объектов, субъектов и механизмов взаимодействия между ними, а также условий, в которых данные взаимодействия осуществляются эффективно [28].

Также интересен подход А.С. Алпеева, который определяет целесообразность использования термина «информационная защищенность» вместо «информационная безопасность», понимая под данным термином защиту свойств информации [34]. М.М. Безкоровайный и А.Л. Татузов, в свою очередь, отмечают, что «кибербезопасность» не может быть направлена на защиту от максимального числа информационных угроз, однако, должна обеспечить максимально благоприятную среду для работы пользователей и всех систем в киберпространстве [35].

Понятие «информационная безопасность» при этом отличается от понятия «кибербезопасность» тем, что первая предназначена для комплексной безопасности информационных активов в любой форме, а «кибербезопасность» обеспечивает исключительно защиту цифровых данных. Так, понятие «кибербезопасность» характеризует защиту сетей, компьютеров и данных от несанкционированного электронного доступа. В свою очередь, «информационная безопасность» связана с защитой информационных активов, независимо от формы их представления.

Переходя к неотъемлемым свойствам информационной безопасности и, в той или иной степени, важной для любого ОГВ, целесообразно конкретизировать и охватить ключевые ракурсы данных понятий (таблица 1.3).

Таблица 1.3 – Ключевые свойства информационной безопасности [составлено автором на основе [30; 36-39]]

Свойство	Содержание
Конфиденциальность	недоступность или закрытость для неавторизованных лиц, сущностей или процессов
Целостность	сохранность правильности и полноты активов (неизменности корректности и аутентичности)
Доступность	готовность к использованию по запросу авторизованных субъектов
Неотказуемость	способность удостоверять имевшее место событие или действие и их субъекты так, чтобы это событие или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение
Подлинность	идентичность информации заявленному содержанию
Достоверность	соответствие информации предусмотренному поведению субъектов и объектов и результатам их деятельности
Подотчетность	ответственность субъектов и объектов за их действия и решения

Стоит отметить, что ключевыми свойствами ИБ для ОГВ остаются конфиденциальность, целостность и доступность информации. Однако, с учетом изменения спектра информационных реалий становятся все более важными такие свойства, как, неотказуемость, подлинность, достоверность и подотчетность.

Государственные информационные системы создаются прежде всего для предоставления определенных информационных услуг. Если получение информации по каким-либо причинам становится невозможным, это приносит ущерб всем субъектам информационных отношений. Из этого можно определить,

что доступность информации стоит на первом месте, что зачастую ущемляет возможности в обеспечении конфиденциальности и целостности. Необходимо также отметить важность подлинности и подотчетности для ОГВ ввиду того, что для принятия управленческих решений зачастую определяющим фактором является качественно и вовремя поданная информация.

В результате исследования термина «информационная безопасность», можно сделать заключение, что все проанализированные трактовки представляются автору неполными с точки зрения специфики функционирования ОГВ. Несмотря на то, что информационная безопасность сопряжена с информацией, методологической основой определения данного понятия для ОГВ должно быть отнесение его не к самой информации, а к субъектам информационной среды – физическим и юридическим лицам, участвующим в информационном процессе.

Из данной гипотезы следует, что в практическом отношении ИБ не существует безотносительно к субъекту информационной среды – именно субъект определяет динамично меняющиеся показатели ее обеспечения. Это относится не только к конкретным субъектам, но и к личности, обществу и государству в целом.

Таким образом, в современных условиях наиболее полным и комплексным, по мнению автора, является трактовка понятия «информационная безопасность» в органах государственной власти как защищенность информационных активов органа от любых случайных или преднамеренных воздействий, результатом которых может явиться нанесение ущерба любым свойствам информации и (или) средствам ее обработки, обеспечивающим удовлетворение информационных потребностей граждан, органов государственной власти и других субъектов информационных отношений за счет внедрения мер, средств и процессов защиты информации, достаточных для нейтрализации существующих угроз безопасности информации в условиях непрерывного совершенствования методов и способов их реализации.

Эффективный процесс обеспечения ИБ представляет собой непрерывное и взаимосвязанное применение правовых, организационных и технических мер, направленных на защиту информационных активов (рисунок 1.3) [40].

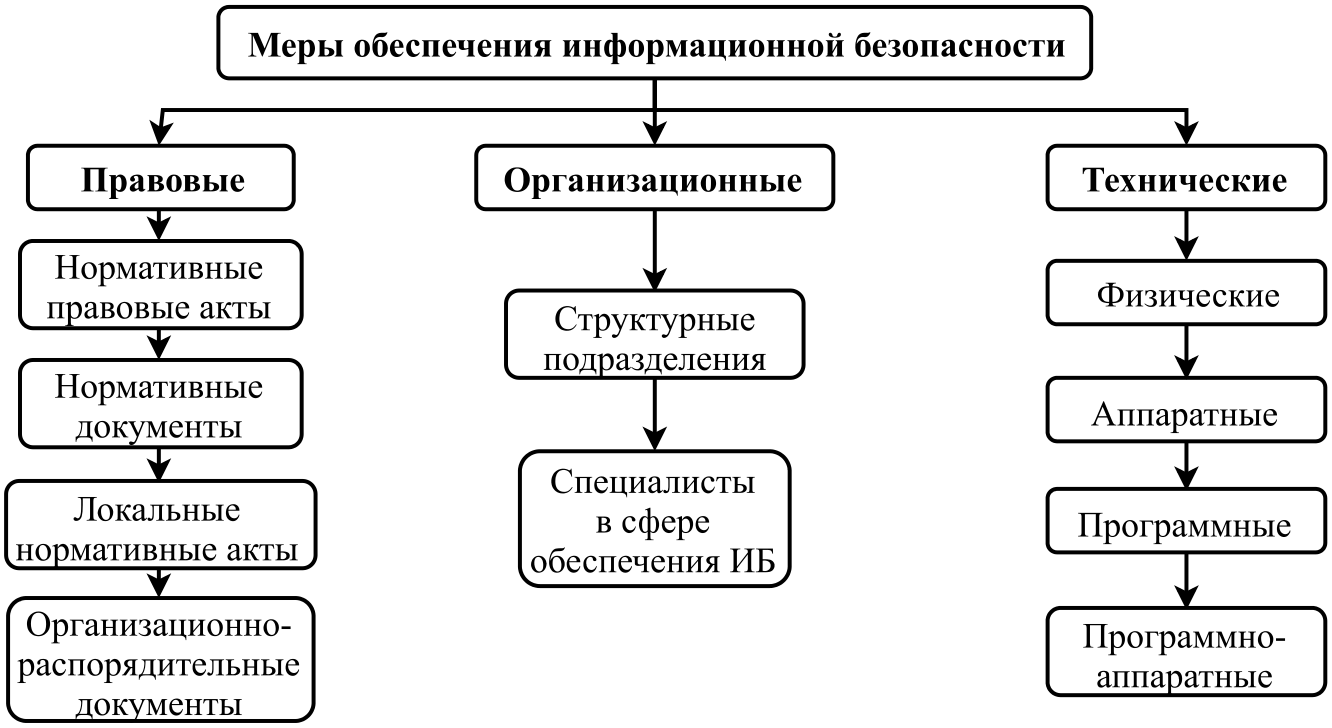

Рисунок 1.3 – Меры обеспечения информационной безопасности [226, с. 40]

В процессе обеспечения ИБ сотрудники ответственных подразделений реализуют меры обеспечения ИБ, направленные на: разработку организационно-распорядительных документов и локальных нормативных актов, создание и эксплуатацию систем защиты информации, в которых осуществляется обработка информации и реализацию других способов обеспечения ИБ. По каждому из существующих направлений обеспечения ИБ для ОГВ государством предъявляются соответствующие требования, эффективная реализация которых способствует нейтрализации и (или) минимизации угроз безопасности информации, защищаемой в ОГВ.

Правовые меры обеспечения ИБ в ОГВ на государственном уровне, включающие нормативные правовые акты и документы (далее – НПА), а на уровне ОГВ – организационно-распорядительные документы и локальные

нормативные акты по вопросам обеспечения ИБ, основываются на нормах морали и этики, принятых в обществе, являются основой обеспечения ИБ и помогают инициировать совершенствование подходов к ее обеспечению, задавая порядки и требования, а также взыскания за несоблюдение данных требований.

Профессионально сформированная нормативная правовая база способствует упорядочиванию функциональной деятельности ОГВ, прозрачности, детерминированности и лучшему контролю. В свою очередь, неполная и противоречивая внутренняя нормативная база приводит к неопределенностям в исполнении функций и полномочий ОГВ, а также к необходимости опираться исключительно на доверие персоналу, ответственному за ИБ, что увеличивает риски ИБ [41; 42].

Организационные меры, в свою очередь, обеспечивают исполнение нормативных актов разного уровня с учетом правил поведения, принятых в ОГВ, и требуют разработки внутренних нормативных документов, не противоречащих правовым нормам. Организационные меры обеспечения ИБ позволяют ответственным структурным подразделениям создать регламенты работы пользователей с информацией, подобрать кадры, организовать работу с документацией и другие процессы [43].

Правила работы пользователей с информационными активами устанавливаются руководством ОГВ на основании требований и рекомендаций нормативных актов уполномоченных регуляторов совместно с ответственными подразделениями с целью создания условий доступа к информационным активам для каждого санкционированного пользователя. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на технических этапах работ [44].

Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз [229, с. 120]. Как отмечают Л.А. Домбровская и Т.Л. Васютина, организационным

мерам защиты отводится особое место при формировании комплексного подхода к обеспечению ИБ, т.к. они позволяют обеспечить:

– организацию охраны, режима, работу с кадрами, с документами, другими носителями;

– использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности;

– комплексное планирование мероприятий по обеспечению ИБ [40].

Таким образом, к основным организационным мероприятиям обеспечения ИБ в ОГВ можно отнести организацию:

– режима и охраны (с целью исключения возможности тайного проникновения на территорию ОГВ и в помещения посторонних лиц);

– работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их обучение правилам работы с информацией ограниченного доступа, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей информации ограниченного доступа, их учёт, исполнение, возврат, хранение и уничтожение;

– использования технических средств сбора, обработки, накопления и хранения общедоступной информации и информации ограниченного доступа;

– работы по анализу внутренних и внешних угроз безопасности информации и выработке мер по обеспечению ее защиты;

– работы по проведению систематического контроля за работой персонала с информацией ограниченного доступа, порядком учёта, хранения и уничтожения документов и технических носителей [251].

Переходя к техническим мерам обеспечения ИБ, стоит отметить, что их условно разделяют на:

– физические – создание преград вокруг информационных активов: охранные системы, укрепление архитектурных конструкций и др.;

– аппаратные – специальные технические средства защиты серверов и корпоративных сетей, системы контроля доступа и др.;

– программные – установка программной оболочки систем защиты, внедрение логических правил разграничения доступа и др.;

– программно-аппаратные – использование аппаратных и программных средств совместно.

Меры обеспечения ИБ представляют собой совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации. В свою очередь, с помощью средств обеспечения ИБ осуществляются меры по защите информационных активов. Как отмечают О.И. Белозеров и И.И. Топоркова, к техническим средствам обеспечения ИБ относятся: средства авторизации и управления доступом, журналирование, системы мониторинга, антивирусные, криптографические средства, электронная подпись и др. В свою очередь, средства обеспечения ИБ, можно условно разделить на нормативно-правовые, административные и морально-этические, инженерно-технические и средства защиты от программно-аппаратных воздействий (рисунок 1.4) [44; 47; 48, с. 13].

С целью формирования комплексного охвата всех аспектов обеспечения ИБ важно конкретизировать объекты, затрагиваемые данным процессом. Как отмечает И.В. Пискунов, классификация информационных активов является крайне важным процессом как для обеспечения ИБ, так и для построения управляемой инфраструктуры организации, т. к. позволяет получить и отслеживать ключевые показатели для используемой информации – ценность, степень влияния на производственные процессы, выполнение требований законодательства и др. От качества выполненной классификации информационных активов, согласно требованиям и рекомендациям многих передовых практик, во многом зависит уровень общей защищенности организации [50-54].

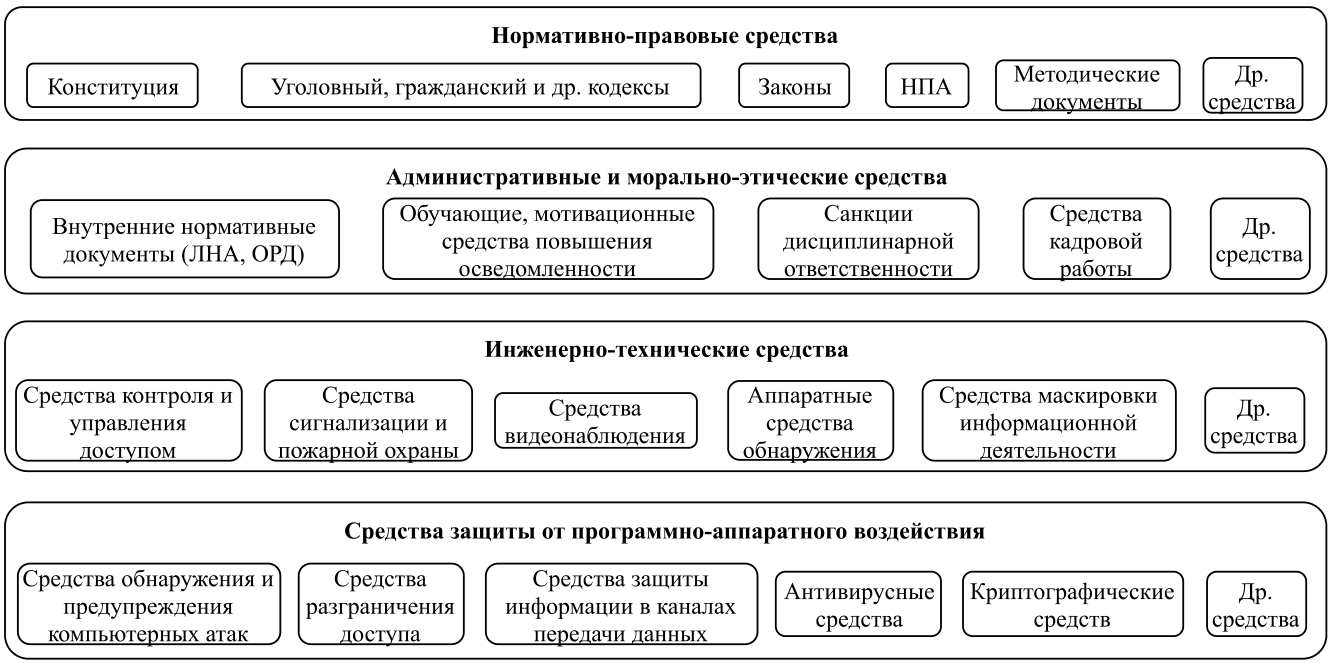

Рисунок 1.4 – Средства обеспечения ИБ [составлено автором на основе [49; 50]]

Под «информационным активом» согласно ГОСТ Р ИСО/МЭК 27000-2012 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология», понимаются знания или данные, которые имеют значение для организации [30]. В свою очередь, РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» определяет «информационный актив» как информацию с реквизитами, позволяющими ее идентифицировать; имеющую ценность для организации банковской системы РФ; находящуюся в распоряжении организации банковской системы РФ и представленную на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме [55].

По мнению автора, существующие определения не позволяют полноценно описать сущность исследуемого понятия в контексте его применения к ОГВ. Поэтому с учетом проведенного анализа, предлагается под понятием «информационный актив» в органах государственной власти понимать

информацию и (или) средство ее обработки, определенные и управляемые как единое целое; с реквизитами, позволяющими их идентифицировать; имеющие ценность для органов государственной власти и находящиеся в их распоряжении; представленные на любом материальном носителе или в его виде в пригодной форме для выполнения присущих им задач; необходимые для реализации социальных, политических, экономических и других функций и полномочий.

Согласно приведенной трактовке, информационными активами для ОГВ являются бумажные и цифровые носители с ценной информацией и данными, информационные системы, базы данных, персональные компьютеры, периферийные устройства, телекоммуникационные сети и др. Помимо категорий, приведенных выше, первичными (нематериальными) информационными активами могут выступать также знания и психика людей, т.к. именно информационное воздействие на человека в настоящее время приобретает масштабы оружия массового поражения, [60, с. 13]. Однако, данный вид активов находится за рамками настоящего исследования.

Под классификацией информационных активов понимают разделение существующих активов организации по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ. Поэтому можно констатировать, что классификация информационных активов формирует базу для определения приоритетности и экономической целесообразности проведения мероприятий по обеспечению их безопасности.

Информационные активы можно классифицировать по типу информации, по способу формирования и распространения информации, по режиму доступа, по виду носителя, по методам организации, хранения, использования и по другим параметрам (рисунок 1.5). Особое внимание для ОГВ важно уделять формированию и использованию информационных активов в части, касающейся обеспечения полноты и своевременности их формирования и актуализации. Поэтому одной из ключевых целей ОГВ является максимально полное и открытое предоставление информации гражданам в порядке реализации их конституционного права на поиск и получение информации.

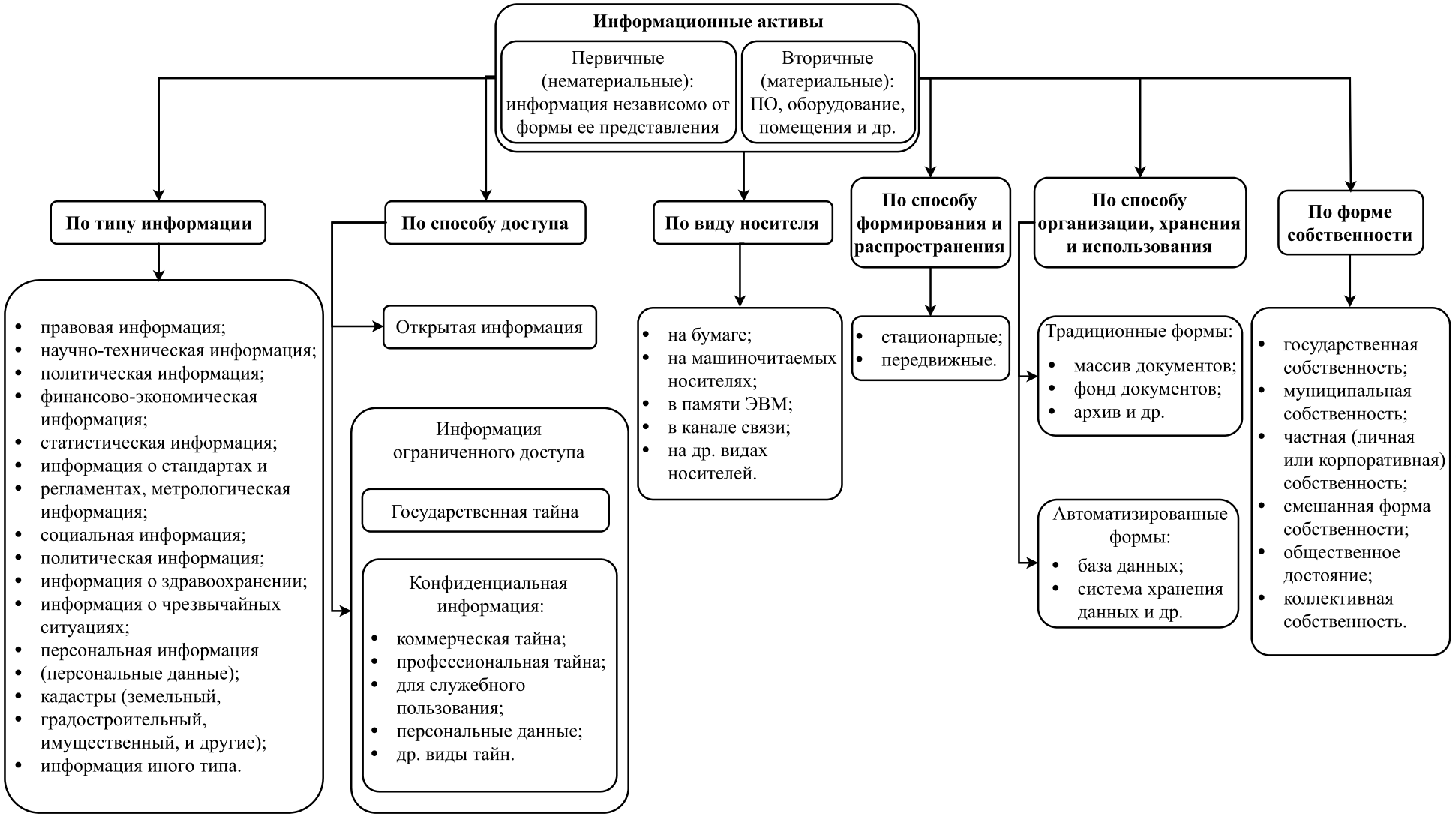

Рисунок 1.5 – Классификация информационных активов ОГВ [составлено автором на основе [57-59]]

Защитить все информационные активы сложно, поэтому из них выделяют ключевые – те, которым целесообразно и необходимо отдавать приоритет при формировании и развитии мер, средств и процессов обеспечения ИБ.

Следуя логике А.Н. Буренина, в качестве информационных активов ОГВ, подлежащих приоритетной защите, можно определить важные средства и данные для обеспечения эффективного информационного обмена в конкретной ведомственной информационной системе [56]. Поэтому в ОГВ должны защищаться информационные активы, содержащие информацию ограниченного доступа, бумажные и цифровые носители, а также информационные системы, сети передачи данных и др. К ключевым категориям информационных активов в ОГВ можно отнести:

– общедоступную информацию (информация, доступ к которой не ограничен);

– информацию ограниченного доступа (государственная, служебная тайна, персональные данные и др.);

– информационные системы, предназначенные для хранения, поиска и обработки информации, и обеспечивающие их функционирование организационные ресурсы (человеческие, технические, финансовые и др.);

– информационную инфраструктуру (центры обработки данных, каналы связи, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации).

Субъектами ИБ в ОГВ являются другие ОГВ, физические и юридические лица (граждане, организации, субъекты других государств и др.). Различают способствующие, противодействующие, а также внешние и внутренние субъекты ИБ. К внешним субъектам, способствующим обеспечению ИБ, относят: ОГВ разного уровня, банки и иные хозяйствующие субъекты, граждан и др. К внешним субъектам, противодействующим обеспечению ИБ, относят теневые экономические структуры, зарубежные спецслужбы, хакерские группировки и др.

К внутренним субъектам, способствующим обеспечению ИБ, относятся сотрудники и структурные подразделения, непосредственно участвующие в

процессах по обеспечению ИБ (служба безопасности, ИТ-отдел, юридическая, кадровая и другие службы). Сотрудники и структурные подразделения, преследующие обратные цели, относятся к внутренним противодействующим обеспечению ИБ субъектам.

Стоит отметить, что в настоящее время в ОГВ выделяется, в лучшем случае, одно подразделение ответственное за обеспечение ИБ, полностью снимая ответственность с других. Однако, данный подход сложно назвать оптимальным. С учетом реалий функционирования ОГВ дифференциация должностных обязанностей сотрудников сложно осуществима. В определенных случаях сотрудникам ОГВ целесообразно совмещать несколько ролей. Однако, по мнению автора, перекладывание всей ответственности на одного сотрудника, либо подразделение не является оптимальным способом распределения обязанностей. Поэтому ответственность за обеспечение ИБ в ОГВ должна лежать и на пользователях, и на руководстве, и на ответственных подразделениях, четко разделяться и регламентироваться, т.к. на современном этапе организация может эффективно обеспечить весь цикл необходимых работ только сообща.

Как отмечает Е.И. Жук, к поддерживающей инфраструктуре, входящей в понятие «информационная безопасность», могут относиться как персональные компьютеры и серверные, так и помещения, системы электро-, тепло-, водоснабжения, средства коммуникаций и т.п. элементы, а также обслуживающий ее персонал [60]. Стоит отметить, что внутренняя инфраструктура тесно интегрирована во всеобщую государственную и мировую инфраструктуру. При этом с учетом данной интегрированности во многих случаях функционирование внутренней инфраструктуры невозможно без внешней.

В настоящее время удаленные от инфраструктуры ОГВ центры обработки данных являются все более распространенным явлением в деятельности ОГВ, т.к. позволяют оптимизировать распределение кадровых и финансовых ресурсов. Данная всеобъемлющая тенденция к всеобщей интегрированности информационных инфраструктур и хранящихся в ней данных в ОГВ требует систематизированных, скоординированных, четко выстроенных взаимосвязей,

состоящих из правовых, организационных и технических мер, реализуемых ответственными государственными структурами, регулирующими отрасль, осуществляющими контрольно-надзорные функции и координирующими ОГВ в вопросах обеспечения ИБ.

Переходя к описанию сущности процесса обеспечения ИБ в ОГВ, важно систематизировать ключевые каналы угроз для активов информационной среды ОГВ, к которым можно отнести: прямой физический доступ к защищаемым объектам, перехват информации через открытые каналы связи, несанкционированный доступ через защищенные каналы связи, перехват информации на стороне получателя – субъекта информационного взаимодействия и др. (рисунок 1.6).

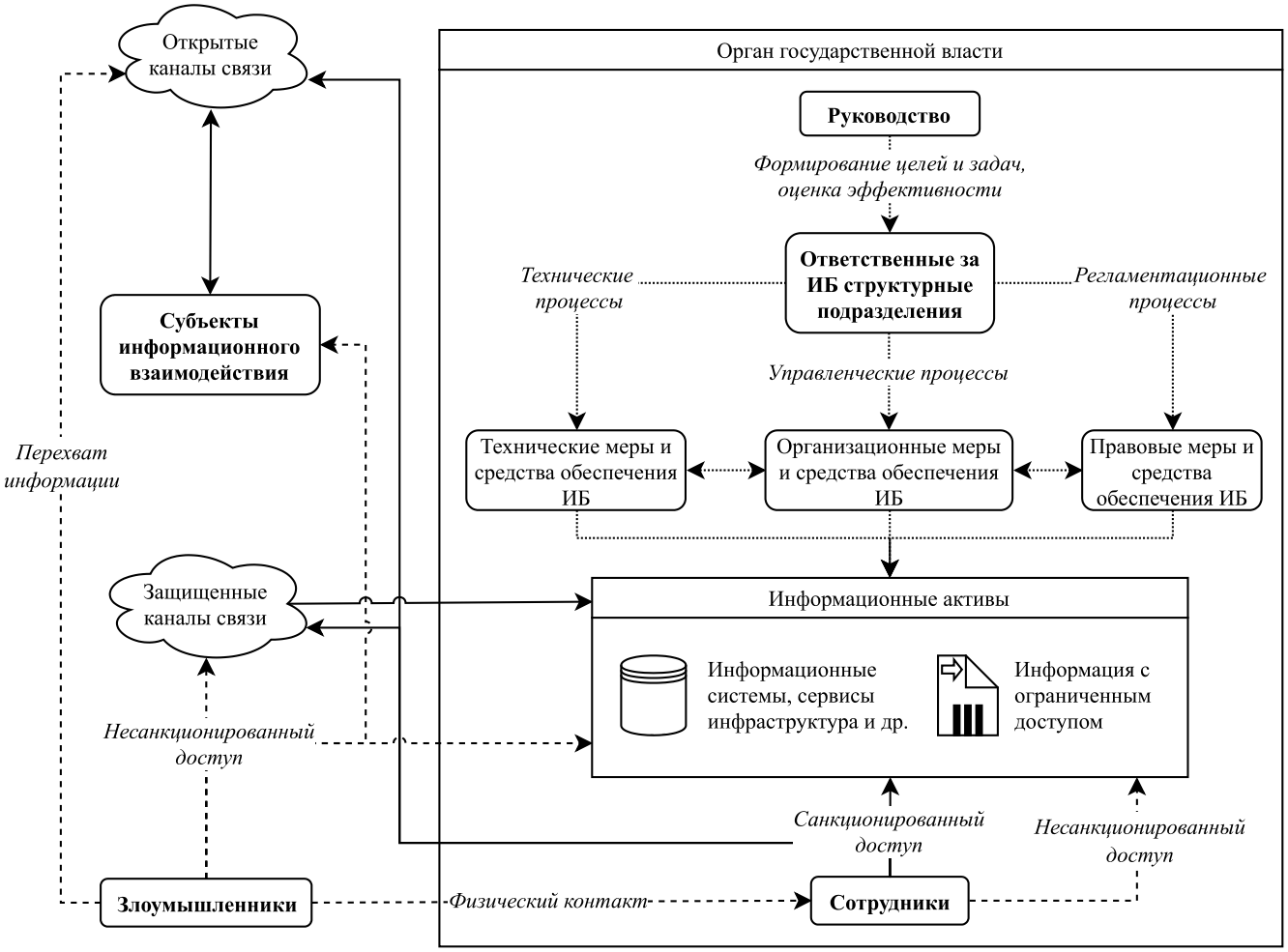

Рисунок 1.6 – Обобщенная структура информационной среды ОГВ в контексте обеспечения информационной безопасности [составлено автором]

С учетом разрозненности каналов угроз безопасности для информационных активов ОГВ возможность минимизации рисков ИБ может быть основана главным образом на всесторонней заинтересованности всех субъектов, участвующих в обеспечении циркуляции потоков данных и поддержке процессов, связанных с информационными средами органов.

Таким образом, для формирования релевантного подхода к поддержке процесса обеспечения ИБ в ОГВ в современных условиях крайне важно, чтобы в ее обеспечение были вовлечены не только передающий и получающий информацию субъект, но и третья сторона, осуществляющая как контрольно-надзорную деятельность, так и оценку эффективности мер, средств и процессов обеспечения ИБ [62]. Таким «третейским судьёй» на современном этапе выступают уполномоченные регуляторы, разрабатывающие нормативные и методические документы с требованиями по ИБ, осуществляющие контрольно-надзорную деятельность и координацию ОГВ в сфере обеспечения ИБ.

Поэтому с учетом разнородности процессов и информационных сред ОГВ, упорядочивание, унификация и централизация информационных активов с постоянным контролем изменений, мониторингом, анализом и оценкой ключевых аспектов обеспечения ИБ возможны только с учетом системного подхода, без которого на современном этапе сложно представить управление ИБ на государственном уровне.

1.2. Подходы к формированию и развитию систем обеспечения информационной безопасности в публичном управлении

Система публичного управления является объединением различных форм социально-политического и экономического взаимодействия между

официальными структурами государственного управления, представителями частного бизнеса и гражданским обществом. Важно учитывать, что современная система публичного управления неотъемлемо связана с информационным обеспечением и должна непрерывно и поступательно двигаться в сторону автоматизации, а затем информатизации и, в конечном счете, цифровизации циркулирующих в ней процессов, в соответствии с ростом уровня зрелости общегосударственных подходов.

Данная тенденция поступательного совершенствования процессов информационного общества в общем виде отражает концептуальный подход к развитию системы информационного обеспечения органов публичного управления, позволяя повышать эффективность и оптимизировать процессы государственного управления. Здесь необходимо отметить важность работ отечественных ученых, затрагивающих вопросы информационного обеспечения органов публичного управления на современном этапе [41; 45; 66; 67].

Ключевым элементом информационного обеспечения органов публичного управления современного государства является электронное правительство, представляющее собой, систему организационных, правовых и технических мер и средств, направленных на обеспечение деятельности по оказанию государственных услуг путем применения информационных технологий, а также межведомственного электронного взаимодействия.

Электронное правительство позволяет оптимизировать все области публичного управления, играя фундаментальную роль в развитии государства и общества, обеспечивая всестороннюю оптимизацию процессов между государством, бизнесом и гражданами, повышая прозрачность и эффективность межведомственного взаимодействия и контрольно-надзорных функций, а в перспективе оптимизируя затраты человеческих, финансовых и иных ресурсов.

Структурные элементы публичного управления, а также цели и задачи, формируемые в рамках влияния на них элементов электронного правительства, представлены на рисунке 1.7.

Рисунок 1.7 – Связь структурных элементов публичного управления и электронного правительства [составлено автором на основе [231; 246]]

В рамках дальнейшего исследования важно сформировать обобщенную инфраструктуру электронного правительства (рисунок 1.8). Каждый компонент инфраструктуры электронного правительства является крайне важным для формирования эффективной системы информационного обеспечения государства на современном этапе. При этом, для органов публичного управления с учетом переориентации всех их ключевых функций и процессов на цифровые платформы в рамках формирования и развития информационных систем и ИТ-инфраструктур, обеспечивающих электронное правительство, существенно возрастают угрозы безопасности информации и связанные с ними риски.

Рисунок 1.8 – Инфраструктура электронного правительства [составлено автором на основе [231]]

В таких условиях, с учетом чувствительности данных, циркулирующих в государственных информационных системах (далее – ИС), особое значение приобретает обеспечение ИБ, что обуславливает целесообразность анализа аспектов формирования и развития системного подхода к ее обеспечению.

Системному подходу к обеспечению ИБ в последнее время уделяется все больше внимания. Высший менеджмент предприятий различных сфер деятельности готов тратить все больше ресурсов на обеспечение ИБ [63]. Как отмечает Д.Г. Кверевкина, системный подход – это совокупность принципов и методов исследования объектов как систем, ориентированный на раскрытие основных системных свойств объектов, выявление всех типов связей и сведение их в единую картину [48, с. 118].

Системный подход учитывает все показатели, влияющие на эффективность конечного результата, и предусматривает широту охвата проблемы в условиях рисков, неопределенности, а также появления новых знаний и технологий. Как отмечают С.В. Белов и Т.М. Исламов, системный подход дает возможность решать задачи, связанные не только с формированием совокупности актуальных

угроз, уязвимостей и путей реализации угрозы, но и с формированием совокупности задач, решение которых обеспечивает требуемый уровень ИБ [64, с. 95]. Система обеспечения информационной безопасности (далее – СОИБ) включает в себя совокупность сил, средств, методов и процессов защиты информационных активов организации.

Как отмечает А.И. Кураленко, развитие теории системности привело к тому, что все мероприятия, затрагивающие обеспечение ИБ, рационально объединять в СОИБ. Такая система обычно включает как техническую инфраструктуру и информационные системы с данными и документацией, так и использующий их персонал, а также все процессы обеспечения ИБ, происходящие в информационном поле организации [65].

Как было отмечено, от уровня обеспечения ИБ прямо зависит качество информационного обеспечения ОГВ, от которого, в свою очередь, зависит экономическое развитие органа. Исходя из этого, можно констатировать что, СОИБ является одним из фундаментальных направлений формирования механизмов устойчивого развития ОГВ [46; 66]. Данное положение подтверждено в Доктрине информационной безопасности РФ 2016 г., где определено, что СОИБ является частью системы обеспечения национальной безопасности РФ, и составляет совокупность сил обеспечения ИБ, осуществляющих скоординированную и спланированную деятельность используемых ими средств [16].

На современном этапе безопасность информационных активов ОГВ может быть обеспечена лишь при комплексном использовании всего спектра имеющихся мер и средств обеспечения ИБ в ключевых структурных элементах производственной системы органа и на всех этапах технологического цикла обработки информации. Наибольший эффект при обеспечении ИБ достигается тогда, когда все используемые средства, методы и меры объединяются в единый целостный механизм, функционирующий, контролируемый, обновляемый и дополняемый в зависимости от изменения внешних и внутренних условий [103; 104].

Отметим, что целью СОИБ в ОГВ является создание и постоянное соблюдение условий, при которых риски органа, связанные с нарушением безопасности его информационных активов, постоянно контролируются и исключаются либо находятся на допустимом (приемлемом) остаточном уровне. Важными задачами обеспечения ИБ в ОГВ можно назвать снижение экономических и технологических рисков органа, связанных с использованием информационных активов, а также создание условий для максимальной автоматизации выполнения операций, относящихся к обработке данных, и исключения ручных операций [252].

Переходя к структуре СОИБ в ОГВ, стоит отметить, что она включает в себя систему информационной безопасности (далее – СИБ) и систему менеджмента информационной безопасности (далее – СМИБ), состоит из совокупности управленческих и исполнительских процессов и включает в себя: комплекс организационных мер правового и административного характера, технических (программных, аппаратных и др.) средств защиты информации и специализированного персонала, реализующего функции по обеспечению ИБ (рисунок 1.9).

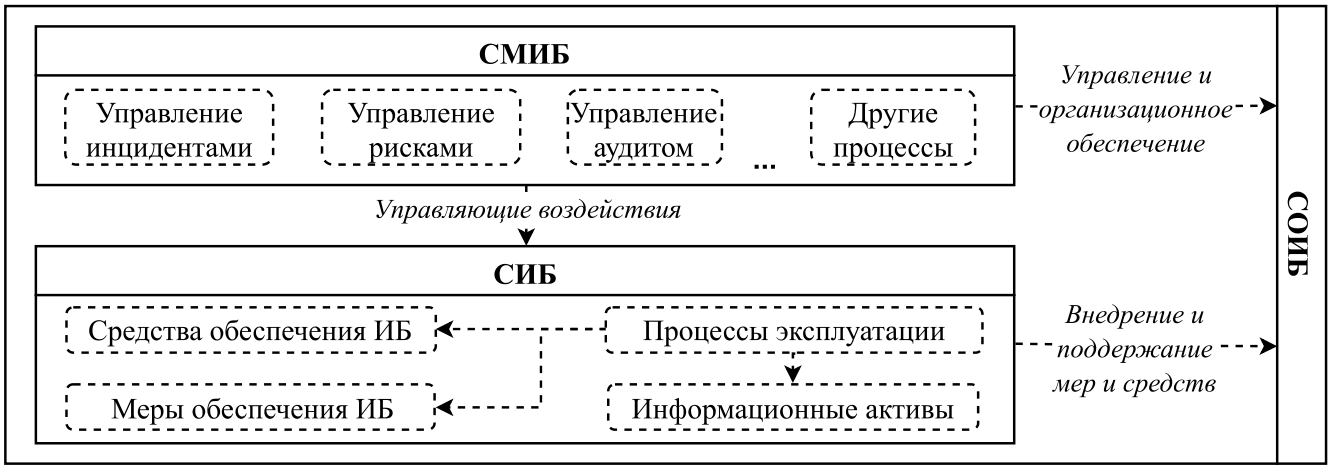

Рисунок 1.9 – Соотношение рассмотренных понятий [составлено автором]

СИБ обеспечивает поддержку СОИБ через внедрение и поддержку мер и средств обеспечения ИБ. СМИБ, в свою очередь, оказывает управленческое и

организационное влияние на СИБ, что говорит о взаимосвязанности компонентов и процессов подсистем СОИБ друг с другом [68]. СИБ включает в себя совокупность защитных мер, реализующих процессы обеспечения ИБ организации и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение (таблица 1.4).

Таблица 1.4 – Терминологическая основа СОИБ [составлено автором на основе [30; 47; 53]]

Термин	Определение
Система информационной безопасности (СИБ)	совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение
Система менеджмента информационной безопасности (СМИБ)	часть общей системы управления, основанная на использовании методов оценки производственных рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ
Система обеспечения информационной безопасности (СОИБ)	совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения ИБ

СМИБ состоит из совокупности процессов управления ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов [17; 69; 90]. С учетом этого можно выделить следующие ключевые компоненты СОИБ в ОГВ:

– меры (правовые, организационные и технические), направленные на предотвращение различных угроз безопасности информации;

– средства, необходимые для реализации мер обеспечения ИБ;

– управленческие процессы, направленные на реализацию мер и средств обеспечения ИБ;

– обеспечение необходимого уровня поддержания свойств информационных активов за счет внедрения и поддержки, а также управления и организационного обеспечения мер и средств обеспечения ИБ [71].

С учетом акцента работы на управленческие аспекты формирования СОИБ, особого внимания заслуживает СМИБ (как составная часть системного управления ИБ). Под управлением ИБ в ОГВ можно понимать целенаправленное изменение состояния информационных активов ОГВ с целью минимизации

возможного ущерба (обеспечения приемлемого уровня рисков) в интересах достижения производственных целей органа.

Управление ИБ может быть корректирующим (коррекционные действия, следящее управление), предиктивным или упреждающим (проактивные действия, прогнозирующее управление). Здесь важно отметить особое значения управления рисками ИБ, позволяющее планомерно оптимизировать процессы СОИБ. Особого внимания в данном контексте с учетом скорости развития процессов исследуемой сферы заслуживает предиктивное управление рисками ИБ, которое может считаться наиболее эффективным подходом [72].

СМИБ в ОГВ на организационном уровне включает в себя структуры и штатные единицы, в полномочия которых входит управление ИБ, а также нормативно-методическое, информационно-справочное и техническое обеспечение данных процессов.

Переходя к аспектам формирования оптимальной СОИБ в ОГВ, важно отметить, что П.А. Лонциха и О.М. Сафонова отмечают следующие преимущества для организации при использовании процессно-ориентированного подхода к обеспечению ИБ:

– повышение конкурентных преимуществ;

– рост организации в международных рейтингах;

– повышение стоимости акций;

– демонстрация партнерам и клиентам организации высокого уровня надежности за счет повышения управляемости СОИБ;

– снижение рисков для активов, связанных с возможными затратами;

– повышение прозрачности процессов управления в организации [73].

Поэтому необходимо проанализировать использование системного подхода вместе с процессным. На рисунке 1.10 отображен комплексный подход к формированию и развитию СОИБ в ОГВ. Такой подход позволяет увидеть взаимосвязь между ключевыми ответственными за обеспечение ИБ подразделениями и обобщенный перечень ключевых процессов, входящих в основные подсистемы [74; 75].

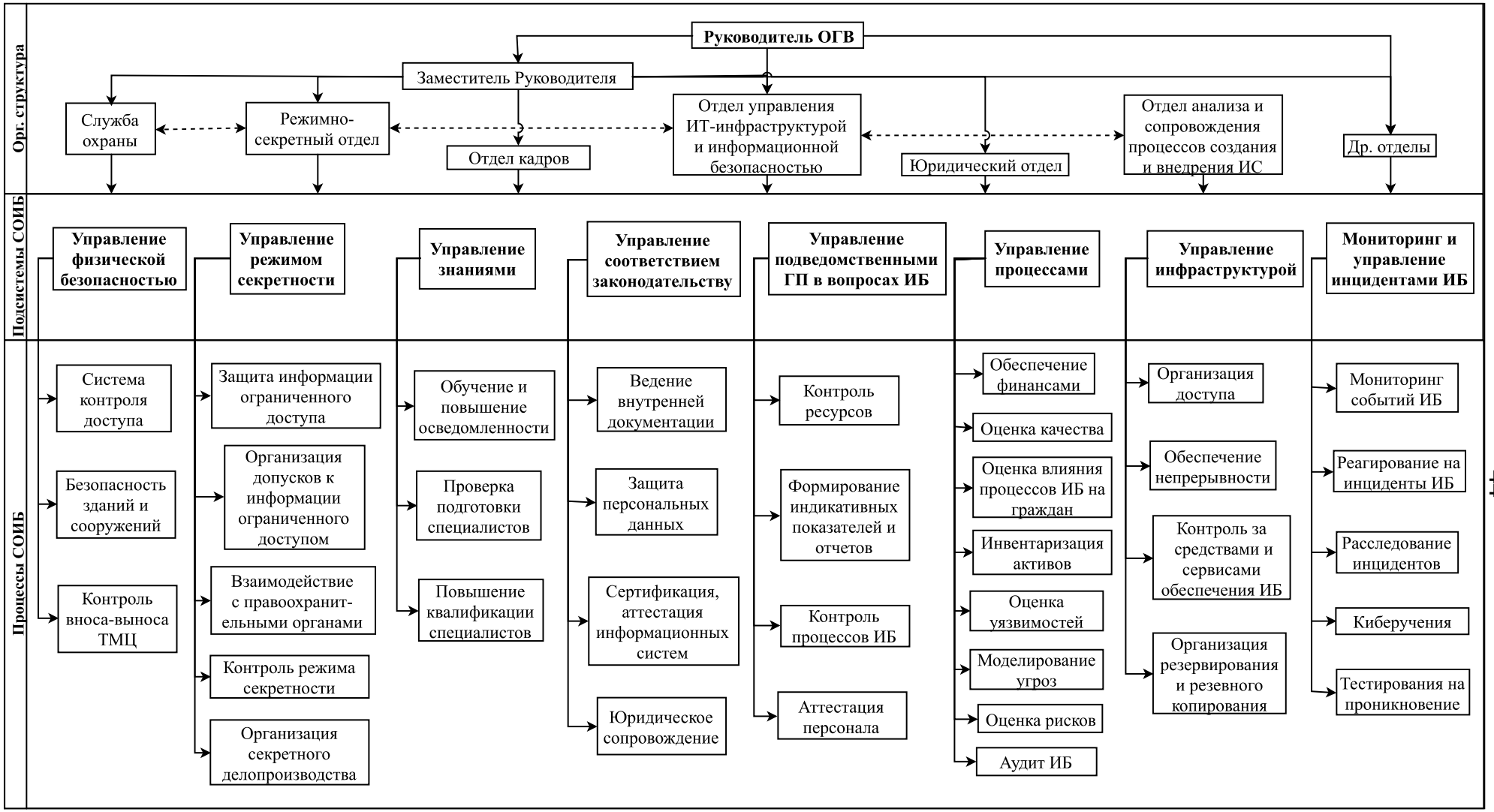

Рисунок 1.10 – Комплексный подход к формированию и развитию СОИБ в ОГВ [составлено автором]

Комплексная СОИБ в ОГВ включает в себя совокупность мероприятий, выполняемых структурными подразделениями и ответственными лицами органов, и создается с использованием мер, средств и способов обеспечения ИБ, основанных на процессах, организованных и функционирующих согласно нормативно закрепленным правилам.

Особое значение здесь приобретает связь системного и процессного подходов при реализации контрольно-надзорных функций уполномоченными регуляторами за выполнением требований законодательства, позволяя подходить к совершенствованию СОИБ в ОГВ не только с точки зрения оценки соответствия формальным требованиям, но осуществляя гибкий подход к анализу и оценке рисков и зрелости процессов обеспечения ИБ. Построение представленной схемы помогает определить ключевые подсистемы и процессы СОИБ в ОГВ. Важно отметить, что по мнению автора, именно комплексная модель, включающая элементы системного и процессного подхода, является наиболее гибкой и эффективно интегрируемой в управленческие модели.

Отметим, что во многих ОГВ отделы, в компетенцию которых входят осуществление функций поддержки и развития ИТ и ИБ-систем, объединены. Однако, как в соответствии с «лучшими практиками», так и согласно нормативным правовым актам РФ, вопросами обеспечения ИБ должно заниматься выделенное структурное подразделение с определенными компетенциями и полномочиями. Указанный подход можно считать оптимальным для ОГВ, т.к. он сочетает четкую иерархию исполнения и гибкую структуру процессов, детально распределенных между ответственными за обеспечение ИБ подразделениями и сотрудниками [76-78].

Данный тезис подкрепляется тем, что обеспечение ИБ в ОГВ с учетом постоянно меняющейся информационной среды в настоящее время не может быть одноразовым актом. Эффективное обеспечение ИБ в ОГВ осуществляется непрерывно и заключается в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития СОИБ через непрерывный контроль ее состояния, выявление и устранение ее слабых мест.

При внедрении СМИБ общепринятой «лучшей практикой» является обеспечение функционирования системы согласно циклу Деминга (далее – PDCA), в основе которого лежит процессный циклический подход, включающий этапы планирования, реализации, контроля и совершенствования. Актуальность применения цикла PDCA, несмотря на давность его существования, остается явной, о чем свидетельствуют научные работы и современные стандарты (ГОСТ, ISO, NIST и др.) [79-81; 83, 88; 144; 220; 221]. Применение цикла PDCA позволяет эффективно систематизировать деятельность и выстроить эффективную структуру процессных взаимосвязей на управленческом и исполнительском уровне [84; 85].

Рассмотрим альтернативную подходу PDCA семиуровневую модель управления информационными технологиями, принятую в стандарте COBIT 5. Такая модель на этапе средней зрелости процессных подходов в ОГВ, превалирующем на постсоветском пространстве не повысит эффективность внедряемых мер, т.к. внесение дополнительных уровней только увеличит неопределенность [82].

С учетом изученных работ можно сделать вывод о том, что для ОГВ подходы, использующие цикл PDCA, могут являться базой для применения на практике, однако, важно также учитывать непрерывно, нелинейно и хаотично меняющиеся реалии информационного пространства. Такой подход возможен только при тщательном отслеживании всех изменений в информационном поле ОГВ, учете всех рисков ИБ, эффективной их оценке и переоценке, и главное – адаптируемости (гибкости) внедряемых процессов ИБ под отраслевые и производственные реалии, в которых функционирует орган с постоянным учетом тенденций и трендов, формируемых как злоумышленниками, так и регуляторами.

Принимая во внимание основные тенденции в сфере обеспечения ИБ, базируясь на одной из основополагающих в области управления ИБ серии стандартов ГОСТ Р ИСО/МЭК 2700х, в рамках диссертационного исследования автором составлена оптимизированная модель ключевых процессов СОИБ (рисунок 1.11).

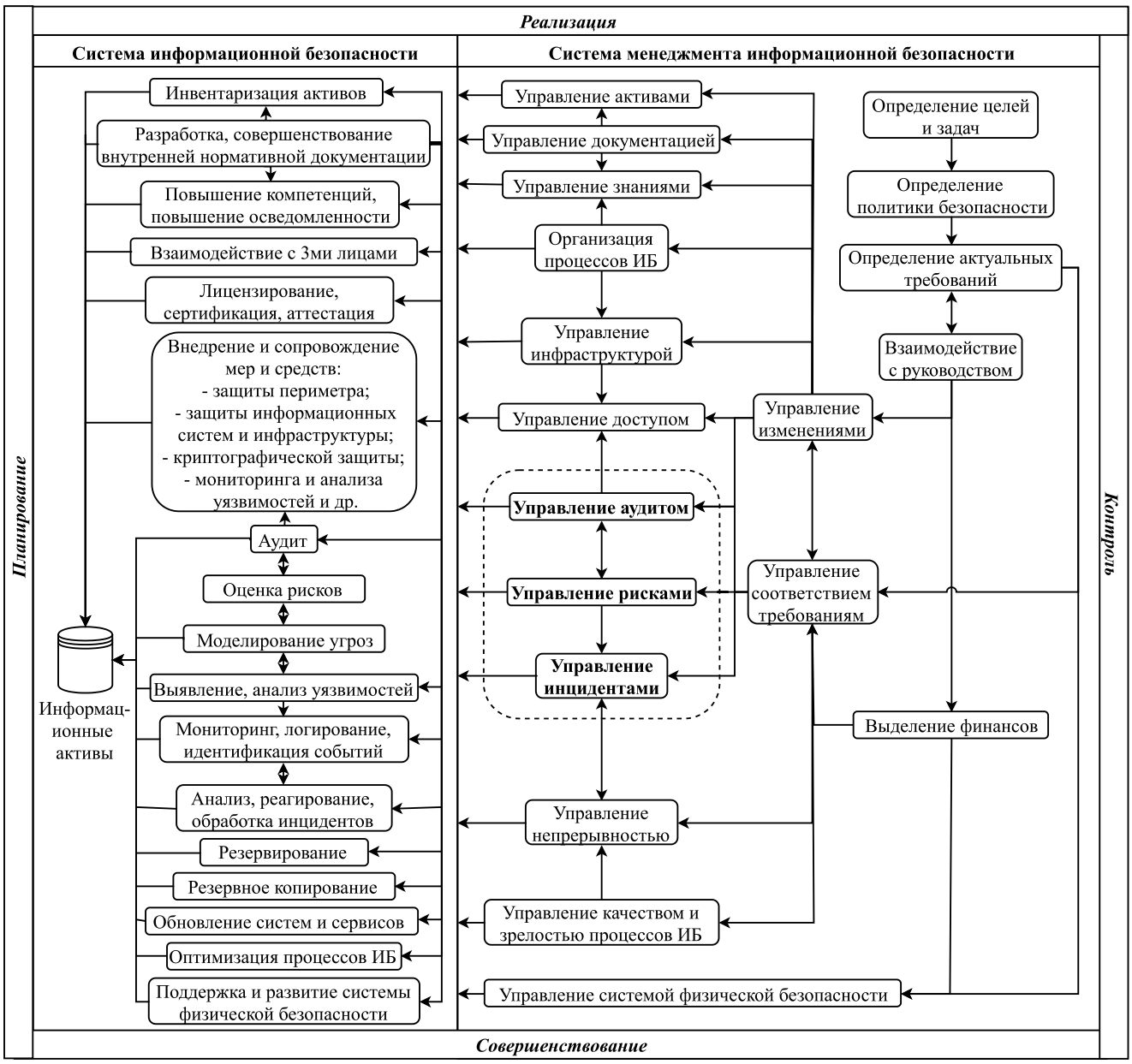

Рисунок 1.11 – Модель процессов СОИБ согласно серии ГОСТ Р ИСО/МЭК 2700х [составлено автором на основе [17; 53; 86; 88]]

Анализ каждого из рассматриваемых процессов позволяет определить связи и элементы по формированию СОИБ. Исходя из приведенной схемы, основными процессами, способствующими совершенствованию СОИБ при ее оценке и анализе в рамках СМИБ, можно назвать:

– управление аудитом (анализ и оценка состояния мер, средств и процессов обеспечения ИБ);

– управление рисками (анализ, выявление угроз и уязвимостей, оценка и обработка рисков ИБ);

– управление инцидентами (организация процессов обнаружения, обработки и реагирования на инциденты ИБ).

Особое значение для настоящего исследования с точки зрения его важности для управленческих аспектов имеет управление рисками, аудитом и инцидентами ИБ, которые являются обязательными требованиями многих передовых стандартов и методологий. Реализация указанных процессов позволяет эффективно и своевременно выявлять недостатки СИБ и СМИБ, по сути, являясь ключевыми инструментами для внутреннего взаимодействия на разных уровнях полномочий и компетенций, обеспечивая основу для оценки эффективности мер, средств и процессов ИБ в ОГВ [43; 105].

Также, исходя из приведенной схемы, важнейшими процессами СМИБ являются «управление доступом» (организация процессов предоставления доступа), и «управление инфраструктурой» (организация внедрения и сопровождения мер и средств защиты информации, мониторинга, анализа и др.).

Переходя к анализу подходов к формированию СОИБ в ОГВ, важно учесть недостатки обобщенных стандартизированных подходов, устранение которых заключается в адаптации подсистем и процессов под реалии и специфику конкретного ОГВ. На основе работы А.С. Исаева определен и оптимизирован перечень недостатков типовых подходов к обеспечению ИБ в ОГВ [89] (таблица 1.5).

В результате определения недостатков реализации типовых подходов к обеспечению ИБ в ОГВ и путей их оптимизации, можно сделать вывод о том, что несмотря на целесообразность и необходимость использования стандартизированных методологий и «лучших практик», крайне важную роль в настоящее время занимает гибкий анализ и непрерывный мониторинг состояния СОИБ, а также компетентность ответственных за обеспечение ИБ сотрудников, функции которых состоят в адаптации передовых методик к производственной деятельности [90; 194; 195].

Таблица 1.5 – Пути оптимизации основных недостатков при реализации типовых подходов к обеспечению ИБ в ОГВ [составлено автором на основе [89]]

Недостаток	Следствия (проблемы)	Решения (способы оптимизации)
Отсутствие единой системы управления ИБ	Отсутствие единого подхода к управлению ИБ в ОГВ (невозможность вести стратегическое, тактическое и оперативное управление ИБ), что создает условия невозможности предиктивного управления ИБ	– создание консультационной комиссии внутри ОГВ; – разработка релевантной нормативной базы); – повышение заинтересованности руководства ОГВ в совершенствовании подходов к ИБ; – детализация и перераспределение полномочий между подразделениями, выделение ответственных; – создание дополнительных подразделений по ИБ; – автоматизация процессов управления ИБ; – разработка релевантной нормативной правовой базы.
	Снижение эффективности СИБ за счет увеличения времени реакции персонала по ИБ из-за отсутствия единых правил и механизмов управления	
	Увеличение нагрузки на ответственный за ИБ персонал, ввиду необходимости применения различных механизмов управления множеством составных элементов СИБ	
Отсутствие качественной обратной связи от исполнителей	Отсутствие возможности рационального планирования работ по ИБ	– создание комиссии внутри ОГВ с полномочиями по формированию Политики ИБ; – повышение компетентности персонала ответственного за обеспечение ИБ; – автоматизация процессов обратной связи; – повышение заинтересованности исполнителей и руководителей в обратной связи; – формирование гибких риск-ориентированных циклических системных подходов с регулярными оценками процессов; – создание отлаженных механизмов по взаимодействию исполнителей с руководством и управлению инцидентами.
	Создание документов, неполноценно соответствующих реальным потребностям и требованиям ИБ в ОГВ для реализации организационных и технических мер	
	Усложнение принятия своевременных и эффективных управленческих решений по ИБ для обеспечения непрерывности работы ОГВ	
	Отсутствие должного внимания руководства ОГВ к анализу и оценке подходов к обеспечению ИБ	
Неиспользование средств автоматизации при использовании и реализации средств и мер обеспечения ИБ	Низкая эффективность работы ответственных, при реализации организационных и технических мер обеспечения ИБ	– повышение заинтересованности руководства ОГВ в совершенствовании подходов к ИБ; – повышение компетентности ответственных за обеспечения ИБ; – оптимизация имеющихся, внедрение недостающих средств автоматизации процессов обеспечения ИБ.
	Отсутствие замкнутости жизненного цикла организационно-распорядительных документов по ИБ в ОГВ	
	Существенные временные разрывы между процедурами внедрения технических средств обеспечения ИБ и сопровождающих их организационных мер	
Отсутствие аналитической составляющей процессов СОИБ	Существенные затруднения при противодействии новым, нестандартным действиям нарушителей, при использовании ими нетиповых методов обхода средств обеспечения ИБ	– формирование комплексных подходов к обеспечению ИБ; – внедрение передовых методик по мониторингу и анализу защищенности через оценку мер средств, процессов, а также угроз, уязвимостей и рисков ИБ через использование эффективных методологий; – оценка рисков, гибкий, периодичный и максимально расширенный анализ текущего состояния СОИБ и эффективности применяемых методов и способов защиты; – проведение учений, отработка инцидентов ИБ в лабораторных условиях.
	Нерациональное планирование и расходованию бюджета, выделяемого на обеспечения ИБ из-за отсутствия анализа текущего состояния СОИБ, а также эффективности применяемых методов и способов защиты	
	Отсутствие эффективных инструментов по отслеживанию состояния ИБ в органе и подведомственных ему учреждениях	

Исходя из проведенного анализа следует, что систематизация и структуризация ключевых процессов обеспечения ИБ позволяет выработать подход «от общего к частному» и сформировать не только комплексное всестороннее рассмотрение исследуемых процессов, но и выстроить четко отлаженную и понимаемую вертикаль взаимодействия ответственных за ИБ сотрудников с руководством ОГВ с помощью оценки состояния СОИБ, а также оптимизировать принятие решений по внедрению рекомендаций, отраженных в отчетах по результатам анализа, и сформировать циклический подход к совершенствованию процессов ИБ в ОГВ [91].

Как было отмечено, эффективное управление ИБ требует непрерывного получения достоверной и своевременной информации о состоянии обеспечения ИБ и принятия своевременных управленческих решений. В данном смысле особое значение приобретают подсистемы «мониторинг и управление инцидентами» и «управление инфраструктурой», в которых реализованы такие ключевые процессы как «обеспечение непрерывности» и «мониторинг событий ИБ», позволяющие вести наблюдение за состоянием ключевых компонентов СОИБ, осуществлять сбор, анализ и обработку данных под заданные руководством цели, связанные с защитой информационных активов ОГВ, и обеспечивать бесперебойность выполнения производственной деятельности [92; 93].

Эффективное управление подсистемами СОИБ высшим руководством ОГВ, формирующего стратегию развития системы, требует релевантного инструмента для оценки процессов обеспечения ИБ. Данным инструментом является «аудит ИБ», который по мнению многих экспертов является одним из наиболее эффективных процессов корпоративного контроля за обеспечением ИБ, значимость которого постоянно повышается [94].

Как отмечают С.И. Козьминых и П.С. Козьминых, только на основе выявленных в процессе проведения аудита ИБ и своевременно устраненных недостатков можно создавать эффективные и надежные СОИБ [95]. Таким образом, оценка состояния СОИБ через ее аудит является одним из ключевых процессов формирования, управления и поддержки ИБ в ОГВ, позволяя

руководству организации определить состояние ключевых подсистем и процессов, оценить их защищенность, риски ИБ, корректно и обоснованно подойти к вопросу обеспечения ИБ.

Периодическая проверка защищенности СОИБ через аудит ИБ, согласно «лучшим практикам», является неотъемлемым процессом, играющим крайне важную роль для формирования СОИБ, давая возможность определить слабые места в системе защиты, выявить уязвимости, дать оценку подготовленности персонала, а также сформировать всесторонние приоритезированные риск-ориентированные рекомендации по совершенствованию системы [96].

Также актуальность регулярного аудита ИБ обусловлена тем, что он является обязательным с точки зрения нормативных правовых актов РФ в сфере обеспечения ИБ [78; 55]. В настоящее время в РФ во многих отраслях законодательно закреплена необходимость проведения оценки состояния СОИБ в форме внутреннего аудита, проводимого силами работников организации, или внешнего аудита, проводимого специализированными организациями.

Как было отмечено ранее, адаптация любой «эталонной» модели под конкретные условия ОГВ, эффективная оценка, учет всех изменений и тенденций, несмотря на все опасности возникновения волюнтаристских подходов, являются ключевыми факторами обеспечения эффективности СОИБ, и, по мнению автора, должны использоваться в дополнение к любой методологии или стандарту [100].

Во многих проанализированных исследованиях отмечается тот факт, что мониторинг, прогнозирование управления состояниями информационных активов и иные процессы, затрагивающие СОИБ в ОГВ, на современном этапе не оптимизированы и нуждаются в качественных изменениях, что говорит об актуальности проводимого исследования [97-99].

Ключевыми целями проведения аудита ИБ в ОГВ можно назвать:

– оценку эффективности расходуемого на СОИБ бюджета (включает в себя анализ затрат на зарплаты специалистов, затрат на оборудование и др.);

– оценку эффективности ответственных за процессы СОИБ отделов, а также общий уровень подготовки кадров;

– определение технических, правовых и организационных аспектов, требующих оптимизации, выработка рекомендаций по повышению эффективности СОИБ;

– оценку соответствия СОИБ существующим стандартам и нормативным документам регуляторов;

– выработку рекомендаций по внедрению новых и повышению эффективности существующих мер и средств обеспечения ИБ [95, с. 183].

Важно провести корреляцию вышеуказанных целей с анализом работы В.В. Сагитовой, которая выделяет три основные вида оценки СОИБ:

1. Активная оценка защищенности заключается в проведении аудиторской группой атак на исследуемую систему и представляет собой анализ ее защищенности с точки зрения злоумышленника. Данный тип аудита состоит в исследовании защищенности обследуемых активов от внешних и внутренних атак. Результатом активного аудита ИБ является отчет об уязвимостях исследуемых активов, степени их критичности и включающий рекомендации по их устранению. Проведение активной оценки ИБ позволяет повысить уровень защищенности информационных активов организации при выявлении наиболее актуальных технических уязвимостей. Однако, результаты проведения только данного вида аудита могут оказаться недостаточными для создания эффективной и комплексной СОИБ, так как при нем недостаточно внимания уделяется проверке организационных и правовых мер, средств и процессов, позволяющей выявить нарушения в механизмах и регламентах по обеспечению ИБ.

2. Оценка на соответствие стандартам ИБ заключается в проверке состояния СОИБ требованиям государственных и отраслевых стандартов в сфере обеспечения ИБ (в РФ – ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 57580.1, Приказы ФСТЭК и др.). Результатом данного типа аудита является определение степени соответствия проверяемой информационной системы или среды стандартам, собственным внутренним требованиям организации в сфере обеспечения ИБ, нормативным правовым актам, документам, рекомендациям по созданию или модернизации СОИБ и др. требованиям.

3. Экспертная оценка, при которой производится подробное исследование СОИБ и ее сравнение с некоторой эталонной моделью, которая может формироваться на основе требований заказчика и (или) методологий (фреймворков) и (или) собственного опыта компании аудитора. При данном виде аудита собирается информация об ИС, организационно-распорядительных документах и локальных нормативных актах организации, результатах предыдущих проверок. Данная информация детально анализируется аудитором, выявляются недостатки систем. Сбор данных о СОИБ также проводится путем интервьюирования руководства и специалистов организации и заполнения специальных опросных анкет. По результатам экспертной оценки предлагаются рекомендации по устранению выявленных уязвимостей, уменьшению рисков ИБ, выбору и внедрению мер и средств ИБ, совершенствованию СОИБ [101, с. 27].

По мнению автора, экспертная оценка СОИБ имеет ряд преимуществ перед другими видами, т.к. она позволяет произвести гибкий системный анализ, выполнить требования руководящих документов и оценить процессы обеспечения ИБ, используя различные инструменты, а также применить индивидуальный подход, основанный на опыте экспертов и методологической базе мирового сообщества. Однако, с учетом всех реалий экспертная оценка должна быть дополнена качественным инструментальным тестированием СОИБ.

Целесообразно отметить важность оценки соответствия требованиям регуляторов и «лучшим практикам» через аудит ИБ, т.к. именно этот способ позволяет как комплексно оценить уровень организационных, технических и правовых мер и средств обеспечения ИБ, так и выстраивать общегосударственную СОИБ используя оценку уровня ИБ в ОГВ [102; 106].

С учетом постоянно растущего количества угроз безопасности информации указанные варианты оценки СОИБ по отдельности не могут эффективно выявить существующие уязвимости, угрозы и оценить риски ИБ в ОГВ. При этом особую роль на современном этапе играет именно «активная» оценка, при которой в результате экспертного анализа можно увидеть состояние информационных активов ОГВ и оценить все риски в максимально детализированном формате.

Исходя из этого, способствовать эффективной оценке состояния СОИБ может только комплексный подход, сочетающий экспертный аудит с элементами оценки на соответствие требованиям нормативных документов, оценки рисков ИБ и перевод максимального количества подходящих для этого процессов в автоматизированный вид.

Процесс цифровизации сопровождается постоянным ростом угроз и уязвимостей, а также развитием методов и средств их эксплуатации. В таких условиях вышеперечисленные виды оценки могут не давать достаточный уровень достоверности в том, что СОИБ в ОГВ является эффективной, а вероятность возникновения инцидента ИБ минимизирована. Поэтому в сложившейся ситуации крайне важным инструментом по оценке СОИБ в ОГВ является проведение силами квалифицированных экспертов регулярного качественного инструментального тестирования на проникновение (Penetration Test) или наиболее приближенного к реалиям формата (Red Team).

В результате проведенного исследования работ, затрагивающих вопросы оценки состояния СОИБ, был сделан вывод о том, что существующие обобщенные модели имеют ряд недостатков и могут быть усовершенствованы для ОГВ с точки зрения точности, системности и детальности компонентов и процессов. Важно отметить отсутствие универсального метода оценки, т.к. ни один из способов не позволяет удовлетворить все потребности и устранить все актуальные для ОГВ угрозы безопасности информации. Определив сильные и слабые стороны способов оценки состояния СОИБ, можно констатировать, что для ОГВ наиболее подходящим является использование подхода, синтезирующего риск-ориентированную модель экспертного «аудита» – для оценки на организационно-техническом уровне, с форматами оценки на соответствие стандартам ИБ и активного аудита. При таком подходе, включающем в себя оценку на разных уровнях, по мнению автора, состояние СОИБ в ОГВ будет возможно оценить наиболее эффективно и комплексно.

1.3. Зарубежный опыт функционирования систем обеспечения информационной безопасности в органах государственной власти

Массовые потери данных, кража интеллектуальной собственности, кредитных карт, персональных данных (далее – ПД), угрозы конфиденциальности и отказа в обслуживании – это реалии современного киберпространства, в котором активно функционируют различные криминальные группы и международные террористы, осуществляется экономический и военный шпионаж и попытки вывести из строя целые предприятия и объекты инфраструктуры. По своим последствиям экономический, политический и военный ущерб от кибератак в настоящее время может превышать потери от экономических санкций и даже от военных конфликтов [110].

Сложность взаимодействий между субъектами обеспечения ИБ растет, взаимозависимости расширяются, пользователи информационных систем ОГВ становятся более мобильными, а угрозы эволюционируют. Новые технологии приносят большие преимущества одновременно создавая массу рисков и угроз. Поэтому с учетом масштабов цифровизации ни один руководитель ОГВ на современном этапе не может думать о вопросе обеспечения ИБ как об отдельной проблеме. Решить накопившиеся вопросы можно только сообща, формируя эффективные общегосударственные и межгосударственные механизмы взаимодействия [107-109].

В существующих условиях согласованные действия государств по обеспечению ИБ на национальном и глобальном уровне сталкиваются с многочисленными препятствиями, включая различие интересов стран, разный уровень социального, технического, экономического развития. Проблемы обеспечения ИБ остро стоят перед всеми, даже самыми развитыми государствами, политическими и государственными институтами, корпорациями и финансовыми структурами. Поэтому особую важность для настоящего исследования имеет

анализ организационно-правовых подсистем развитых государств, позволяющий сформировать комплексное видение преимуществ и недостатков используемых подходов [111; 112].

Ключевым геополитическим соперником РФ на информационном поле является США, поэтому, как с данной позиции, так и с точки зрения того, что данное государство является первооткрывателем интернета и обладает наиболее весомым экономическим и технологическим потенциалом в исследуемой области, анализ СОИБ США представляет особый интерес. Важно также обозначить, что как отмечает Н. В. Киселёва, в современных условиях полноценный цифровой суверенитет есть только у США [113].

В США ИБ является неотъемлемой частью национальной безопасности. Ключевым системообразующим регулятором в сфере обеспечения ИБ является Минобороны США, включающее более 40 подведомственных структур. Конгресс выделяет бюджет на запрашиваемое Администрацией Президента финансирование. Совет по национальной безопасности и Комитет начальников штабов вместе с Президентом формируют стратегию развития отрасли. Бюджет США, расходуемый на инвестирование множества институтов, агентств и органов власти несопоставим ни с одним бюджетом в мире и прямые расходы на решение вопросов кибербезопасности непрерывно растут. Так, в 2019 г. США выделило на расходы в сфере кибербезопасности 8,5 млрд долл. США, а сумма в проекте бюджета на 2020 г. превысила 9,6 млрд долл. США [114].

Переходя к анализу подсистемы нормативного регулирования в сфере обеспечения ИБ США, стоит отметить о ее сложности и разветвленности. Как отмечает Н. В. Киселева, только за 2002 г. в Конгресс было представлено более 400 законопроектов, призванных регулировать информационную сферу и в дальнейшем число предлагаемых законопроектов, ещё более увеличивалось. Вопросы обеспечения ИБ в США регулируются преимущественно федеральным законодательством. Первым фундаментальным законодательным актом США в сфере обеспечения ИБ был Закон об информационной безопасности (Computer Security Act of 1987), который установил минимальный уровень требований по

обеспечению ИБ федеральных информационных систем и, по сути, заложил правовую основу создания американской федеральной СОИБ. В соответствии с данным законом операторы всех федеральных информационных систем, содержащих какую-либо конфиденциальную информацию, должны были разработать собственные планы обеспечения ИБ [113].

В 2000 г. в США были смягчены экспортные ограничения для информационных технологий и принят новый стандарт электронной цифровой подписи. Закон 2000 г. «О защите авторских прав в цифровую эпоху» установил ответственность за нарушение авторского права. Также в 2000 г. «Национальным планом защиты информационных систем на 2000-2003 гг.» был создан новый координирующий орган – Национальный консультативный совет по инфраструктуре (NIAC) и одобрено формирование специальных ведомственных центров ИБ, которые на основе федеральной сети обнаружения вторжения (FIDNet) выявляют вторжения и оповещают государственные, частные и производственные организации об угрозах ИБ [115].

В октябре 2001 г. был принят «Акт о патриотизме» (USA Patriot Act), в котором обозначены системы и средства, которые важны для США в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации – жизненно важной (критической) информационной инфраструктуры. Объём отраслей, затронутых данной сферой, включил экономику, социальную сферу, все средства связи, энергетику, транспорт, ОГВ и др. [116].

В 2002 г. Министерство внутренней безопасности США (The United States Department of Homeland Security) представило «Национальную стратегию внутренней безопасности» (National Strategy for Homeland Security), в которой защита критической информационной инфраструктуры определялась как одна из ключевых задач обеспечения национальной безопасности. Закон 2002 г. «О внутренней безопасности» (Home Security Act, H.R. 5005) установил, что для обеспечения безопасности создаются специальный Комитет (House Homeland Security Committee) и Министерство внутренней безопасности, первоочередной

задачей которых было снижение уязвимости информационной инфраструктуры США. В составе Министерства внутренней безопасности были созданы Управление анализа информации и защиты инфраструктуры (IAIP), Управление науки и технологий (S&T), Национальное подразделение кибернетической безопасности (NCSD), главным элементом которого становился Центр экстренного реагирования на компьютерные происшествия в США (US-CERT – U.S. Computer Emergency Response Team), образованный за счет объединения трех ранее существовавших групп немедленного реагирования (CC/CERT, NCS, NIPC) [117; 118].

Касательно обобщенного подхода к регулированию области обеспечения безопасности критической информационной инфраструктуры – в США каждый критически важный сектор обладает уникальными характеристиками, операционными моделями и профилями рисков, подкрепляется отраслевыми агентствами, обладающими специализированными институциональными знаниями по конкретным секторам. Важно отметить, что нормативное регулирование в каждой сфере (к примеру, энергетики или связи) в США осуществляют отдельные органы, издающие обязательные к выполнению НПА.

Рекордное многообразие органов и различных НПА в исследуемой сфере является спецификой американского регулирования, которое затрудняет имплементацию подобного подхода в иных юрисдикциях. Государственный департамент в координации с Министерством национальной безопасности и другими федеральными департаментами, агентствами привлекают иностранные правительства и международные организации для укрепления безопасности и устойчивости критической информационной инфраструктуры, расположенной за пределами США, а также для содействия общему обмену «лучшими практиками» и опытом.

В 2003 г. в США была принята «Национальная стратегия физической защиты критической инфраструктуры и важнейших объектов» (The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. 2003», которая установила стратегические цели, задачи и принципы государственных

структур в области обеспечения безопасности критической информационной инфраструктуры. Также в 2003 г. была опубликована «Национальная стратегия защиты киберпространства» (National Strategy to Secure Cyberspace), которая строилась на фактическом отстранении государства от решающей роли в вопросах защиты критической информационной инфраструктуры, сосредотачиваясь на стандартизации и общем руководстве совместной деятельностью государственных и негосударственных организаций, возлагая на частный капитал большую часть ответственности за обеспечение ИБ [120].

Стоит отметить, что наделение различных ОГВ США полномочиями в сфере обеспечения ИБ позволяет создать всестороннее и сбалансированное регулирование в данной области (таблица 1.6) [121, с. 47].

Таблица 1.6 – Основные регуляторные органы США в сфере обеспечения ИБ и их функции [составлено автором на основе [122-130]]

Регулятор	Основные функции, связанные с обеспечением ИБ
1	2
Федеральная комиссия по связи (Federal Communications Commission)	– определение и расстановка приоритетов регулирования сферы коммуникационной инфраструктуры; – выявление уязвимостей сектора связи и работа с отраслью и другими заинтересованными сторонами для устранения этих уязвимостей; – привлечение иностранных правительств и международных организаций к повышению уровня безопасности и устойчивости критической информационной инфраструктуры в сфере связи; – содействие развитию и внедрению передового опыта, способствующего обеспечению безопасности и устойчивости критической информационной инфраструктуры в сфере связи.
Министерство внутренней безопасности (Department of Homeland Security, DHS)	– оценивание национальных возможностей и проблем в области обеспечения безопасности критической информационной инфраструктуры; – анализ угроз, уязвимостей и потенциальных последствий всех угроз для критической информационной инфраструктуры; – определение функций безопасности и устойчивости, которые необходимы для эффективного взаимодействия между государственным и частным секторами во всех секторах критической информационной инфраструктуры; – разработка национального плана и показателей по координации с отраслевыми агентствами и другими партнерами в области обеспечения безопасности критической информационной инфраструктуры; – объединение и координация федеральных межсекторальных мероприятий по обеспечению безопасности и устойчивости критической информационной инфраструктуры; – выявление и анализ ключевых взаимозависимостей между важнейшими секторами критической информационной инфраструктуры; – сообщение об эффективности национальных усилий по укреплению безопасности и устойчивости критической информационной инфраструктуры.
Министерство обороны (Department of Defense, DoD)	– обеспечение безопасности, функционирования и развития технических средств разведки и ИТ при обеспечении безопасности военных систем; – различные координационные функции между государственными субъектами ИБ по розничным направлениям.

Продолжение таблицы 1.6

1	2
Министерство юстиции (Department of Justice, DOJ)	Расследование, препятствование, преследование по закону и уменьшение иным образом иностранных разведывательных, террористических и других угроз безопасности информации, а также фактические или попытки нападения, или саботажа, связанного с критической информационной инфраструктуры.
Федеральное бюро Расследований (Federal Bureau of Investigation, FBI)	– проведение контртеррористических и контрразведывательных расследований и связанной с этим деятельности правоохранительных органов в секторах критической информационной инфраструктуры; – осуществление сбора, анализа и распространения информации о киберугрозах на национальном уровне; – несет ответственность за деятельность NCIJTF.
Агентство кибербезопас-ности и защиты инфраструктуры США (Cybersecurity and Infrastructure Security Agency CISA)	– является национальным консультантом по рискам, сотрудничая с партнерами в целях защиты от угроз для создания более безопасной и устойчивой инфраструктуры; – сотрудничество с субъектами отраслей индустрии и Правительством для понимания и управления рисками критической информационной инфраструктуры; – наращивание национального потенциала для защиты от кибератак; – работа с федеральным правительством по предоставлению инструментов кибербезопасности, служб реагирования на инциденты и возможностей оценки защиты сетей, поддерживающих ключевые операции; – координация усилий по обеспечению безопасности и устойчивости критической информационной инфраструктуры, используя надежные партнерские отношения между частным и государственным секторами; – предоставление технической помощи и оценки федеральным субъектам, а также владельцам инфраструктуры и операторам; проведение общенациональной информационно-пропагандистской работы по поддержке и расширению возможностей реагирования на инциденты ИБ.
Национальный институт стандартов и технологий (NIST)	– разработка методологических основ для минимизации рисков кибербезопасности критической информационной инфраструктуры; – получение обратной связи от субъектов ИБ и инкорпорации «лучших отраслевых практик».
Национальная объединенная рабочая группа по кибер-расследованиям (National Cyber Investigative Joint Task Force, NCIJTF)	– выступает в качестве межведомственного национального координационного центра; – координация, интеграция и обеспечение обмена информацией при поддержке расследований киберугроз; – предоставление и поддержка анализа разведывательных данных, а также обеспечение ценности других текущих усилий в борьбе с киберугрозами.

В организационной структуре СОИБ США явно прослеживается неразрывность связи военной и национальной безопасности с информационной, т.к. ключевыми регуляторами являются Министерство обороны и Министерство внутренней безопасности (Приложение Б), что говорит об уровне осознания государством взаимосвязи национальной и информационной безопасности [121, с. 45]. Так, на Национальный институт стандартов и технологий (NIST) возложена общая ответственность за исполнение требований Закона в сфере обеспечения ИБ и разработку стандартов и руководств по вопросам ИБ. Кроме того, институт должен регулярно вести научные исследования по выявлению

угроз и уязвимостей ИБ и оценивать их масштаб, а также вырабатывать целесообразные меры по защите для их применения как в государственных, так и в частных информационных системах.

В структуре федеральных ОГВ, вовлеченных в обеспечение безопасности критической информационной инфраструктуры, создаются специальные структуры, разрабатывающие методологические подходы и руководства, и реализующие программы информационной поддержки в отдельных областях, закрепленных за ними [113]. Однако, такой подход требует существенных расходов со стороны государства, поскольку каждое ведомство инициирует и реализует программы в рамках отдельных бюджетов, а также предъявляет высокие требования к уровню профессиональной подготовки штата в рамках каждого уполномоченного ведомства, что на практике может вызвать затруднения при отсутствии достаточного количества высококвалифицированных специалистов. Кроме того, в подобной США системе значительные ресурсы должны быть направлены на координацию совместных усилий нескольких уполномоченных ОГВ.

С целью придания комплексности проводимому анализу важно проанализировать Европейские подходы к обеспечению ИБ. Здесь стоит отметить, что большинство направлений реализации контрольно-надзорной деятельности внутри государств Европейского Союза (далее – ЕС) согласно тенденциям последних лет характеризуется ужесточением государственного контроля. Это проявляется, в первую очередь, в принимаемых законодательных нормах о полномочиях специальных служб, конкретизации требований и введении финансовых взысканий.

Отметим, что одним из приоритетных направлений в сфере обеспечения ИБ для ЕС является защита ПД. Как отметили В.М. Володин, Л.В. Рожкова и О. В. Сальникова, международные события последних лет выявили потребность в поиске баланса между обеспечением прав и свобод индивидов, тесно связанного с обеспечением ИБ в национальном масштабе [131, с. 60]. Сбор, анализ и перемещение ПД по всему миру приобрели огромное экономическое значение.

ПД в настоящее время – это «валюта» современной экономики и важность обеспечения их контроля и сохранности с целью избегания утечек и манипуляций третьими лицами признаны на общеевропейском уровне [132].

Так, международное признание важности проблемы защиты ПД было закреплено в 1981 г. принятием странами Совета Европы Конвенции по защите данных о личности при автоматизированной обработке информации. Показательным элементом осознания важности системных подходов к обеспечению ИБ в ЕС является Общий Регламент по защите данных (далее – GDPR), разработанный и одобренный Европейским парламентом в 2016 г. и вступивший в силу 2018 г., который является экстерриториальным и распространяет свое действие на различные сферы общественной жизни, защищая ПД европейцев не только в странах ЕС, но и далеко за его пределами. В случае нарушения данного регламента предусмотрены штрафы, достигающие 20 млн евро или 4% оборота денежных средств нарушителя [133].

Для соответствия требованиям GDPR необходимо разработать внутренние политики защиты данных, обучать персонал, проводить проверки деятельности по обработке данных, вести документацию по процессам обработки, внедрять меры по встроенной системе конфиденциальности, назначить сотрудника ответственного за обработку ПД и др.

GDPR является важнейшим законодательным актом, который существенно повышает уровень защиты данных в ЕС и за его пределами, давая ясность и последовательность правил, обеспечивая доверие граждан, позволяя государству и бизнесу максимально использовать возможности на едином цифровом рынке ЕС и упрощая возможности следования единому набору правил защиты и обработки данных для внеевропейских игроков вместо необходимости учитывать национальные нюансы обработки ПД каждого отдельного государства, как это приходилось делать до введения GDPR. Более того, реформа направлена на стимулирование экономического роста путем сокращения расходов и бюрократии для компаний, работающих в ЕС, ввиду чего соблюдение одного правила вместо

множества помогает маленьким и развивающимся компаниям выйти на новые рынки.

В рамках регулирования области обеспечения безопасности критической информационной инфраструктуры в ЕС была разработана Директива №2016/1148 от 06.07.2016, положения которой имплементируются в законодательство стран ЕС [134]. Проведенный анализ ключевых НПА в сфере обеспечения ИБ в ЕС (Приложение В) показал, что несмотря на все существующие вызовы и трудности, связанные с разным уровнем развития государств, общегосударственные подходы к формированию и совершенствованию СОИБ в государствах ЕС интенсивно развиваются.

Происходит данное развитие ввиду быстрого накопления опыта регулирования, координации действий государств и использования системных стратегий. Это подтверждает тот факт, что необходимость адекватного ответа на все новые вызовы и угрозы в киберпространстве становится одним из ключевых стимулов для формирования единого политического пространства ЕС [157].

Главными межгосударственными структурами по организации работ в области обеспечения ИБ ЕС является Организация Объединенных Наций и Совет Безопасности ООН, координирующие усилия государств по осуществлению мероприятий в сфере обеспечения ИБ и борьбы с преступлениями в отрасли ИТ. Анализ функций, задач и полномочий ключевых органов ЕС в сфере обеспечения ИБ показал, что пристальное внимание к системному подходу при обеспечении ИБ уделяется как на уровне Союза и государств ЕС, так и на уровне государственных и частных организаций (таблица 1.7).

Также проведенный анализ демонстрирует явное понимание в Европе необходимости улучшения взаимодействия и координации между различными учреждениями. Для поддержки кибербезопасности ЕС сотрудничает с такими структурами, как Организация экономического сотрудничества и развития, Генеральная Ассамблея ООН, Международный телекоммуникационный союз, ОБСЕ, Саммит информационного общества, Форум управления в интернете, а центральным остается сотрудничество ЕС с НАТО.

Таблица 1.7 – Основные регуляторные органы ЕС в сфере обеспечения ИБ [составлено автором на основе [135-138]]

Орган	Основные функции, связанные с обеспечением ИБ
Европейское агентство по сетевой и информационной безопасности (ENISA)	1. Оказание содействие государствам-членам ЕС в выполнении требований ИБ, включая нынешнее и будущее законодательство ЕС. 2. Поддержка в организации общеевропейских учений по кибербезопасности. 3. Выполнение роли центра экспертных знаний как для государств-членов ЕС, и учреждений ЕС с целью получения консультаций по ИБ.
Европейский центр по борьбе с киберпреступностью (ЕС3)	1. Выполнение роли центра кибер-криминальной информации и разведки. 2. Сопровождение операций по расследованию киберпреступности в государствах ЕС (оперативный анализ, координация и консультативная поддержка). 3. Выполнение широкого спектра функций стратегического анализа. 4. Комплексная информационно–пропагандистская функция, связывающая правоохранительные органы, борющиеся с киберпреступностью совместно с частным сектором, научными кругами и другими партнерами. 5. Поддержание подготовки кадров и наращивание потенциала кибербезопасности, в частности для соответствующих органов в государствах ЕС. 6. Обеспечивает высокоспециализированную техническую и цифровую судебно-медицинскую поддержку расследований и операций. 7. Представление правоохранительного сообщества ЕС в таких областях, как: исследования и разработки, управление интернетом и разработка общегосударственных политик.
Европейский Контролер (инспектор) по защите данных (EDPS)	1. Мониторинг и обеспечение защиты и конфиденциальности ПД при обработке учреждениями и органами ЕС. 2. Консультирование учреждений и органов ЕС по всем вопросам, связанным с обработкой ПД, по запросу или по нашей собственной инициативе. 3. Мониторинг и анализ технологий, которые могут повлиять на защиту ПД. 4. Взаимодействие с судом ЕС для предоставления экспертных консультаций по толкованию закона «О защите данных». 5. Сотрудничество с национальными надзорными органами и другими надзорными органами в целях повышения согласованности при защите ПД.
Группа по сотрудничеству (NIS)	Координация в вопросах оказания поддержки и упрощения стратегического сотрудничества и обмена информацией между государствами-членами ЕС.

Агентство ENISA, начиная с 2004 г., является ключевым институтом в области обепечения кибербезопасности ЕС, главной задачей которого является развитие сотрудничества между странами-членами ЕС. ENISA также призвано реализовывать три ключевых документа: Стратегию европейской кибербезопасности (2013 г.), Рамочный документ о европейской политике в области киберзащиты (2014 г.) и Стратегию о Едином европейском цифровом рынке (2015 г.). С целью преобразования теоретических знаний в практические навыки и определения готовности государственных и частных организаций ЕС к отражению кибератак в 2010, 2012, 2014 гг. ENISA проводило киберучения. Также важно отметить такие структуры, как созданный в 2013 г. Европолом Европейский центр по борьбе с киберпреступлениями (ЕСС), оказывающий

всестороннюю поддержку в вопросах расследований киберпреступлений на региональном и международном уровнях [139-142].

Европейский центр по борьбе с киберпреступностью (EC3) – орган, созданный Европолом в 2013 году с целью усиления правоохранительных органов ЕС в сфере кибербезопасности, а также защиты граждан, бизнеса и ОГВ ЕС от киберпреступности. EC3 фокусируется на мошенничестве с платежами, преступлениях, связанных с сексуальной эксплуатацией детей онлайн и другими киберпреступлениями.

В состав Группы по сотрудничеству (NIS) входят представители государств-членов ЕС, Европейской Комиссии и ENISA. Отметим также, что в соответствии с п. 1 и 3 ст. 8 Директивы NIS, а также ст. 9 Директивы 2016/1148, каждое государство-член ЕС должно [134; 143]:

– назначить один или несколько национальных компетентных органов, ответственных за безопасность сетевых и информационных систем (CA);

– создать единый национальный контактный пункт по вопросам безопасности сетевых и информационных систем (SPOC);

– создать группы реагирования на инциденты ИБ (CSIRT).

Важной мерой по усилению уровня обеспечения ИБ, с точки зрения Европейской комиссии, является предложенное комиссией в 2017 г. введение сертификатов для выпускаемой в странах ЕС цифровых активов и услуг, что может играть важную роль в усилении безопасности и развитии единого цифрового рынка ЕС с учетом ориентации процедуры на обеспечение ИБ. При этом само по себе введение сертификации не обеспечивает ИБ и не страхует от кибератак.

Переходя к уровню функционирования государственных СОИБ стран ЕС, сложно не согласиться с В.И. Пантиным и Н.В. Кардавой, в том, что особый интерес представляет подход Германии, отличительной чертой которого является комплексность и фундаментальный характер, включающий систему НПА, мер и институтов, отвечающих за их реализацию [145, с. 9]. Так, основа регулирования сферы обеспечения ИБ в ФРГ была заложена разработанным и принятым в 2005 г.

«Национальным планом защиты информационной инфраструктуры, (NPSI), и развита в 2007 г. – Планом его реализации (CIP Implementation Plan of the NPSI), разработанным при участии правительства и бизнеса и определяющим общую стратегию реагирования на кризисы в отрасли ИТ содержащим рекомендации по действиям в случае крупных кибератак [146]. Указанные документы обязали структуры разрабатывать и внедрять соответствующие процедуры реагирования на инциденты. Кроме того, в CIP Implementation Plan содержатся указания по созданию рабочих групп по различным аспектам кибербезопасности, включая кризисное управление, проведение киберучений и обеспечение постоянной доступности систем критической информационной инфраструктуры [147].

Принятая в 2011 г. «Национальная стратегия в области защиты критической информационной инфраструктуры» (CIP Strategy) обеспечивает формирование всестороннего межведомственного подхода к обеспечению безопасности критической информационной инфраструктуры ФРГ и включает в себя следующие основные направления [148]:

– осуществление ИБ на основании совместной деятельности гражданского общества и государства;

– обеспечение оптимизации оперативного сотрудничества между ОГВ и защиты критической информационной инфраструктуры с помощью Национального центра кибербезопасности (Nationales Cyber-Abwehrzentrum, NCAZ);

– координация превентивных мер и междисциплинарных подходов в области обеспечения кибербезопасности в государственном и частном секторах также возложена на NCAZ, который выступает дополнительным связующим звеном управления отраслью ИТ на федеральном уровне с участием ОГВ;

– повышение эффективности контроля за киберпреступностью включающее участие комплекса институтов с участием предпринимателей и правоохранительных органов, разрабатывающих нормативную правовую базу и рекомендации [148, с. 10].

В 2011 г. ФРГ приняла первую Федеральную стратегию кибербезопасности, которая вводила следующие основные положения:

1. Приоритет защиты критической информационной инфраструктуры и сотрудничества в сфере кибербезопасности, определяемое планом CIP.

2. Обеспечение ИБ на основе совместной деятельности общества и государства, строящегося на соотнесении уровня предпринимаемых мер и угроз безопасности информации при расширении инструментов защиты.

3. Укрепление ИБ в ОГВ строится на единообразной и безопасной сетевой инфраструктуре федеральной администрации.

4. Национальный центр киберреагирования (National Cyber Response Centre) оптимизирует оперативное сотрудничество между ОГВ, обеспечивая развитие мер обеспечения ИБ и подходов по реагированию на инциденты.

5. Национальный совет кибербезопасности (National Cyber Security Council) осуществляет координацию, связанную с превентивными инструментами и междисциплинарными подходами к кибербезопасности в государственном и частном секторе, выступая связующим звеном управления на федеральном уровне.

6. Эффективный контроль за киберпреступностью включает в себя комплекс институтов с участием предпринимателей и профильных правоохранительных органов, осуществляющих разработку рекомендаций.

7. На основе Конвенции Совета Европы о киберпреступности ожидается значительный рост глобальной гармонизации в области уголовного права.

8. Намерения ФРГ по развитию исследований в сфере кибербезопасности и защиты объектов критической информационной инфраструктуры, направленные на укрепление технологического суверенитета и экономического потенциала государства.

Обновленная Стратегия кибербезопасности Германии, принятая в 2016 г., определяет своими целями: борьбу с киберпреступностью, повышение осведомленности граждан, защиту критической информационной инфраструктуры, формирование национальных планов реагирования на

инциденты кибербезопасности, международное сотрудничество, институционализацию форм сотрудничества между ОГВ, НИОКР и др. [149].

В рамках имплементации положений Директивы NIS, ФРГ стала одной из первых в ЕС стран, которая внесла существенные изменения в законодательство в сфере обеспечения ИБ. Так, в 2015 г. Германия приняла Акт об информационной безопасности (ITSG), который внес поправки в ряд законов (Акт о телекоммуникациях от 2004 г., Акт об энергетической промышленности от 2005 г., Акт о телекоммуникационных медиа от 2007 г. и др., включая Акт о повышении безопасности ИТ Федерации (BSIG) от 2009 г. – ключевой национальный закон, регулирующий вопросы обеспечения ИБ).

Поправки, принятые в рамках Акта об информационной безопасности, заложили фундамент реформам в области обеспечения безопасности критической информационной инфраструктуры. Так, Актом были заложены рамочные основы систем классификации, таксономии и категорирования объектов критической информационной инфраструктуры – введена система требований к операторам объектов критической информационной инфраструктуры, порядок их взаимодействия и отчетности перед регуляторными органами, сроки и задачи разработки внутренней документации и др. [150; 151].

Что касается вопросов защиты ПД в ФРГ, стоит отметить, что Федеральный закон Германии «О защите данных» (BDSG 2018) от 25 мая 2018 г. вступил в силу одновременно с GDPR и регулирует защиту данных в государственном и частном секторах, как и прежний BDSG 2003 г., в т.ч., имплементируя положения GDPR и Директивы 2016/680 [152]. В Германии, как и в США, предусмотрена уголовная и административная ответственность за киберпреступления. Согласно ч. 4 ст. 303 УК ФРГ за компьютерный саботаж, который повлиял на снабжение населения жизненно важными услугами, предусматривает наказание в виде лишения свободы на срок до 10 лет. Согласно ст. 14 закона Act on the Federal Office for Information Technology (BSIG) предусмотрен штраф в размере до 100 тыс. евро, при этом административное правонарушение может быть совершено как умышленно, так и по неосторожности [153; 154].

Организационная структура СОИБ ФРГ строится вокруг Федерального управления по ИБ (BSI), которое является ключевым регуляторным органом государства, уполномоченным в сфере обеспечения ИБ на национальном уровне. Органом, подконтрольным Федеральному Министерству внутренних дел, строительства и общественных отношений (BMI), является BSI, в полномочия которого входит защита критической информационной инфраструктуры и защита данных. BMI формирует политику и план действий в сфере обеспечения ИБ, а главной задачей Министерства является обеспечение ИБ на правительственном уровне. Основные регуляторные органы ФРГ в сфере обеспечения ИБ представлены в таблице 1.8.

Таблица 1.8 – Основные регуляторные органы ФРГ в сфере обеспечения ИБ [составлено на основе [155-158]]

Орган	Основные функции, связанные с обеспечением ИБ
1	2
Федеральное Министерство внутренних дел, строительства и общественных отношений (BMI)	1. Осуществление надзорных функции за отраслью. 2. Формулировка общей стратегии кибербезопасности. 3. Оценка рисков от внедрения ИТ систем. 4. Разработка критериев, методов и испытательных средств для оценки степени защищенности национальных коммуникационных систем. 5. Проверка степени защищенности информационных систем и выдача соответствующих сертификатов. 6. Выдача разрешений на внедрение информационных систем, относящихся к критической информационной инфраструктуре.
Национальный центр кибербезопасности (National Cyber Defence Centre/Nationales CyberAbwehrzentrum, NCAZ)	1. Координация деятельности по реагированию на инциденты ИБ между правительством и частным сектором. 2. Профилактика и раннее предупреждение кибератак, направленное на защиту данных и государственных информационных систем.
Федеральное управление по информационной безопасности (BSI)	1. Обеспечение безопасности онлайн-коммуникаций. 2. Сертификацией продуктов ИБ и аккредитация лабораторий по тестированию решений в области обеспечения ИБ. 3. Контрольно-надзорная деятельность за выполнением мер обеспечения ИБ. 4. Защита критической информационной инфраструктуры. 5. Регулирование криптографической защиты данных. 6. Организация информационного обмена с негосударственными организациями, включая малый и средний бизнес.
Федеральный уполномоченный по защите данных и свободе информации (BfDI)	Выполнение функции омбудсмена в области свободы информации и защиты данных.
Национальный совет по кибербезопасности (National Cyber Security Council)	1. Активизация сотрудничества между организациями государственного и частного сектора. 2. Развитие активного международного сотрудничества для координации деятельности по обеспечению кибербезопасности. 3. Разработка и создание надежных и защищенных ИТ-продуктов. 4. Подготовка и тренинг сотрудников федеральных ОГВ и эффективного использования инструментария ОГВ.

Продолжение таблицы 1.8

1	2
CERT-Bund (Computer Emergency Response Team for federal agencies)	1. Исследование уязвимостей в аппаратных и программных продуктах. 2. Создание и публикация рекомендаций по превентивным мерам. 3. Предложение мер по устранению известных уязвимостей. 4. Поддержание усилий ОГВ по реагированию на инциденты ИБ. 5. Управление национальным ИТ-Ситуационным центром ФРГ.
Федеральная разведывательная служба Германии (BND)	1. Обеспечение внутренней защищенной связи. 2. Составление и реализация специальных ИТ-требований. 3. Разработка технических средств, недоступных в свободной продаже. 4. Формирование и поддержка политики безопасной, надежной эксплуатации и поддержки технических систем и процедур.
Центральное управление информационных технологий в секторе безопасности (ZITiS)	1. Разработка и тестирование стратегии, технических решений и инструментов и координация совместных проектов для органов безопасности. 2. Оказание компьютерной помощи другим правительственным учреждениям, в частности, в сферах: – цифровой криминалистики; – телекоммуникационного мониторинга; – криптографии и анализа больших данных; – технические вопросах по борьбе с киберпреступностью.
Федеральное министерство транспорта и цифровой инфраструктуры (BMWI)	Координация взаимодействия с бизнесом, реализация совместных инфраструктурных проектов на базе цифровых технологий, разработка и реализация пилотных проектов и тестирование в нише беспилотного транспорта и в других областях.
Альянс за кибербезопасность (Alliance for Cyber Security)	Сбор всесторонней базы данных, а также поддержка обмена знаниями и опытом.

Национальный совет по кибербезопасности отвечает за стратегические вопросы ИБ. BfDI, в свою очередь является надзорным органом по защите данных. BMWI – центральный регулятор в области цифровой экономики в ФРГ.

Альянс за кибербезопасность – созданная BSI совместно с Федеральной ассоциацией ИТ и новых средств коммуникации (BITKOM) организация, осуществляет содействие в реализации широких политических задач по упрочению СОИБ Германии за счет повышения киберустойчивости государства.

Об уровне осознания проблематики рассматриваемых вопросов в ФРГ говорит также то, что в 2017 г. вооруженные силы Германии создали киберкомандование (Cyber and Information Space Command, CIS), численность которого, согласно разработанному ВС ФРГ плану, должна составить 14,5 тыс. сотрудников, из которых 1,5 тыс. гражданских лиц. Указанные факты, наряду с тем, что в 2017 г. правительство ФРГ рассматривало возможность внесения изменений в Конституцию с целью нанесения ответных ударов по хакерам, говорит об наднациональном характере исследуемых вопросов.

На основе проведенного анализа можно сделать вывод, что в вопросах ИБ подходы США существенно отличается от подходов ЕС, по следующим основным причинам:

1. Приоритетным вопросом для США считается обеспечение технической защиты информации (защиты от взломов, хакерских атак), а враждебные действия против критической информационной инфраструктуры рассматриваются в США прежде всего как проблема информационной войны.

2. Для США, как и для ЕС, существенным аспектом является защита ПД, интеллектуальной собственности, сведений частного характера. Однако, по мнению автора, система защиты ПД ЕС является много более подконтрольной.

3. Различные подходы к установлению требований к безопасности критической информационной инфраструктуры характеризуются разветвленной структурой ведомств в США с делегированием в рамках риск-ориентированного подхода надзора за выполнением требований законодательства. В некоторых странах ЕС подходы схожи, однако, в ФРГ используется более жесткая и подконтрольная государству система выполнения обязательных требований по обеспечению ИБ [113].

Важным также в рамках настоящего исследования представляется опыт РФ, общегосударственная СОИБ которой строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального, субъектного и ведомственного уровня, а также служб предприятий и организаций. Стоит отметить, что Стратегия развития информационного общества в РФ на 2017-2030 годы определяет одной из ключевых задач – обеспечение безопасной информационной среды [159].

Стратегия национальной безопасности РФ от 2015 г. (утв. Президентом РФ от 31.12.2015 №683) определяет учет угроз безопасности информации в части нарушения устойчивости функционирования объектов критической информационной инфраструктуры РФ как важнейшую задачу [9]. Отметим также, что в 2014 г. была принята Военная доктрина РФ (утв. Президентом РФ 25 декабря 2014 г. №Пр-2976331), в которой выделяется тенденция смещения

военных опасностей и угроз в информационное пространство и внутреннюю сферу РФ [160].

Доктрина ИБ РФ, введенная Указом Президента РФ от 05.12.2016 г. № 646, отражает ключевые современные вызовы в сфере обеспечения ИБ и является важным элементом формирования законодательства в исследуемой сфере [16]. Помимо этого, Конституция РФ закрепляет фундаментальные права и свободы граждан в сфере обеспечения ИБ (право на поиск, получение, передачу, распространение информации, неприкосновенность частной жизни, личную и семейную тайну, тайну переписки) и является фундаментом для формирования нормативного поля РФ [161].

Гражданский кодекс РФ закрепляет нормы, регулирующие отношения в области защиты конфиденциальной информации, а также служебной, коммерческой и др. видов тайн, а также признания электронной подписи средством удостоверения сделки [162]. Кодекс РФ об административных правонарушениях (далее – КоАП) устанавливает ответственность за отказ в предоставлении гражданину информации, за нарушение установленного законом порядка сбора, хранения, использования или распространения ПД, нарушение правил зашиты информации, и др. правонарушения в исследуемой области. Статьи 13.11 и 13.12 КоАП предусматривают взыскания за нарушение правил защиты информации и в соответствии с ними уполномоченные регуляторы (ФСБ и ФСТЭК) проводят проверки ОГВ на предмет соответствия требованиям законодательства [163].

Уголовный кодекс РФ (далее – УК) устанавливает ответственность за нарушения в информационном пространстве. В рамках пресечения компьютерных преступлений согласно ст. 274.1 УК РФ за неправомерное воздействие на критическую информационную инфраструктуру РФ предусмотрено наказание от пяти до десяти лет. Глава 28 УК РФ регулирует отношения, связанные с неправомерным доступом к информации, созданием, использованием и распространением вредоносного ПО, нарушением правил эксплуатации средств хранения, обработки или передачи информации.

В свою очередь, статьи 159.3, 159.6 УК РФ определяют информацию в качестве орудия преступления в рамках совершения мошенничества с использованием платежной карты или путем обработки компьютерной информации. Неправомерный доступ к компьютерной информации предусматривает наказания за нарушения в сфере защиты и обработки ПД и регулируется статьями 137, 140 и 272 УК РФ [164].

Фундамент правового регулировании отношений в сфере обеспечения ИБ закладывается следующими основополагающим Федеральными законами РФ: «О безопасности» от 28.12.2010 г. № 390-ФЗ, «О государственной тайне» от 21.07.1993 г. № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ, «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ, «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ, «О связи» от 07.07.2003 г. № 126-ФЗ, «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 г. № 187-ФЗ и др. [165-171] (Приложение Г).

С целью анализа организационной структуры СОИБ РФ важным представляется рассмотрение иерархии государственных структур (Приложение Д). Правительство РФ координирует деятельность федеральных органов исполнительной власти (далее – ФОИВ) по выполнению первоочередных задач в сфере обеспечения ИБ, регулирует и совершенствует деятельность государственной СОИБ, формирует в установленном порядке статьи федерального бюджета в целях обеспечения ИБ и реализации федеральных целевых программ в указанной области, а также утверждает федеральные целевые программы по обеспечению безопасности информационного общества.

Ключевыми органами, осуществляющими регуляторное, контрольное и надзорное обеспечение государственной СОИБ РФ являются ФСБ и ФСТЭК со своими управлениями по территориальным округам. ФСТЭК РФ организует деятельность государственной СОИБ, осуществляет межотраслевую координацию и функциональное регулирование деятельности в сфере обеспечения ИБ, а также государственный контроль в исследуемой сфере.

Минобороны РФ, ФСБ, Министерство внутренних дел РФ (МВД), Служба внешней разведки РФ (СВР), Федеральная служба охраны РФ (ФСО), Центральный банк РФ, координируют, организуют, обеспечивают и контролируют в пределах своих полномочий деятельность в сфере обеспечения ИБ в соответствующих сферах и подведомственных организациях. Контролирующими и правоохранительными органами федерального уровня, обеспечивающими соблюдение нормативно-правовых норм, являются: Генеральная прокуратура, Конституционный и Верховный Суд. Другие ФОИВ в пределах своей компетенций организуют, обеспечивают и контролируют деятельность в сфере обеспечения ИБ в своих подведомственных организациях [250].

Органы исполнительной власти субъектов РФ и органы местного самоуправления являются следующим уровнем организационной структуры СОИБ РФ, взаимодействующим с ФОИВ по вопросам исполнения законодательства, решений Президента и Правительства РФ и реализации федеральных программ в сфере обеспечения ИБ. Органами местного самоуправления совместно с органами исполнительной власти субъектов РФ осуществляются мероприятия по привлечению граждан и организаций к оказанию содействия в вопросах обеспечения ИБ. На уровне областей разрабатывается и реализуется соответствующая законодательная база. Правительство областей разрабатывает и принимает муниципальные программы в рассматриваемой сфере.

Органы местного самоуправления отвечают за соблюдение законодательства РФ. Органы судебной власти и прокуратуры субъектов РФ осуществляют правосудие по делам о преступлениях, связанных с информационной сферой. В структуре органов исполнительной власти субъектов РФ созданы специальные службы и комиссии, деятельность которых направлена на организацию процессов информатизации, а также разработку НПА регионального уровня [172]. Резюмируя анализ организационной структуры СОИБ РФ, важно систематизировать полномочия основных регуляторов в сфере обеспечения ИБ (таблица 1.9).

Таблица 1.9 – Основные регуляторные органы РФ в сфере обеспечения ИБ и их функции [составлено автором на основе [173-178]]

Орган	Основные функции, связанные с обеспечением ИБ
1	2
Совет безопасности РФ (Совбез)	1. Рассмотрение вопросов, касающихся обеспечения безопасности личности, общества и государства, предотвращения внутренних и внешних угроз, международное сотрудничество в области обеспечения безопасности. 2. Анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности о соблюдении прав и свобод человека и гражданина 3. Разработка и уточнение стратегии национальной безопасности, иных концептуальных и доктринальных документов, критериев и показателей обеспечения национальной безопасности. 4. Осуществление стратегического планирования в области обеспечения безопасности; 5. Рассмотрение проектов законов и НПА по вопросам, отнесенным к сведению Совбеза; 6. Подготовка проектов НПА Президента РФ по вопросам обеспечения безопасности 7. Организация научных исследований по вопросам, отнесенным к ведению Совбеза.
Федеральная служба безопасности (ФСБ)	1. Обеспечение защиты сведений, составляющих государственную тайну, и противодействия иностранным техническим разведкам. 2. Формирование и реализация государственной и научно–технической политики в сфере обеспечения ИБ. 3. Обеспечение организации и функционирования криптографической и инженерно-технической безопасности информационно–телекоммуникационных систем. 4. Установка требований к средствам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. 5. Разработка и утверждение документов, связанных с безопасностью критической информационной инфраструктуры в рамках своих полномочий. 6. Оценка безопасности критической информационной инфраструктуры в рамках своих полномочий. 7. Координация деятельность ФОИВ в рамах своих полномочий. 8. Лицензирование мероприятий в области защиты информации и сертификация средств защиты информации.
Министерство цифрового развития, связи и массовых коммуникаций (Минцифры)	1. Регулирование отрасли электронной подписи. 2. Регулирование вопросов защиты персональных данных. 3. Регулирование вопросов защиты информационных систем (исключая информационные ресурсы критической информационной инфраструктуры). 4. Согласование порядка установки технических средств. 5. Является центром управления инцидентами кибербезопасности на объектах критической информационной инфраструктуры в своей сфере регулирования.
Роскомнадзор (РКН)	1. Осуществление контроля и надзора в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи. 2. Осуществление контроля и надзора за соответствием процессов обработки персональных данных требованиям законодательства. 3. Исполнение функций по организации деятельности радиочастотной службы.
Федеральная служба по техническому и экспортному контролю (ФСТЭК)	1. Организация и проведение лицензирования деятельности по осуществлению мероприятий и (или) оказанию услуг в области технической защиты информации, по созданию средств защиты информации, по разработке и (или) производству средств защиты конфиденциальной информации. 2. Оценка безопасности критической информационной инфраструктуры в рамках своих полномочий. 3. Утверждение документов в области обеспечения безопасности критической информационной инфраструктуры в рамках своих полномочий. 4. Регулирующая и координационная деятельность субъектов критической информационной инфраструктуры 5. Организация и контроль проведения работ по обеспечению ИБ в ОГВ и предприятий. 6. Установка требований к созданию систем безопасности и обеспечения их функционирования. 7. Осуществление государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. 8. Установка требований, отслеживание за обеспечением ИБ субъектов критической информационной инфраструктуры. 9. Лицензирование по осуществлению мероприятий в области защиты информации и сертификации средств защиты информации.

Продолжение таблицы 1.9

1	2
Национальный координационный центр по компьютерным инцидентам (НКЦКИ)	1. Координация мероприятий по реагированию на компьютерные инциденты и непосредственное участие в таких мероприятиях. 2. Организация и осуществление обмена информацией о компьютерных инцидентах. 3. Участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак. 4. Осуществление методического обеспечения деятельности субъектов критической информационной инфраструктуры по вопросам предупреждения компьютерных атак. 5. Осуществление сбора, хранения и анализа информации о компьютерных инцидентах и атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению, реагированию и ликвидации их последствий. 6. Определение необходимых для организации взаимодействия форматов представления информации о компьютерных инцидентах в государственную систему обнаружения и предупреждения компьютерных атак. 7. Определение состава технических параметров компьютерного инцидента.
Центральный Банк (ЦБ)	1. Согласование требований по обеспечению безопасности объектов критической информационной инфраструктуры для своей сферы регулирования. 2. Управление координационным центром ИБ (ФинЦентом) для своей сферы регулирования. 3. Выпуск стандартов, НПА в сфере обеспечения ИБ. 4. Координация деятельности в сфере обеспечения ИБ в своей сфере регулирования.

Кроме того, в состав государственной СОИБ входит совокупность систем и организаций, обеспечивающих ее функционирование, в том числе:

– система научного и нормативного обеспечения работ в сфере обеспечения ИБ;

– система лицензирования деятельности в сфере обеспечения ИБ;

– организации, осуществляющие разработку и производство средств ИБ, а также оказывающие услуги в области обеспечения ИБ;

– система обязательного подтверждения соответствия средств ИБ, процессов их производства, хранения, перевозки, реализации и утилизации требованиям законодательства;

– система подготовки и повышения квалификации в сфере обеспечения ИБ;

– единая информационно-аналитическая система обеспечения деятельности государственной СОИБ и др.

Важно также отметить весомую роль частных вендоров и интеграторов и вносимого экспертным сообществом вклада в сотрудничество с ОГВ и корпорациями по совершенствованию нормативной и методической базы по обеспечению ИБ в РФ [70; 179].

По результатам проведенного анализа можно выделить две основные модели регулирования области обеспечения безопасности критической

информационной инфраструктуры в зависимости от предмета: «объектную» (РФ, Германия и др.) и «субъектно-деятельностную» (США, Китай, Япония и др.) (таблица 1.10).

Таблица 1.10 – Модели регулирования сферы защиты критической информационной инфраструктуры [составлено автором на основе [121]]

Модель	Особенности	Преимущества	Недостатки
Субъектно-деятельностная	– регулирование, направленное на деятельность субъектов критической информационной инфраструктуры; – разрозненность нормативно-правового регулирования; – построение терминологического аппарата от определения жизненно-важных услуг (сервисов); – гибкость в вопросах категорирования, риск-ориентированный подход; – наличие множества регуляторов в разных сферах критической информационной инфраструктуры.	– гибкость выбора требований; – увеличение самостоятельности субъектов; – риск-ориентированный подход.	– недостаточно структурированная; – недостаточно прозрачная; – риск низкого уровня ИБ при недостаточной заинтересованности руководства организации.
Объектная	– регулирование, направленное непосредственно на объекты критической информационной инфраструктуры; – наличие иерархически стройной системы регулирования; – терминологический аппарат, построенный от определения критической информационной инфраструктуры и ее объектов; – четкие критерии категорирования с формированием «пороговых значений»; – точное и явное определение обязанностей субъектов критической информационной инфраструктуры; – наличие ограниченного количества уполномоченных органов с четко-определенной компетенцией.	– упорядочивание гражданского оборота; – упрощение задачи для регуляторов по контролю и надзору за субъектами.	– недостаточная гибкость в части адаптации требований для конкретного объекта; – риск низкого уровня ИБ при фокусировке мер и средств исключительно на выполнение требований НПА (подмена «реальной» ИБ «бумажной»).

Объектная модель позволяет упорядочить гражданский оборот (четкость понимания собственником объекта своей категории и обязанностей) и упростить задачу ОГВ по контролю и надзору за субъектами. Однако, недостатком указанной модели является низкий уровень гибкости в части адаптации требований для конкретного объекта. Ключевым недостатком «объектного»

метода можно назвать распространенность подхода к вопросам ИБ, когда безопасность обеспечивается только с одной целью – закрыть вопрос соответствия требованиям законодательства. Такой подход имеет ряд недостатков и такие СОИБ далеки от эффективности.

Субъектно-деятельностная модель регулирования, в свою очередь, является более гибкой. Например, в ней объект может принадлежать определенному лицу, но не использоваться им, следовательно, ущерб объекту не будет для него существенным (здесь имеет значение хозяйственная деятельность субъекта и риски от компьютерного инцидента приносящие ущерб такой деятельности). Указанный подход предусматривает увеличение самостоятельности субъектов и предполагает риск-ориентированный подход (принятие решения о соразмерности предпринимаемых мер и средств существующим киберугрозам в каждом конкретном случае). Однако, указанная модель является менее структурированной и недостаточно прозрачной.

С целью углубления исследования подходов к построению общегосударственных СОИБ автором исследован глобальный индекс кибербезопасности, Global Cybersecurity Index (далее – GCI), определяющий уровень ИБ государств. Индекс GCI помогает государствам определять уровень СОИБ и направления в сфере обеспечения ИБ, в которых необходимы улучшения, а также стимулирует их принимать меры по укреплению ИБ, повышая таким образом общемировой уровень ИБ. На основании собранной информации в Индексе выявляются практические методы, которые могут внедрить государства и которые соответствуют их национальным условиям. Также GCI способствует распространению передового опыта и формированию глобальной культуры кибербезопасности. Определение весовых коэффициентов показателей, субпоказателей и микропоказателей, содержащиеся в GCI, разработаны Группой экспертов по определению весовых коэффициентов Международного союза электросвязи (МСЭ). В GCI входит 5 блоков мер:

1. Правовые (оценка правовых институтов и программ в сфере обеспечения ИБ).

2. Технические (оценка технических возможностей в сфере обеспечения ИБ).

3. Организационные (оценка наличия и возможностей институтов координации политики и стратегий развития кибербезопасности на государственном уровне).

4. Развитие потенциала (наличие научно-исследовательских, образовательных программ, сертифицированных специалистов и госучреждений, способствующих развитию потенциала в сфере обеспечения ИБ).

5. Сотрудничество (наличие партнерств, механизмов сотрудничества и систем обмена информацией в сфере обеспечения ИБ).

С целью анализа развития СОИБ исследованных государств целесообразно согласно индексу GCI проследить динамику рейтинга кибербезопасности США, РФ и ФРГ (рисунок 1.12).

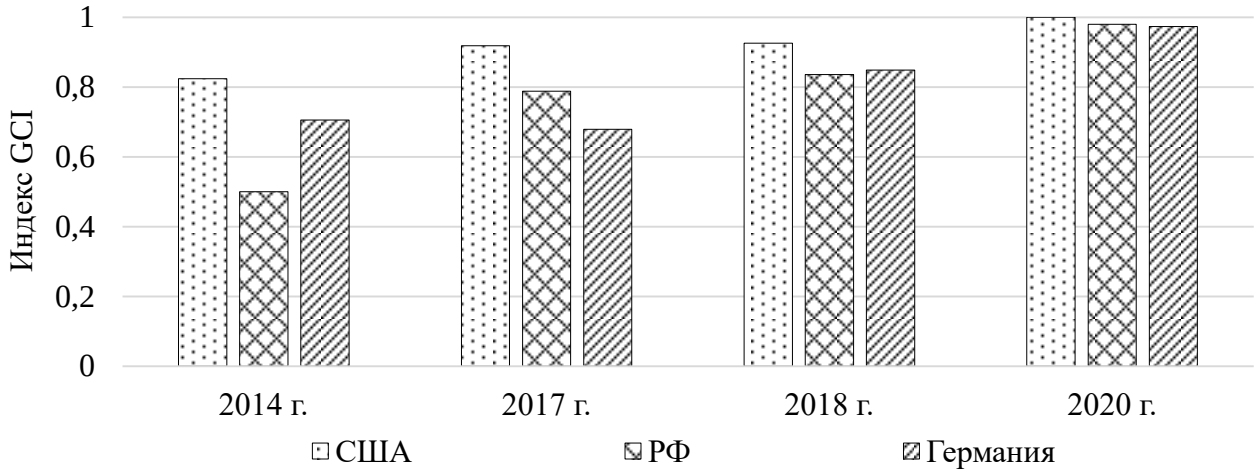

Рисунок 1.12 – Рейтинг кибербезопасности США, РФ и ФРГ, согласно индексу GCI (2014-2020 гг.) [составлено автором на основе [180-182; 230]]

Высокий уровень индекса наряду с растущей динамикой в исследуемых государствах говорит об актуальности проведенного анализа и релевантности подходов к совершенствованию СОИБ. Так, в 2017 г. в тройку наиболее развитых, с точки зрения ИБ, стран попали: 1 место – Сингапур, 2 – США, 3 – Франция. Стоит также отметить, что число стран, имеющих законодательство,

регламентирующее ответственность за киберпреступления, возросло с 79% – в 2017 г. до 91% – в 2018 г. Наиболее примечательным является тот факт, что согласно опубликованным данным, в 2020 г. РФ вновь обогнала ФРГ, вплотную приблизилась к США и заняла 5 место в общемировом рейтинге, что говорит об общепризнанности высокого уровня к обеспечению ИБ в России.

По результатам проведенного исследования, ключевое отличие западного от российского подхода к формированию и развитию общегосударственной СОИБ можно представить на примере США, чей подход заключается в выстраивании риск-ориентированной модели обеспечения ИБ с возложением основных решений по управлению рисками на собственников и субъектов критической информационной инфраструктуры. При этом уполномоченные ОГВ обеспечивают указанные субъекты информацией об угрозах безопасности, стандартах управления рисками и других, способствующих совершенствованию обеспечения ИБ практиках.

В свою очередь, в РФ управление рисками ИБ при построении общегосударственной СОИБ заключается, главным образом, в процедуре категорирования объектов критической информационной инфраструктуры, оставляя управление рисками субъектов в ведении государства и не учитывая возможности гибкой вариативной реализации требований субъектами. В результате, можно отметить, что на общегосударственном уровне, РФ и ФРГ больше следует системному подходу, а США – процессному.

По мнению автора, на ранних этапах зрелости системы правового регулирования оптимальным является именно объектный подход с установлением четких критериев категорирования и явным нормативно закрепленным определением категорий объектов критической информационной инфраструктуры. Данная модель позволяет обеспечить единообразие в указанной сфере и снижает степень неопределенности, связанной с принятием мер обеспечения ИБ на усмотрение субъектов критической информационной инфраструктуры. Также необходимо отметить, что расширение полномочий ОГВ по самостоятельному определению способов исполнения требований ИБ вне

четких критериев представляет собой коррупциогенный фактор и подобное расширение полномочий в сторону – «на усмотрение» субъекта – может привести к игнорированию государственных интересов и низкому уровню защищенности объектов критической информационной инфраструктуры (субъекты имеют возможность по разным причинам не принять эффективные меры по защите ключевых активов).

В свою очередь, подход РФ и ФРГ, в части установления точных критериев и пороговых значений для объектов критической информационной инфраструктуры и дифференциации пороговых значений при отнесении объектов к разным категориям значимости (объектная модель), характерная для российского подхода, представляется оптимальным решением в указанной области, т.к. только через установление четких критериев к определению категорий объектов и субъектов критической информационной инфраструктуры можно добиться конкретного результата – обеспечения высокого уровня ИБ в ОГВ в условиях отсутствия значительных ресурсов (как кадровых так и финансовых), необходимых для альтернативной модели.

Подводя итог, наиболее эффективным, по мнению автора, при построении общегосударственной СОИБ является комбинированный (комплексный) подход, при котором объектная модель может дополняться риск-ориентированным подходом с четко определенными методологиями определения угроз, уязвимостей, а также оценки и управления рисками.

Выводы к главе 1

1. На основе обобщения положений теории информационной безопасности определено, что обеспечение информационной безопасности является сложным,

многоаспектным и многоуровневым процессом, наиболее эффективное обеспечение которого в органах государственной власти должно строиться на комплексном подходе, включающем системную и процессную составляющие. Анализ основных научных направлений теории обеспечения информационной безопасности позволил раскрыть ее сущность и сделать вывод о целесообразности применения комплексного подхода в органах государственной власти по трем аспектам ее совершенствования: организационному, правовому и техническому, направленным на обеспечение ее свойств, а именно, конфиденциальности, целостности, доступности и др.

2. На основе выявления особенностей процесса обеспечения информационной безопасности дана уточненная трактовка понятия «информационная безопасность» в органах государственной власти, в рамках которой предложено интерпретировать данное понятие как защищенность информационных активов органа от любых случайных или преднамеренных воздействий, результатом которых может явиться нанесение ущерба любым свойствам информации и (или) средствам ее обработки, обеспечивающим удовлетворение информационных потребностей граждан, органов государственной власти и других субъектов информационных отношений за счет внедрения мер, средств и процессов защиты информации, достаточных для нейтрализации существующих угроз безопасности информации в условиях непрерывного совершенствования методов и способов их реализации.

3. Анализ существующих подходов к определению сущности информационной безопасности и процесса ее обеспечения позволил уточнить содержание понятия «информационный актив» в органах государственной власти, под которым предложено понимать информацию и (или) средство ее обработки, определенные и управляемые как единое целое; с реквизитами, позволяющими их идентифицировать; имеющие ценность для органов государственной власти и находящиеся в их распоряжении; представленные на любом материальном носителе или в его виде в пригодной форме для выполнения присущих им задач;

необходимые для реализации социальных, политических, экономических и других функций и полномочий.

4. Определено, что современная система публичного управления неотъемлемо связана с информационным обеспечением и должна непрерывно и поступательно двигаться в сторону автоматизации, а затем информатизации и, в конечном счете, цифровизации циркулирующих в ней процессов, в соответствии с ростом уровня зрелости общегосударственных подходов. Определено, что ключевым элементом информационного обеспечения органов публичного управления современного государства является электронное правительство.

5. Исследование системного подхода к обеспечению информационной безопасности в органах государственной власти позволило в рамках общей системы выделить основные ее составляющие, а именно, систему менеджмента информационной безопасности и систему информационной безопасности, сгруппировать основные процессы и обеспечивающие их взаимосвязи. Определена целесообразность использования комплексного подхода как оптимального для органов государственной власти, т.к. он учитывает жесткую иерархию исполнения и гибкую структуру процессов, детально распределенных между ответственными за обеспечение информационной безопасности подразделениями и сотрудниками.

6. На основе обобщения теоретико-методических положений совершенствования системы обеспечения информационной безопасности в органах государственной власти разработана модель процессов системы обеспечения информационной безопасности, которая представляет собой связь основных процессов подсистем.

7. На основе выявленных недостатков реализации типовых подходов к обеспечению информационной безопасности в органах государственной власти и путей их оптимизации сделан вывод о том, что крайне важную роль в настоящее время занимает анализ и непрерывный мониторинг состояния системы обеспечения информационной безопасности с учетом адаптации передовых методик и «лучших практик» к производственной деятельности.

8. Исследование зарубежного опыта функционирования систем обеспечения информационной безопасности США, Европейского Союза, Германии и России позволило установить две основные модели регулирования ключевого направления исследуемой сферы, – области обеспечения безопасности критической информационной инфраструктуры в зависимости от предмета: объектную (характерную для России и Германии) и субъектно-деятельностную (характерную для США, Китая, Японии и др.). Выявлено и обосновано, что для Донецкой Народной Республики наиболее эффективна объектная модель по причинам: формирования законодательства, регулирующего исследуемую сферу, по аналогии с российским; необходимости разработки прозрачных и подконтрольных подходов к обеспечению информационной безопасности в органах государственной власти, а также наличия финансовых ограничений, минимизирующих возможность инвестирования в инфокоммуникационную сферу.

Основные результаты главы опубликованы в научных трудах автора [1; 2; 14; 43; 103-106; 110-112; 157; 172; 179].

ГЛАВА 2. АНАЛИЗ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

2.1. Анализ состояния информационного обеспечения системы публичного управления в Донецкой Народной Республике

Информационное обеспечение системы публичного управления на современном этапе играет одну из определяющих ролей в формировании механизмов устойчивого развития государства, задавая темпы экономического роста и социальной удовлетворенности граждан. В настоящее время значительная доля государств находится в стадии комплексного совершенствования подходов к информационному обеспечению системы публичного управления, важность которых давно признана на общемировом уровне одним из определяющих факторов ее развития.

Государственные ИС в информационном обществе являются ключевыми элементами информационного обеспечения системы публичного управления, что обуславливает важность анализа аспектов их функционирования. Необходимо отметить, что ОГВ и ведомства Донецкой Народной Республики (далее – ДНР) в целях оптимизации их деятельности работают над созданием и совершенствованием информационных систем, представленных в таблица 2.1.

Стоит отметить, что несмотря на функционирование данных информационных систем, отсутствие организационных, правовых и технических возможностей по обмену данными между ними; процессов и результатов проверок на соответствие качеству и безопасности; а также единого подхода к

контролю за сферой их функционирования обуславливает острую необходимость комплексных реформ организационного и правового характера в данной сфере.

Таблица 2.1 – Ключевые информационные системы ОГВ и ведомств ДНР [составлено автором на основе [191; 193; 235-242]]

ОГВ, организации	Системы	Основные задачи
Министерство связи ДНР, ГУП ДНР «Астелит»	ИС сопровождения бумажного документооборота	Обеспечение внутреннего электронного документооборота с интегрированной электронной подписью и возможностью взаимодействия с подведомственными предприятиями
Министерство связи ДНР, ГУП ДНР «Почта Донбасса»	ИС удостоверяющего центра	Обеспечение выдачи сертификатов ключей проверки электронной подписи физическим и юридическим лицам на базе инфраструктуры ГУП ДНР «Почта Донбасса»
Министерство связи ДНР, ГУП ДНР «Астелит», Правительство ДНР	Информационная система контроля НПА и поручений	Оптимизация функций контроля процессов разработки и принятия НПА и исполнения ОГВ поручений, выданных Правительством ДНР
Министерство связи ДНР, Министерство здравоохранения ДНР, ГУП ДНР «Астелит»	ИС обработки вызовов скорой медицинской помощи	Оптимизация процессов приема и обработки вызовов, поступающих в Единую оперативную диспетчерскую Республиканского Центра экстренной медицинской помощи и медицины катастроф ДНР
Министерство информации ДНР	ИС в сфере средств массовой информации	Обеспечение сбора, хранения, учета, поиска, сведений о СМИ, обмен информацией между Министерством информации ДНР и СМИ для принятия мер по ограничению доступа к информации, распространяемой с нарушением требований законодательства
Министерство юстиции ДНР	ИС нормативных правовых актов	Обработка, хранение и предоставление доступа к текстам НПА ДНР и связанных с ними документов
	Единая ИС нотариата	Оптимизация процессов сбора, обработки и хранения сведений о нотариальной деятельности, обеспечение информационного взаимодействия между нотариусами ДНР
Министерство внутренних дел ДНР	Информационно-поисковая система «Полис»	Обеспечение сбора, хранения, учета, поиска, сведений о преступлениях или происшествиях, связанных со сферой полномочий МВД
Министерство экономического развития ДНР	Единая ИС в сфере закупок	Оптимизация процессов осуществления закупок товаров, работ и услуг за бюджетные средства, а также обнародование информации об осуществляемых закупках
Центральный Республиканский Банк ДНР	Система дистанционного банковского обслуживания «ЦРБ онлайн»	Осуществление переводов денежных средств на счета и карты клиентов ЦРБ, оплата налогов, сборов и иных платежей, являющихся источниками формирования бюджетной системы ДНР
	Система дистанционного банковского обслуживания «Клиент-Банк»	Осуществление банковских платежей, получение информации о движениях средств на счете, прием электронных расчетных документов
Министерство финансов ДНР	ИС «Лицензионный реестр»	Обеспечение сбора, хранения, учета, поиска, сведений о выданных лицензиях, формирование, ведение и систематизация данных лицензионных реестров и единого лицензионного реестра ДНР
Министерство доходов и сборов ДНР	ИС «Личный кабинет плательщика»	Обеспечение приема, обработки, передачи информации от субъектов хозяйствования ДНР с целью обеспечения обмена налоговой и таможенной информацией

В настоящее время в ДНР имеет место преимущественно фрагментарные подходы к разработке и внедрению государственных ИС, в рамках которого ОГВ закупают или разрабатывают собственное программное обеспечение (далее – ПО) за счет средств Республиканского бюджета, ориентированное на нужды ведомства, внедряющего данную технологию, что способствует возникновению дополнительных расходов на ПО и оборудование, а также проблем с доработкой ИС, их дальнейшей интеграцией и масштабированием.

Создание ИС в ОГВ в настоящее время происходит в отрыве от изменений в их функциональной деятельности, что приводит к возникновению множества исполнителей при отсутствии планов, учета стандартов и зрелых подходов к обеспечению ИБ. В результате возникает разнородность механизмов, технологий и процедур их внедрения, отсутствие эффективного подхода к развитию информационного обеспечения системы публичного управления и другие сложности, касающиеся отсутствия централизации и стандартизации подходов к рассматриваемым вопросам, что требует всестороннего внимания ответственных ОГВ на предмет пересмотра существующих подходов.

Переходя к вопросам обеспечения безопасности государственных ИС, следует отметить, что требования в данной области, а, следовательно, и уровень доверия, охватывают все слои и элементы данных систем и на каждом из уровней содержат свои решения. К примеру, на уровне данных в государственных ИС должно быть четко определено, какие из них доступны, каким субъектам взаимодействия и на какой конкретный промежуток времени данный доступ предоставляется, а на пользовательском уровне важно учитывать вопросы антикоррупционной безопасности и устранение влияния человеческого фактора при предоставлении доступов и прав сотрудникам ОГВ [87].

При разрешении проблем, возникающих в процессе реализации функций информационного обеспечения ОГВ, особое значение приобретает четкое определение сведений, циркулирующих между участниками, вовлеченными в процесс электронного взаимодействия, а также категорий значимости/уровней/классов защищенности, обрабатывающих данные сведения

систем. Например, до настоящего времени в ДНР не приняты законы, регулирующие защиту коммерческой тайны, не определены требования к защите государственных ИС, состав и содержание мер по обеспечению безопасности ПД в ИС, а также не приняты многие подзаконные НПА, необходимые для нормализации регулирования исследуемой сферы.

Необходимо также учесть, что большинство технологий существующих ИС в ОГВ ДНР строятся на проприетарном программном и аппаратном обеспечении, принадлежащем западным поставщикам (Oracle, VMware, HP, IBM и др.). Поэтому угрозы импортозависимости, могут в том числе повлиять и на экономическую безопасность государства, т. к. права обладателя лицензии проприетарного ПО включают ряд ограничений: невозможность обратной разработки, одновременной работы с системой нескольких пользователей, распространение тестов её рабочих характеристик и др. Помимо этого, существует риск отзыва правообладателем лицензий на использование ПО, прекращения его технической поддержки или обновления, что негативно скажется на процессах информационной деятельности ОГВ.

Более того, проприетарные лицензии могут предусматривать возможность доступа организацией правообладателем к информационным компонентам системы и сбора данных без ведома правообладателя. Так, к примеру, действующее «Заявление о конфиденциальности» компании Microsoft предусматривает указанные возможности [247]. Информация может собираться в интересах иностранных правительственных организаций, что актуально и для ДНР с учетом всех сложных военно-политических условий ее существования.

Указанные риски неприменимы для государственных информационных систем, содержащих массивы наиболее чувствительной информации, охраняемой в соответствии с действующим законодательством, и их устранение на современном этапе является важной задачей для обеспечения надежности и непрерывности выполнения ОГВ своих функций и полномочий. Напротив, свободно-распространяемое ПО лишено всех перечисленных категорий угроз безопасности информации, что делает его в условиях отсутствия отечественных

аналогов наиболее предпочтительным с точки зрения преодоления импортозависимости и обеспечения безопасности государственных ИС.

В свою очередь, общемировая тенденция роста сервисов, разработанных с использованием открытого исходного кода (свободно распространяемого ПО), влечет как массу преимуществ (в т.ч. в виде экономии средств), так и способствует возникновению некоторых угроз безопасности информации ввиду рисков недостаточного доверия к поставщикам. Однако, по мнению автора, данные риски ИБ можно принять, в том числе по причине того, что в ряде случаев поставщики проприетарного ПО так или иначе используют свободно распространяемые репозитории. Поэтому, вопрос стоит в основном в том, будут ли ОГВ работать с данным ПО через поставщиков или формировать свой кадровый потенциал, инициируя тем самым всестороннее комплексное развитие отрасли ИТ.

Таким образом, в сложных экономических условиях существования ДНР важность развития ИС, построенных на использовании свободно распространяемого ПО, по мнению автора, можно назвать одним из важнейших факторов эффективного развития процесса информатизации ОГВ.

Переходя к вопросам защиты конституционных прав граждан, важно отметить, что существенной является роль защиты ПД в государственных ИС. Системы, содержащие ПД, подпадают под категории защищенности, к которым в большинстве стран законодательно предъявляются высокие требования по обеспечению ИБ, т.к. базы данных указанных систем содержат существенные массивы структурированной информации о гражданах.

Однако, в нормативном правом поле ДНР отсутствует множество подзаконных НПА, регулирующих безопасность ИС, содержащих ПД, ввиду чего уровень их защищенности не определен как для владельцев, так и для регуляторов. Поэтому в рамках развития информационного обеспечения ОГВ, важно учесть необходимость надежной защиты ПД граждан, достигаемую в том числе за счет:

– максимально приемлемой синхронизации нормативного поля ДНР и РФ в исследуемой сфере;

– разработки требований сбора и распространения только необходимой для взаимодействия информации о пользователях и механизмов их контроля;

– учета возможности внедрения правил автоматического применения настроек ограничений использования своих данных пользователем (к примеру, их ограниченное использование для конкретных целей);

– нормативного определения ограничения времени, в течение которого организации могут сохранять ПД, а также обеспечения возможности пользователям корректировке и удаления данной информации;

– принятия требований к обеспечению приватности, минимизирующих возможность утечки ПД и позволяющих снизить риски, связанные с передачей данных и связыванием результатов идентификации пользователей среди различных систем, предотвращая возможность создания целостного цифрового профиля гражданина;

– создания и развития организационно-технических методов борьбы с мошенничеством в рамках формирования моделей возможных схем мошенничества, определения характерных признаков данных схем и создания автоматизированных механизмов их выявления.

С учетом вышеуказанной проблематики важнейшей целью развития информационного обеспечения ОГВ ДНР на настоящем этапе можно назвать внедрение централизованного электронного взаимодействия ОГВ друг с другом, а затем между органами, гражданами и бизнесом. Данная цель, является не столько технической, сколько организационной, т. к. строится не только и не столько на переводе функций ОГВ в электронный вид, сколько на системном изменении сложнейшей последовательности взаимоувязанных административных процессов, обеспечивающих данные функции.

Система информационного обеспечения ОГВ призвана обеспечивать реализацию и защиту прав граждан на доступ к информации о деятельности органов в целях достижения необходимого уровня открытости осуществления

общественного контроля за деятельностью государства. На современном этапе, наиболее эффективным инструментом достижения задачи открытости государства, является создание электронного правительства (далее – ЭП), позволяющего осуществлять предоставление государственных услуг в электронном виде, а также:

– ввести межведомственный электронный документооборот, сокращающий бюрократические проволочки и ускоряющий принятие решений;

– переводить в электронную форму взаимодействие ОГВ с гражданами и бизнесом по принципу «одного окна»;

– приближать процессы государственного управления к гражданам;

– повышать прозрачность работы ОГВ.

Переходя к сущности ЭП, и связанных с ней процессов, важно отметить общемировые тенденции, которые в настоящее время включают: возросшее значение обмена знаниями и механизмов коммуникации; трансформацию государственных услуг и их интеграцию; углубление и повсеместное распространение организационных структур. В свою очередь, подходы к формированию электронного правительства (далее – ЭП) в ДНР находятся на начальном этапе своего формирования. Функциональные области электронного правительства и их состояние в ДНР представлены в таблица 2.2.

Таблица 2.2 – Функциональные области электронного правительства и их состояние в ДНР [составлено автором на основе [232, с. 26]]

Область	Сущность	Общемировые тенденции	Состояние в ДНР
1	2	3	4
Электронное управление (E-governance)	Взаимодействие между общественными, неправительственными организациями, корпорациями, гражданами и др. заинтересованными сторонами, в рамках координации внутренних и внешних ресурсов для достижения правительственных целей	– развитие процессов менеджмента знаниями в условиях роста значимости координации и сотрудничества; – развитие технологий, способствующих совместной работе с учетом роста бизнес-процессов, передаваемых на аутсорсинг; развитие электронной коммерции.	Отсутствие единых систем Головного удостоверяющего центра, межведомственного электронного взаимодействия, и иных систем ЭП не позволяют осуществлять юридически значимое электронное взаимодействие ОГВ

Продолжение таблицы 2.2

1	2	3	4
Электронная демократия (E-democracy)	Форма демократии, характеризующаяся структурами, процессами и методами, в которых используются ИТ для увеличения прозрачности, демократического принятия решений, включенности и участия граждан	– новые формы сетевой демократии (онлайн-голосование и др.); – гибридная демократия (способствующая облегчению и интеграции различных управленческих форм и механизмов); – упрощение и интеграция процессов управления.	Информатизация демократических форм и процессов взаимодействия с ОГВ на настоящем этапе не наделена должным уровнем внимания на государственном уровне
Электронная администрация (E-administration)	Состоит из административных и эксплуатационных процессов, связанных с использованием информационных технологий и является тесно связанной с электронным менеджментом (E-management), строящемся на использовании ИТ для улучшения государственных управленческих процессов	– рост интегрированных систем и сервис-ориентированных архитектур; – увеличение гибкости организационных структур и графика работы органов публичного управления; – рост глубины и случаев перепроектирования (реинжиниринга) бизнес-процессов ОГВ; – менеджмент знаний становится все более важной функцией в условиях постоянных изменений и роста объемов информации.	Системный подход к информатизации государственных управленческих процессов находится на начальной стадии формирования. Правовая, организационная и техническая поддержка не отлажена должным образом
Электронные услуги (E-services)	Информационные, коммуникационные и транзакционные услуги, оказываемые в различных сферах общественной деятельности (здравоохранение, образование и др.), предоставляемые гражданам и другим целевым аудиториям с использованием ИТ	– рост систем с использованием сквозных технологий; – расширение участников цепочек предоставления услуг; – рост бесшовных интеграций, систем с высокой доступностью, открытых данных, «умных городов»; – рост влияния потребностей граждан и бизнеса на услуги; – интеграция и фрагментация сервисов.	ОГВ предпринимают усилия по автоматизации процессов предоставления государственных услуг, однако отсутствие единого подхода на государственном уровне способствует возникновению фрагментарности подходов

Эффективное внедрение рассмотренных функциональных областей ЭП позволяет достигнуть широчайшего спектра преимуществ в работе ОГВ – от минимизации рисков возникновения коррупции до оптимизации качества процессов и уровня прозрачности их работы. ЭП позволяет достигать не только более эффективного и менее затратного администрирования, но и кардинально менять систему взаимоотношений между государством и гражданами, способствуя тем самым повышению уровня демократии и ответственности власти

перед народом. Несмотря на это, состояние указанных областей в ДНР не до конца соответствуют общемировым тенденциям.

Проблема кадрового дефицита ДНР в отрасли ИТ и сфере обеспечения ИБ в сложившихся экономических и военно-политических условиях требует приоритетного внимания, т. к. формирование системы эффективного информационного обеспечения ОГВ требует высокого уровня профессиональных навыков у государственных служащих и сотрудников организаций, обслуживающих государственные ИС.

В условиях отсутствия централизованного согласованного видения проблем и задач в сфере информационного обеспечения ОГВ подходы к формированию и развитию кадров, при низком уровне их востребованности, порождают массу негативных последствий, сопровождающихся оттоком специалистов как из сферы государственного управления, так и за пределы государства. Поэтому особую важность на настоящем этапе приобретают системные реформы в сфере образования, связанные с повышением качества процессов обучения, что, главным образом, необходимо осуществлять через тесное взаимодействие с ОГВ, уполномоченными в сфере формирования и развития информационного обеспечения, которые, в свою очередь, должны принимать участие в формировании профессиональных стандартов, определении концептуальных основ развития образовательных компетенций, стажировке, повышении квалификации обучающихся и государственных служащих, а также других процессах, требующих переосмысления на настоящем этапе.

В существующих условиях с целью поддержки кадрового обеспечения ОГВ в отрасли ИТ и сфере обеспечения ИБ, представляется необходимым предусмотреть:

– подготовку и проведение научно-исследовательских работ в области специального, высшего профессионального и дополнительного профессионального образования, учитывая специфику и требования, относящиеся к целям и задачам формирования и развития информационного обеспечения ОГВ;

– разработку соответствующих узконаправленных учебных курсов по организационному, правовому и техническому обеспечению процессов, относящихся к целям и задачам формирования и развития информационного обеспечения ОГВ;

– повышение квалификации государственных служащих;

– популяризацию «лучших практик», относящихся к целям и задачам формирования и развития информационного обеспечения ОГВ, включая проведение различных конференций, форумов и открытых уроков;

– вовлечение ведущих экспертных и научных профильных организаций в тесное сотрудничество с ОГВ по указанным вопросам.

Вышеуказанные положения должны реализовываться через формирование государственных концепций и программ, развитие законодательства, преобразование институтов публичной власти, субсидирование важнейших для государства проектов в отрасли ИТ и иных необходимых для развития современного государства комплексных реформ.

С учетом назревшей необходимости формирования и развития ЭП в ДНР целесообразно проанализировать состояние существующих инфраструктурных ресурсов, необходимых для осуществления данных процессов. В информационно-аналитическом обеспечении, краеугольным элементом является информационно-телекоммуникационная инфраструктура, Индекс развития которой (Telecommunication Infrastructure Index, TII) является одним из трех составных элементов Индекса развития электронного правительства (E-Government Development Index, EGDI), определяемого Департаментом экономического и социального развития ООН [243]. Поэтому в рамках настоящего анализа целесообразно определить состояние и динамику развития данного Индекса и его компонентов в ДНР (рисунок 2.1).

Из рисунка видно, что телекоммуникационная инфраструктура ДНР, являющаяся проводником ЭП, обеспечивающим доступность услуг и сервисов, развивается интенсивно. Положительная динамика развития

телекоммуникационной инфраструктуры сопровождается приростом как числа пользователей сети интернет, так и числа абонентов мобильной связи.

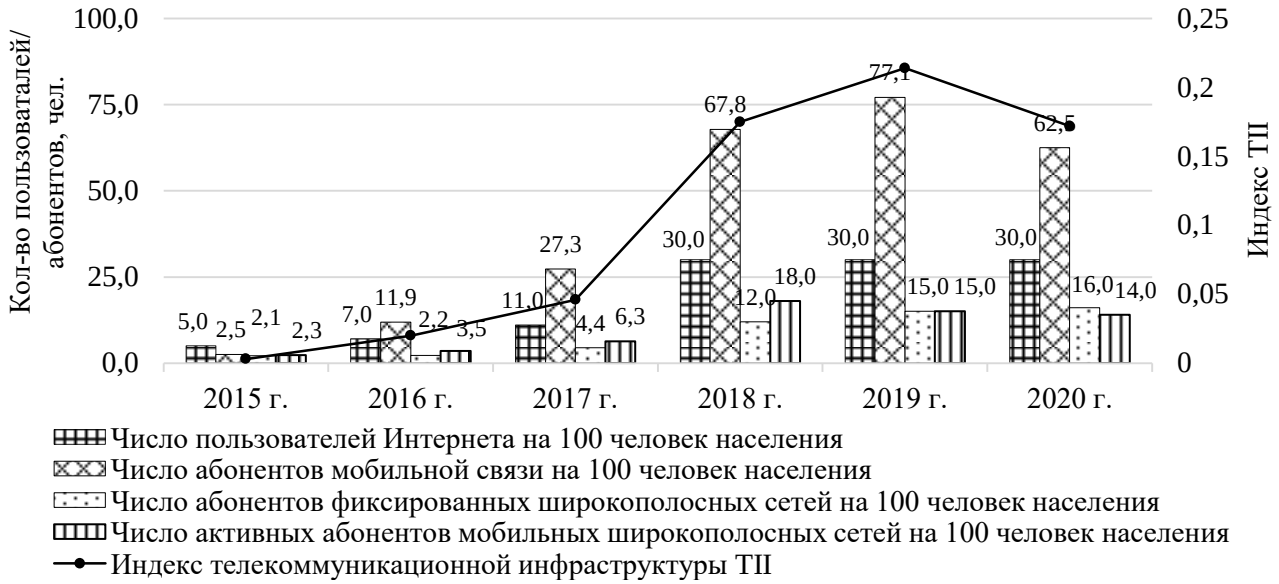

Рисунок 2.1 – Динамика развития Индекса телекоммуникационной инфраструктуры TII и его составляющих в ДНР, 2015-2020 гг. [составлено автором на основе [243; 249]]

Проведенный анализ развития Индекса TII указывает на то, что на настоящем этапе уровень готовности информационно-телекоммуникационной инфраструктуры ДНР позволяет говорить о наличии технической возможности поступательного перехода на предоставление государственных услуг в электронном виде. Однако, вопросы наличия технических мощностей для создания единого государственного центра обработки данных, необходимого для формирования ЭП, требуют отдельного исследования.

Важно подчеркнуть, что на современном этапе для ОГВ ДНР основополагающим этапом является разработка и внедрение ИС, обеспечивающих сопровождение внутреннего электронного документооборота и законодательное урегулирование их создания и функционирования. Важнейшими функциями данных систем, в частности, должно стать делопроизводство и хранение электронных документов.

Вместе с тем, необходимо учитывать, что внедрение цифровых технологий неизбежно инициирует возникновение рисков ИБ для государственных ИС, входящих в ЭП. Снижение до принимаемого уровня данных рисков в условиях увеличения набора и повышения значимости электронных услуг, требует создания единой общегосударственной СОИБ. Данной задаче в РФ служит Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, созданная для обеспечения централизованного системного управления безопасностью наиболее важных для функционирования информационного пространства государства объектов.

Также стоит отметить, что в рамках ЭП функционируют государственные ИС, являющиеся значимыми объектами критической информационной инфраструктуры и подпадающие под действие 187-ФЗ РФ. Поэтому с целью гармонизации с РФ правовых, организационных и технических подходов к обеспечению ИБ в ОГВ важно создать единую общегосударственную систему управления ИБ, которая позволит выстраивать эффективное взаимодействие в области защиты критической информационной инфраструктуры ДНР [171]. В таблице 2.3 обобщена структура существующих проблем развития информационного обеспечения системы публичного управления ДНР.

Ключевым элементом стратегического планирования при развитии информационного обеспечения функций ОГВ при осуществлении своих полномочий является кадровый ресурс, качество подготовки которого прямо зависит от уровня востребованности работодателями. Решение проблем на начальном этапе видится через стандартизацию процессов и требований к государственным ИС. В условиях значительного ограничения в финансовых, кадровых и иных ресурсах с учетом важности обеспечения ИБ и необходимости совершенствовать подходы к формированию ЭП для ДНР особую роль приобретает принцип единства (централизации и унификации процессов и элементов).

Таблица 2.3 – Ключевые проблемы развития информационного обеспечения системы публичного управления ДНР [составлено автором на основе [185-187]]

Сфера	Проблемы	Направления решения	Ожидаемые результаты
1	2	3	4
Законодательство	1. Отсутствие эффективного контроля за принятием подзаконных НПА. 2. Смешанная модель законодательства (перенятая из РФ, Украины, СССР) приводит к длительным по времени процессам согласования и внесения изменений в проекты НПА, увеличению количества бюрократических процессов и правовым коллизиям. 3. Наличие массивного пласта не разработанных и не принятых законов и подзаконных НПА, необходимых для эффективного развития сферы информатизации. 4. Отсутствие четкого определения уполномоченных органов, нераспределенные функции и полномочия.	1. Формирование и утверждение согласованной на общегосударственном уровне дорожной карты по разработке и принятию законов и подзаконных НПА в отрасли ИТ с определением ответственных и установлением четких сроков этапов ее реализации. 2. Формирование эффективного механизма контроля за разработкой, согласованием и принятием законов и подзаконных актов. 3. Разработка и принятие недостающих законов и НПА в указанной сфере.	1. Урегулирование системы правового сопровождения процесса информатизации ОГВ. 2. Обеспечение уполномоченных органов в отрасли ИТ и сфере ИБ достаточными регуляторными инструментами и полномочиями по ее развитию.
Экономика, юридическая, социальная сфера	1. Недостаток источников инвестиций/кредитования. 2. Значительная доля наличного оборота денежных средств находится в «тени». 3. Недостаток достоверной информации о ресурсах государственной инфраструктуры (производственные и торговые площади, земельные участки). 4. Отсутствие единых подходов к информационно-аналитическому обеспечению. 5. Отсутствие единой квалифицированной электронной подписи. 6. Отсутствие необходимых для информационного обеспечения ОГВ реестров и систем.	Урегулирование, разработка и внедрение, комплекса единых государственных ИС, входящих в состав ЭП, в частности: – Единого портала и реестра государственных услуг; – ИС головного удостоверяющего центра; – ИС межведомственного электронного взаимодействия; – ИС идентификации и аутентификации – ИС межведомственного электронного документооборота; – ИС нормативной справочной информации и др.	1. Стимулирование экономического развития отраслей государства. 2. Повышение уровня социального обеспечения и общественного благосостояния. 3. Формирование юридической значимости всех видов правоотношений в электронном виде.
Государственное управление	1. Отсутствие технологической, организационной, и правовой возможности осуществлять автоматизированное межведомственное взаимодействие между ОГВ, бизнесом и гражданами. 2. Наличие недостоверных и искаженных данных в информационных системах ОГВ. 3. Отсутствие централизованных систем приема и предоставления государственных услуг.	1. Поступательная централизация и стандартизация государственных ИС. 2. Урегулирование, разработка и внедрение, в частности: системы обеспечения законодательной деятельности, системы управления информатизацией ОГВ, системы формирования и обработка данных в сфере государственного управления и др.	1. Сокращение искажения информации, централизация данных. 2. Облегчение поиска, получения и обмена информацией между ОГВ. 3. Оптимизация процессов государственного управления.

Продолжение таблицы 2.3

1	2	3	4
Образование	1. Отсутствие квалифицированного кадрового ресурса, а также должного уровня востребованности в данном ресурсе по причине низкого уровня заинтересованности многих уполномоченных регуляторов в способствовании развитию сферы информатизации. 2. Несоответствие уровня подготовки выпускников требованиям работодателей в связи с отсутствием практического опыта работы с современными технологиями.	1. Совершенствование системы взаимодействия ОГВ и учреждений профессионального, общего и дополнительного образования по вопросам кадровой подготовки и научных исследований для целей информатизации. 2. Обновление образовательных программ под нужды информатизации. 3. Создание системы выявления и поддержки одаренных школьников и студентов.	1. Создание эффективной системы подготовки кадров для целей информатизации прямо влияющее на качество процессов информационного обеспечения ОГВ. 2. Повышение конкурентоспособности выпускников на рынке труда.
Здравоохранение	1. Очереди на прием к медицинским специалистам. 2. Заполнение большого количества медицинских форм в бумажном виде. 3. Необходимость защиты потребителей от фальсифицированных, контрафактных, а также, не отвечающих установленных требованиям к качеству лекарственных препаратов.	1. Урегулирование, разработка и внедрение Единой медицинской информационной системы для учреждений оказания медицинской помощи. 2. Урегулирование, разработка и внедрение Единой информационной системы мониторинга движения лекарственных препаратов.	1. Повышение оперативности и качества оказания медицинской помощи. 2. Оптимизация процессов поставок, сокращение оборота фальсифицированных и контрафактных лекарственных препаратов.
Сфера информационно-коммуникационных технологий	1. Недостаток возможностей по модернизации эксплуатируемых аппаратных мощностей серверных помещений ОГВ ввиду сложности в покрытии необходимых для этого бюджетных запросов. 2. Недостаток финансовых, технологических и кадровых возможностей обустройства центров обработки данных для каждого ОГВ в соответствии с требованиями применяемых стандартов (качества, безопасности, отказоустойчивости и др.).	1. Обеспечение финансовых, организационных, правовых и технологических ресурсов для запуска единого государственного центра обработки данных. 2. Интеграция имеющихся ключевых государственных информационных систем в единое информационное пространство ОГВ. 3. Создание единых государственных программ формирования электронного правительства.	1. Сокращение стоимости создания и поддержки ИТ-инфраструктуры ОГВ. 2. Повышение уровня качества государственных ИС. 3. Развитие технологических и кадровых ресурсов государства. 4. Оптимизация процессов государственного управления.
Сфера обеспечения информационной безопасности	1. Отсутствие необходимых НПА делает невозможным контрольно-надзорную деятельность за сферой обеспечения ИБ ОГВ, а также сокращает спрос, а следовательно, и качество кадрового ресурса. 2. Отсутствие необходимых требований безопасности к ключевым государственным информационным активам и контрольно-надзорной деятельности за их исполнением снижает управляемость и общегосударственный уровень обеспечения ИБ.	1. Создание контрольно-надзорного органа, уполномоченного в областях, связанных с обеспечением ИБ в ОГВ. 2. Разработка и принятие необходимых законов и подзаконных актов в сфере обеспечения ИБ. 3. Унификация и централизация информационных систем ОГВ. 4. Перевод государственных информационных систем на единые стандарты.	1. Повышение уровня общегосударственной безопасности. 2. Повышение непрерывности и качества процессов государственного управления. 3. Повышение доверия к государству у граждан, бизнеса и др. субъектов.

Данный принцип позволяет создать условия для формирования единого информационного пространства ОГВ и включает следующие ключевые положения:

– разработку единых стандартов и требований к основным элементам информационно-технического обеспечения, позволяющих обеспечить согласованное развитие и совместимость программно-технических решений;

– создание единых общегосударственных систем ЭП, разрабатываемых в целях обеспечения единства политики государственной регистрации и учета, предоставления оперативного доступа к целостной, актуальной, достоверной и непротиворечивой информации об основных объектах, формах, способах и результатах государственного управления и ее совместного использования на межведомственном уровне;

– формирование законодательной, подзаконной и методической базы для указанных систем и процессов;

– создание единой системы повышения квалификации государственных служащих, включая определение требований к их квалификации, развитие инфраструктуры центров по их подготовке и повышению квалификации на базе высших учебных заведений ДНР, профессиональное обучение и сертификацию ответственных за разработку и внедрение информационных ОГВ, а также создание системы мотивации, поощрения и регламентации процессов использования государственными служащими информационных технологий.

В настоящее время все развитые страны понимают целесообразность формирования единых общегосударственных подходов к формированию ЭП. Конвергенция информационных сред государственных институтов и частных коммерческих организаций уже сейчас происходит в большинстве государств и будет только развиваться. Данная тенденция, в первую очередь, основана на их единстве (целостности, унификации, однородности). В условиях масштабных экономических ограничений существования ДНР именно централизация и стандартизация позволяет существенно снизить издержки на дублирование информационных ресурсов, ИТ-инфраструктуры и повысить качество

информационных сред ОГВ. Поэтому как внутренние, так и внешние ИС ОГВ должны быть легко адаптируемыми к изменению задач и структуры органов и проектироваться для решения задач системы публичного управления в целом.

Централизованное представление данных и системных компонент позволяет выстроить более качественное управление безопасностью и интероперабельностью государственных ИС. Наличие платформы единого информационного пространства, включающей государственные ИС и формирующей централизованный механизм управления развитием ЭП, позволит организовать распространение «лучших практик», архитектурных решений, функциональных и информационных возможностей.

Также использование единых подходов позволит создать гибкие, расширяемые шаблоны, которые могут быть использованы для обмена данными между всеми участниками и поставки данных в единое информационное пространство обмена. Поэтому основным организационно-техническим направлением оптимизации существующей системы информационного обеспечения ОГВ ДНР можно назвать интеграцию государственных ИС и процессов информационного обеспечения ОГВ в единое информационное пространство.

Здесь необходимо учитывать, что процесс формирования единого информационного пространства ОГВ требует определения технологической политики, включающей следующие аспекты создания и эксплуатации ИС ОГВ:

1. Критерии выбора технологий ИБ в государственных ИС.

2. Возможность использования недоверенных технологий для создания систем и сервисов государственных ИС.

3. Требования к разработчикам и поставщикам средств защиты информации по обеспечению их интеграции в единое информационное пространство.

4. Требования к разработчикам государственных ИС по обеспечению безопасности при разработке прикладного ПО и использованию эффективных централизованных механизмов ИБ.

5. Порядок проверки государственных ИС на соответствие требованиям ИБ на различных этапах жизненного цикла ИС.

6. Порядок использования централизованных механизмов ИБ в государственных ИС.

Важно также учитывать основные аспекты, связанные с информационными средами ОГВ, которые должны быть учтены проектировщиками, организаторами, операторами и другими субъектам формирования и функционирования единого информационного пространства ОГВ ДНР:

1. Разные типы и степени развития информационных сред ОГВ пересекаются и объединяются в естественным образом интегрируемой среде.

2. Разный масштаб информационных сред ОГВ, понимаемый как степень охвата субъектов и/или типов частных сред, а также объем данных.

3. Информационные среды ОГВ могут менять свой масштаб во времени, поэтому, в общем случае, информационная среда обладает свойством многоаспектного масштабирования.

4. Необходимость определения центрального субъекта единого информационного пространства, формирующего ее границы.

5. Информационные среды ОГВ изменчивы, при этом различаются изменения указанных сред за счет целенаправленной деятельности центрального субъекта и за счет действий иных субъектов среды.

6. Централизация информационных сред способствует возникновению некоторых рисков ИБ.

В свою очередь, основными направлениями для создания системы управления ИБ в едином информационном пространстве ОГВ можно назвать:

– совершенствование нормативной правовой базы в сфере обеспечения ИБ, обеспечивающее дифференциацию государственных ИС по степени защиты;

– определение ответственного ведомства за процессы обеспечения ИБ, а также правил взаимодействия регуляторов и операторов государственных ИС;

– разработку методической базы, способствующей совершенствованию подходов к оценке состояния СОИБ в ОГВ, процессов управления ИБ, единых метрик ИБ и показателей, основанных на этих метриках;

– разработку технологической политики обеспечения ИБ в рамках систем единого информационного пространства ОГВ ДНР;

– разработку и внедрение набора глобальных сервисов ИБ в рамках единой инфраструктуры ИС ОГВ, включающих в себя: средства мониторинга ИБ, средства контроля защищенности ИС ОГВ, средства защищенного пользовательского доступа, средства анализа и контроля безопасности прикладного ПО и др. средства;

– унификацию процессов, средств и каналов защищенного информационного обмена в рамках создания централизованной системы управления ИБ в ОГВ.

Проведенный анализ позволяет сделать вывод о том, что для формирования ЭП в рамках единого информационного пространства ОГВ ДНР ключевыми являются следующие направления:

– инициация процессов анализа информационных сред ОГВ на предмет определения их технологического состояния с целью повышения уровня конвергентности и интероперабельности;

– формирование концептуальных подходов, государственных программ, дорожных карт, а также требований и иных НПА, способствующих созданию и обеспечению безопасности государственных ИС и развитию ЭП в рамках единого информационного пространства ОГВ ДНР;

– разработка и принятие необходимых для развития ЭП в ДНР законов и подзаконных НПА;

– вовлечение существующих подведомственных Правительству и ОГВ ДНР предприятий с компетенциями, необходимыми для разработки ИС ЭП;

– тесное сотрудничество уполномоченных органов (Минсвязи ДНР, МГБ ДНР и др. ОГВ с Министерством образования и науки ДНР и образовательными

учреждениями ДНР) с целью внедрения реформ, позволяющих формировать и развивать компетенции, необходимые для целей информатизации.

Подводя итог, важно отметить, что электронное правительство, будучи важнейшим элементом информационного общества, является концепцией новой системы управления государством, эффективное внедрение которой, позволяет повысить прозрачность и целеориентированность процессов публичного управления, обеспечивая тем самым устойчивое развитие государства.

Однако, несмотря на все преимущества и назревшую необходимость формирования ЭП в ДНР, накопившиеся проблемы правового и организационного характера создают разнородные сложности, всячески затрудняющие формирование системного подхода к информатизации ОГВ. С переходом процессов ОГВ на инфокоммуникационные платформы неизбежно возникают определенные риски ИБ, которые должны быть оценены и учтены на всех этапах – от проектирования до выведения из эксплуатации государственных ИС. Все это обуславливает особое значение анализа и развития организационных, правовых, технических, методических и иных подходов к обеспечению ИБ.

2.2. Тенденции развития системы обеспечения информационной безопасности в Донецкой Народной Республике

Общегосударственная безопасность не может быть обеспечена без такой ее составляющей как информационная. Согласно докладу Всемирного экономического форума-2020 в Давосе кибербезопасность (кибератаки, кража ПД и др.) названа одной из 5-ти ключевых проблем современности [244]. Также важность обеспечения ИБ в ОГВ на современном этапе подтверждается отчетом одного из ведущих игроков на рынке ИБ-услуг РФ, Positive Technologies от 2021

года, согласно которому, большинство компьютерных атак, по-прежнему, совершается в отношении государственных учреждений (около 19% от всех атак, направленных на организации) [245]. Указанные факты, с учетом чувствительности циркулирующих в ОГВ данных, свидетельствуют о необходимости комплексного пересмотра существующих подходов к обеспечению ИБ на общегосударственном уровне. Поэтому от своевременности их осознания зависит качество и скорость развития информационного обеспечения деятельности ОГВ в ДНР.

В то время как в мире создаются государственные программы по обеспечению ИБ, формируются центры и институты, целью которых является совершенствование подходов к ее обеспечению, принимаются концепции и закрепляются нормы на конституционном уровне, в ДНР развитию подходов в указанном направлении не уделяется достаточно внимания, несмотря на наличие различных возможностей по всесторонней оптимизации ситуации на организационном, правовом и техническом уровнях [184].

Количество информационных ресурсов в ДНР постоянно растет наряду с важностью данных, циркулирующих в них. Компьютерные атаки активно проводятся как на открытые, так и на внутренние информационные ресурсы ОГВ. Отсутствуют возможности получения соответствующих статистических данных с конкретизацией произошедших с информационными ресурсами ОГВ ДНР инцидентов, как по причине отсутствия ведения на территории ДНР таковой статистики, так и в рамках невозможности ее запросить по причине нежелания органов делиться конфиденциальными сведениями.

Постоянно совершенствующиеся методы и способы компрометации данных, существующие децентрализованные подходы к обеспечению ИБ в ОГВ всячески усложняют формирование полноценного системного подхода к информационному обеспечению на общегосударственном уровне. А тот факт, что масштаб от последствий произошедших инцидентов ИБ в ОГВ ДНР с учетом трансграничных и геополитических особенностей является внушительным и с существующими подходами будет только расти, не вызывает сомнения.

Как было отмечено, нормативное правовое обеспечение играет ключевую роль в обеспечении формирования и развития государственных ИС. Руководствуясь Концепцией внешней политики ДНР, утвержденной Указом Главы ДНР от 1 марта 2019 года № 56, определяющей в качестве одного из стратегических приоритетов взаимодействие с РФ и закрепляющей стремление к совершенствованию законодательства ДНР путем его гармонизации с законодательством России, целесообразно провести сравнительный анализ основных законов, регулирующих вопросы создания и обеспечения безопасности государственных ИС [234].

В рамках проведенного анализа правового обеспечения выделены и проанализированы ключевые законы ДНР в указанной сфере (Приложение Е), в результате чего, можно выделить в общем виде следующую структуру (рис 2.2).

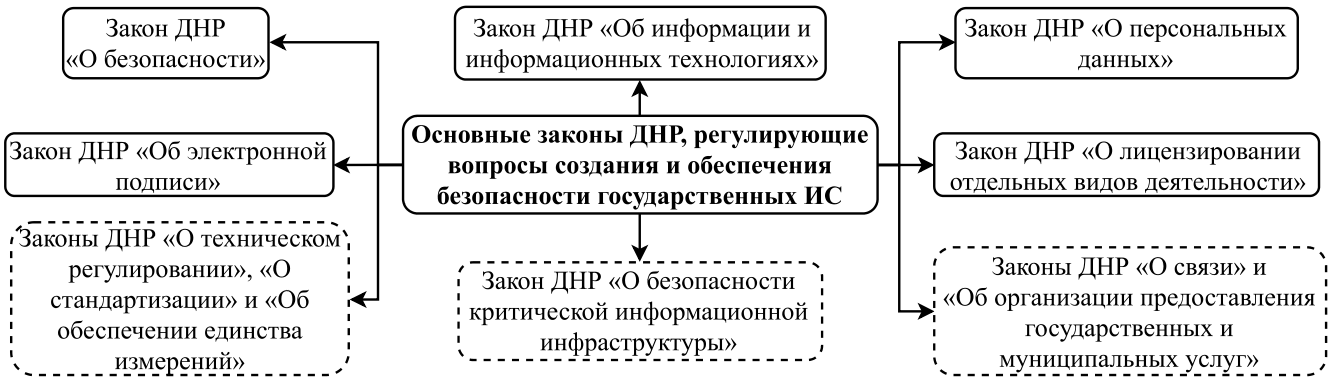

Рисунок 2.2 – Основные Законы ДНР, регулирующие вопросы создания и обеспечения безопасности государственных ИС [составлено автором]

Несмотря на схожесть систем правового регулирования сферы обеспечения ИБ с РФ, в ДНР отсутствуют целые пласты законодательства: в частности, полностью отсутствует регулирование в областях обеспечения безопасности критической информационной инфраструктуры и предоставления государственных и муниципальных услуг в электронном виде. Закон ДНР № 18-IНС от 27.02.2015 «О лицензировании отдельных видов хозяйственной деятельности» не соответствует редакции аналогичного Закона в РФ, т.к. из него

исключены положения, затрагивающие аспекты: технической защиты конфиденциальной информации; разработки и производства средств защиты конфиденциальной информации; разработки, производства и распространения криптографических средств и иные положения, что, с учетом отсутствия иных Законов и НПА по данному направлению, указывает на отсутствие регулирования в области лицензирования в сфере обеспечения ИБ [197].

Также не принят ряд подзаконных НПА для системообразующих в исследуемых сферах Законов ДНР: «Об информации и информационных технологиях» № 71-IНС от 07.08.2015, «Об электронной подписи» № 60-IНС от 19.06.2015, «О персональных данных» № 61-IНС от 19.06.2015, что не дает возможности уполномоченным органам полноценно развивать отрасль ИТ [185-187; 233]. Проведенный анализ позволил определить состояние регулирования указанных сфер через выявление принятых и рекомендуемых к принятию подзаконных НПА к существующим Законам ДНР (рисунок 2.3).

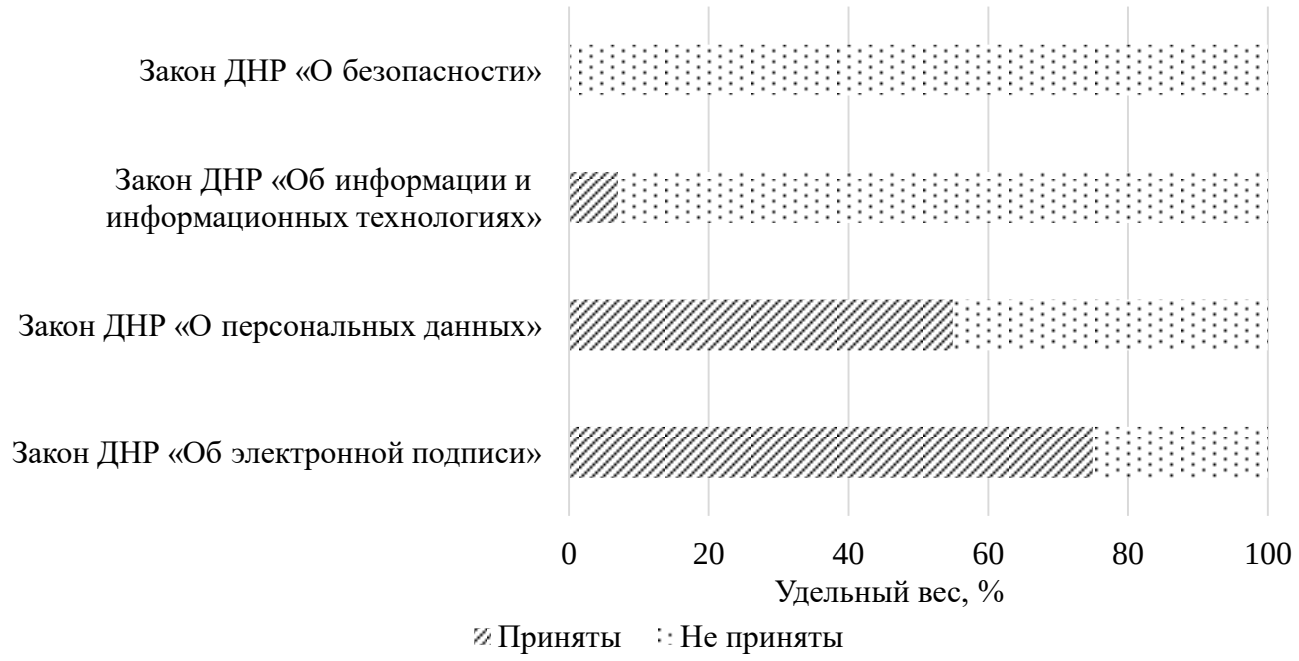

Рисунок 2.3 – Удельный вес подзаконных НПА к Законам ДНР, регулирующим вопросы создания и обеспечения безопасности государственных ИС, 2021 г., % [составлено автором на основе 185-187; 233]

Из рисунка видно, что в настоящее время не разработан ряд подзаконных НПА для ключевых законов, а следовательно, регулирование указанных областей, не может осуществляться эффективно. Стоит также отметить, что во многих законах ДНР отсутствует четкое наименование подзаконного НПА и(или) не определен ОГВ, осуществляющий его разработку и(или) принятие. Помимо этого, не приняты важнейшие законы: «О техническом регулировании», «О коммерческой тайне» и другие необходимые для регулирования исследуемых сфер законы и НПА.

Приведенные факты создают правовые пробелы в законодательстве ДНР в сферах ИБ и ИТ, усложняющие развитие отраслей вследствие отсутствия возможности эффективной реализации соответствующих полномочий. Проведенный анализ нормативного правового поля ДНР показал, что при разработке законодательства ДНР сформировалась проблематика, значительно затрудняющая формирование ЭП, в частности, и развитие отрасли ИТ и сферы обеспечения ИБ, в целом, обусловленная следующими правовыми пробелами и коллизиями (таблица 2.4).

Отметим, что Министерство связи ДНР является профильным ведомством по формированию электронного правительства и осуществляет функции по разработке, реализации государственной политики и нормативному правовому регулированию в областях: электронного взаимодействия ОГВ; защиты прав субъектов ПД; электронной подписи; телекоммуникаций; почтовой и специальной почтовой связи и др. Указанным Министерством разработан ряд законодательных и подзаконных актов, а также реализованы проекты и мероприятия по оптимизации существующего состояния в исследуемой сфере.

В частности, совместно с другими ОГВ осуществлен ряд инициатив по внесению изменений в существующие Законы, разработаны подзаконные НПА, постоянно осуществляется взаимодействие с профильными ведомствами, разрабатываются и внедряются информационные системы и совершенствуется общегосударственная информационно-коммуникационная инфраструктура.

Таблица 2.4 – Ключевые проблемы регулирования ДНР в отрасли ИТ и сфере обеспечения ИБ [составлено автором]

Проблема	Описание	Следствия
В нормативном правовом поле ДНР отсутствует понятие остаточная (сферальная) компетенция	В Законе ДНР «О системе органов исполнительной власти ДНР» отсутствуют нормы, аналогичные нормам, приведенным в Указе Президента РФ «О системе и структуре федеральных органов исполнительной власти», а также действует Закон ДНР «О нормативных правовых актах» (который не имеет аналогов в РФ и не позволяет реализовывать ОГВ сферальную компетенцию)	Невозможность полноценно обеспечить потребности ОГВ в ходе информатизации процессов государственного управления
Проекты НПА подлежат проведению антикоррупционной экспертизы Министерства юстиции ДНР	Результаты антикоррупционной экспертизы обязательны для исполнения республиканскими органами исполнительной власти, однако Министерством юстиции ДНР допускается трактовка норм законов за пределами компетенции, что не позволяет обеспечить гармонизацию законодательства ДНР с законодательством РФ	Наличие коллизий и пробелов в законодательстве, препятствующих, либо полностью останавливающих действие Законов
Отсутствие легальной возможности создания государственных ИС	Действующая редакция Закона ДНР «Об информации и информационных технологиях» не соответствует требованиям Закона ДНР «О нормативных правовых актах» и не содержит необходимых полномочий Правительства ДНР и Министерства связи ДНР, вследствие чего ОГВ пренебрегают требованиями в отрасли ИТ и сфере обеспечения ИБ	Создание угроз безопасности ИС ОГВ, а также дополнительных расходов Республиканского бюджета на создание ИС ОГВ
Неурегулированность вопросов создания головного удостоверяющего центра и использования усиленной квалифицированной электронной подписи	Действующая редакция закона ДНР «Об электронной подписи» не предусматривает однозначно выписанные полномочия Министерства связи на создание головного удостоверяющего центра, помимо этого Правительством ДНР не установлены виды электронных подписей, используемых ОГВ и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой	Отсутствие условий для создания усиленных квалифицированных электронных подписей, а также возможностей использования электронной подписи в рамках межведомственного взаимодействия
Отсутствие легальной возможности эксплуатации государственных ИС без надлежащего оформления прав на использование ее компонентов	Законом ДНР «Об информации и информационных технологиях» определено, что не допускается эксплуатация государственных ИС без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности, однако, в настоящее время, формы, правила и порядки, необходимые для указанного процесса, приведенные в Гражданском Кодексе ДНР Правительством ДНР не утверждены	Отсутствует возможность надлежащего оформления прав интеллектуальной собственности, на использование государственных ИС, разработанных в ДНР
Отсутствие необходимых законов и НПА в сфере обеспечения ИБ, а также системы аттестации ПО и оборудования, используемого ОГВ	Законом ДНР «Об информации и информационных технологиях» определено, что требования о защите информации, содержащейся в государственных ИС, устанавливаются МГБ ДНР, однако разработка данных требований не осуществлена. Неурегулированность сферы обеспечения ИБ делает невозможным разработку, проектирование и создание государственных ИС, а также цифровизацию процессов государственного управления с советующим уровнем обеспечения ИБ.	Создание угроз безопасности ИС ОГВ, отсутствие возможности осуществлять надзорную деятельность в сфере обеспечения ИБ, отсутствие системного подхода к формированию и развитию отрасли ИТ и сферы обеспечения ИБ

Однако, несмотря на ряд осуществленных мероприятий по информатизации ОГВ, сложности, указанные в таблице 2.4, не позволяют сформировать системный подход к развитию исследуемой сферы на общегосударственном уровне.

Переходя к анализу полномочий регуляторов, уполномоченных организаций в сфере обеспечения ИБ, стоит отметить, что ключевым ОГВ здесь является Министерство государственной безопасности ДНР (далее – МГБ), в полномочия которого входит защита государственной тайны, область криптографической защиты информации, лицензирование и сертификация по вопросам обеспечения ИБ и др. (таблица 2.5).

Закон ДНР № 04-IНС от 12.12.2014 «О безопасности» по аналогии с российским, определяет статус Совета Безопасности ДНР. Данный орган является важнейшим в контексте стратегического формирования политики в сфере обеспечения ИБ. Однако, о результатах работы данного органа, после его создания в 2014 г., в открытых источниках информации нет, в результате чего не разработана ни Концепция национальной безопасности, ни Доктрина информационной безопасности ДНР, необходимые для формирования базы для развития законодательных и иных инициатив [187].

Кроме этого, указанными в таблице 2.5 регуляторами не ведется контрольно-надзорная деятельность за обеспечением безопасности критической информационной инфраструктуры, защитой государственных ИС и ИС, содержащих ПД, т.к. не приняты законы и подзаконные НПА, необходимые для осуществления данных процессов, оставляя пробелы и коллизии в законодательстве, создающие неопределенность в работе отрасли ИТ и сферы обеспечения ИБ.

Организационная структура СОИБ ДНР (Приложение Ж) схожа со структурой РФ, однако такие аспекты как: неразработанные подзаконные НПА, неопределенные полномочия ОГВ, указанные в законах и отсутствие стратегических взглядов на исследуемую сферу, свидетельствуют о явной необходимости всестороннего пересмотра существующих подходов.

Таблица 2.5 – Основные регуляторные органы ДНР в сфере обеспечения ИБ и их функции [составлено автором на основе [187-190; 196]]

Орган	Основные функции, связанные с обеспечением ИБ
Совет безопасности	– рассмотрение вопросов, касающихся обеспечения безопасности личности, общества и государства, предотвращения внутренних и внешних угроз, вопросов международного сотрудничества в области обеспечения безопасности; – анализ информации о реализации основных направлений государственной политики в области обеспечения безопасности о соблюдении прав и свобод человека и гражданина; – разработка и уточнение стратегии национальной безопасности, иных концептуальных и доктринальных документов, критериев и показателей обеспечения национальной безопасности; – осуществление стратегического планирования в области обеспечения безопасности; – рассмотрение проектов законов и НПА по вопросам, отнесенным к сведению Совбеза; – подготовка проектов НПА Главы ДНР по вопросам обеспечения безопасности; – организация научных исследований по вопросам, отнесенным к ведению Совбеза.
Министерство государственной безопасности	– обеспечение защиты сведений, составляющих государственную тайну, и противодействия иностранным техническим разведкам; – лицензирование деятельности по разработке и производству средств защиты информации; – лицензирование деятельности по технической защите конфиденциальной информации; – сертификация технических средств защиты информации; – формирование и реализация государственной и научно-технической политики в сфере обеспечения ИБ, в том числе с использованием инженерно-технических и криптографических средств; – обеспечение криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации; – организация разработку и выполнение государственных программ в области защиты государственной тайны.
Министерство связи	Выработка и реализация государственной политики и нормативного правового регулирования в сферах: – ИТ при формировании и развитии цифрового правительства, в том числе электронного взаимодействия ОГВ и органов муниципального управления ДНР; – защиты прав субъектов ПД; – электронной подписи; – телекоммуникаций, в т.ч. радиочастотного ресурса; – специальной почтовой связи; – проектов в отрасли связи.
Министерство информации	– осуществление государственного контроля за соблюдением законодательства о средствах массовой информации, о защите детей от информации, причиняющей вред их здоровью и (или) развитию; – обеспечение защиты интересов ДНР в области авторского права и смежных прав в сфере массовых коммуникаций и средств массовой информации.
Центральный Республиканский Банк	– разработка и издание НПА, регулирующих правила построения систем ИБ и использования средств криптозащиты в банках и финансовых учреждениях, а также при оказании банковских и финансовых услуг; – устанавливает требования по ИБ платежных систем, терминального оборудования и прочих технических и информационных средств, используемых для осуществления банковских и финансовых операций.

Существующие проблемы в сфере обеспечения ИБ не позволяют реализовывать ряд краеугольных государственных проектов по формированию электронного правительства. Главными причинами этому являются отсутствие: имплементированных в законодательстве ДНР положений, распределения полномочий в определенных законодательством областях, а также комплексных подходов к решению накопившихся проблем.

Помимо этого, отсутствие должного уровня правовых и организационных подходов в исследуемых сферах приводит к условиям, когда непрерывная конкретизация в законодательствах всех развитых государств требований к обеспечению прав на: свободу выражения мнения; неприкосновенность частной жизни; личную и семейную тайны; защиту чести и доброго имени; тайну переписки и телефонных переговоров (ст. 22 п. 1, 4, 5; ст. 16 п. 1, 2 Конституции ДНР) остается в неопределенном состоянии при формировании приоритетов государственного регулирования [198].

Поэтому приоритетными направлениями для ДНР на современном этапе можно назвать создание и (или) реформирование уполномоченных структур в сфере обеспечения ИБ, адаптацию и синхронизацию нормативного поля с российским, а также устранение коллизий в уже разработанном законодательстве т. к. нераспределенные полномочия и отсутствие должного уровня регулирования, максимально затрудняют развитие информационного пространства ДНР.

Ядром, вокруг которого должно создаваться единое информационное пространство ОГВ ДНР, являются государственные ИС, обеспечение безопасности которых с учетом наличия во включенных в них важнейших процессов и данных, по мнению автора, можно назвать приоритетом развития общегосударственной СОИБ. Поэтому необходимость формирования эффективных систем безопасности государственных ИС, зрелость которых будет адекватна уровню приемлемых рисков, требует учета факторов, представленных на рисунок 2.4.

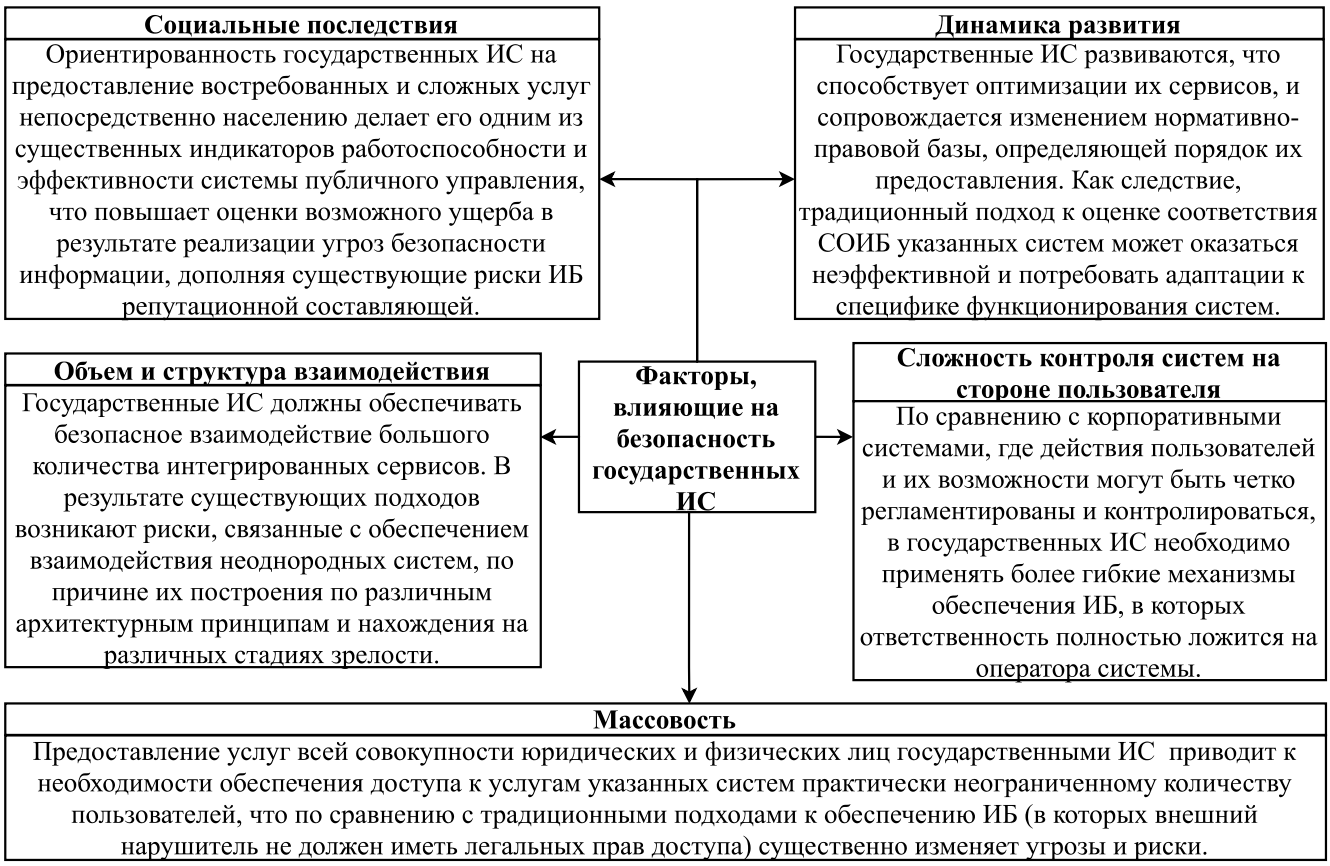

Рисунок 2.4 – Группы факторов, влияющих на безопасность государственных ИС в ДНР [составлено автором]

Оценка приведенных факторов подтверждает, что на современном этапе особую важность проведения анализа технологических угроз безопасности информации, актуальные типы которых для информационных сред ОГВ ДНР, представлены в таблице 2.6.

Одной из ключевых целей потенциального злоумышленника по отношению к государственным ИС является получение контроля над системами на уровне процессов деятельности, т.к. доступ на данном уровне, к примеру, путем раскрытия конфиденциальной информации более эффективен для злоумышленника и опаснее для оператора, чем атака, требующая специфического опыта, знаний и ресурсов (в т.ч. временных и технологических), и, следовательно, данная атака является менее эффективной согласно соотношения «затраты/получаемый результат».

Таблица 2.6 – Некоторые актуальные типы технологических угроз безопасности, свойственные информационным средам ОГВ ДНР и основные методы их устранения [составлено автором]

Типы угроз	Методы устранения и минимизации угроз
1	2
Угрозы, связанные с процессами предоставления доступа и недостаточным уровнем контроля над процессами ИБ	1. Закрепить законодательно административную и уголовную ответственность за нарушения, связанные с обеспечением безопасности государственных ИС, информационных систем ПД и иных ИС ОГВ. 2. Закрепить нормативно требования по безопасности ИС ОГВ, в частности (государственных ИС, ИС персональных данных, а также требования к безопасности значимых объектов критической информационной инфраструктуры). 3. Фиксировать выявленные нарушения (по сообщениям от пользователей, по результатам аудитов СОИБ), учитывать их как основу для вычисления рисков, реагировании и обработке инцидентов ИБ. 4. Обеспечить правовую финансовую, правовую, организационную и техническую возможности создания головного удостоверяющего центра, реализующего выдачу усиленной квалифицированной электронной подписи. 5. Обеспечить операторами государственных ИС возможности интеграции с электронной подписью. 6. Предусмотреть возможность перевода государственных ИС на платформу электронного правительства с единым порталом государственных услуг, в рамках повышения качества контроля за обеспечением ИБ. 7. Разработка и внедрение по аналогии с опытом РФ доверенного плагина единого портала государственных услуг, учитывающего возможность аутентификации с использованием электронной подписи. 8. Формирование качественных риск-ориентированных процессных подходов к управлению ИБ в ОГВ в рамках совершенствования СМИБ с ориентацией на стандарты серии ГОСТ Р ИСО/МЭК 2700х.
Угрозы, связанные с хранением аутентификационных данных	1.Стимулировать использование механизмов усиленной и строгой аутентификации пользователей. 2.Интегрировать механизмы 2-ух факторной аутентификации в государственные ИС. 3.По аналогии с опытом РФ, разработать единую систему идентификации и аутентификации с последующим стимулированием подключения к ней всех государственных ИС. 4.Установить требования по обязательному применению средств усиленной и строгой аутентификации. 5.Улучшить средства мониторинга ИС ОГВ с доступом через сеть интернет с целью обеспечения возможности оповещения пользователей о событиях входа с использованием его учетной записи на незнакомых устройствах.
Угрозы в рамках действующих сессий взаимодействия	1.Внедрить механизм обязательной повторной авторизации при выполнении значимых для безопасности действий. 2.Повышать уровень экспертизы разработчиков в создании защищенного кода. 3.При подключении сторонних систем к ИС ОГВ предусмотреть экспертизу качества подключения.
Угрозы при осуществлении идентификации и аутентификации	Предусмотреть нормативное закрепление, а также контроль за исполнением требований для ИС ОГВ к: – контролю за реализацией организационных и технических мер, усложняющих успешное выполнение фишинга. – периодическому информирование пользователей об угрозах ИБ и мерах противодействия, а также парольные политики, предотвращающие использование простых паролей в ИС ОГВ.

Продолжение таблицы 2.6

1	2
Угрозы, связанные с восстановлением доступа	1. Создать центры обслуживания пользователей государственных ИС, предоставляющих государственные услуги постепенно отказываться от небезопасных схем самостоятельного восстановления забытого пароля. 2. Установить эффективные механизмы применения контрольных вопросов и ответов при самостоятельном восстановлении забытых паролей в ИС ОГВ. 3. Установить требования к процедуре предоставления доступа в государственных ИС.
Угрозы, связанные с неправомерным использованием ПД	1. Разработать и принять подзаконные НПА закона ДНР «Об электронной подписи», осуществлять контроль за ними. 2. Предусмотреть требования к поставщикам услуг и периодические аудиты на соответствие данным требованиям ИБ. 3. В рамках разработки и внедрения Единой системы идентификации и аутентификации должны быть предусмотрены функции, связанные с поддержкой жизненного цикла учетной записи ИС ОГВ: актуализации сведений учетной записи, удаление учетной записи и прекращение обработки ПД по инициативе пользователя.
Угрозы информационной инфраструктуре ОГВ и подключенным к ней системам	1. Непрерывно развивать и совершенствовать базовые сервисы обеспечения ИБ инфраструктуры ИС ОГВ. 2. Предусмотреть организационные и технические меры профилактики и выявления нарушений среди обслуживающего персонала. 3. Разработать общегосударственную методологию управления рисками ИБ в ОГВ, выявить риски ИБ и контролировать мероприятия, позволяющие их купировать или минимизировать.
Угрозы возникновения недекларированных возможностей	1. Разработать процедуру категорирования производителей «по степени доверия», формировать список стратегических технологических поставщиков в ДНР, разработать процедуры сертификации ИС и сервисов согласно ГОСТ Р ИСО/МЭК 15480х, используя в ОГВ, только прошедшие сертификацию и имеющие высокий уровень доверия. 2. Исключение возможности прямого доступа поставщиков услуг к ИС ОГВ. Осуществлять процессы обновления ИС и иные технические меры по обслуживанию исключительно доверенными сотрудниками ОГВ и(или) при их непрерывном контроле. 3. Регулярный аудит ИБ и анализ уязвимостей в государственных ИС в рамках внутренних и внешних проверок. 4. Устранение выявленных уязвимостей, формирование комплексных СОИБ в ОГВ. 5. Принятие требований, связанных с практиками безопасной разработки ПО (SSDLC) для поставщиков услуг.
Угрозы зависимости от правообладателей при развитии, обновлении и(или) поддержки систем	1. Обеспечить финансирование ключевых направлений ИТ в рамках стимулирования процессов импортозамещения. 2. Реализовать гибридное импортозамещение (определение зарубежных продуктов и решений, от которых можно отказаться и их альтернатив, а также выявления существующих компетенций для создания отечественных аналогов. 3. Принять концепции и дорожные карты, учитывающие планы по переходу на свободно распространяемое ПО. 4. Развивать сферу образования в контексте подготовки кадров, владеющих знаниями, необходимыми для целей импортозамещения, а также оптимизация взаимодействия ОГВ, ответственных за отрасль ИТ и сферу ИБ с образовательными учреждениями в рамках формирования ИТ-инкубаторов для студентов, конференций, производственных практик, а также инициация и поддержка научных исследований в исследуемой сфере.

Перечисленные угрозы в совокупности с указанными факторами оказывают существенное влияние на риски безопасности, связанные с функционированием государственных ИС, ИТ-инфраструктур и выбор подходов к их минимизации. В рамках конкретизации влияния указанных угроз и факторов целесообразно выделить существующие в ДНР группы рисков, связанных с различными аспектами создания и функционирования государственных ИС (таблица 2.6).

Таблица 2.7 – Анализ основных групп рисков безопасности, свойственных информационным средам ОГВ ДНР [составлено автором]

Риски	Описание
1	2
Системные риски	
Отсутствие критериев управления рисками ИБ	Процедуры управления рисками ИБ в ИС ОГВ отсутствуют, что не дает возможности сопоставлять реальные уровни защищенности в различных системах. Также отсутствуют утвержденные метрики ИБ и основанные на них показатели, в результате чего объективная оценка уровня ИБ затруднена.
Неоднородность защиты	Государственные ИС имеют собственные автономные СОИБ, построенные по различным требованиям, не согласованным между собой. В результате данные системы защищены неоднородно как в части требований, которые выдвигаются к различным системам, так и в части уровня зрелости при их выполнении.
Формальность реализации требований ИБ	В силу ограниченности ресурсов ОГВ задачи обеспечения ИБ в ИС финансируются по остаточному принципу, что приводит к формальной реализации требований ИБ с переводом нереализованных механизмов на уровень организационных мер. В результате СОИБ данных систем строится в основном на документационном уровне и не функционирует в цикличной парадигме, а проверки защищенности проводятся в лучшем случае по формальному принципу.
Отсутствие синхронизации жизненных циклов отрасли ИТ и сферы обеспечения ИБ	ИС ОГВ подвержены регулярным изменениям, связанным с необходимостью развития функционала и изменениями нормативной базы. При этом отсутствуют процедуры проверки соответствия (аттестации), в результате чего проверки систем, в лучшем, случае производятся либо на начальных стадиях их эксплуатации, либо нерегулярно. В результате жизненные циклы отрасли ИТ и сферы обеспечения ИБ оказываются рассинхронизованными, что ведет к эксплуатации систем без учета требований ИБ.
Операторские риски	Операторы ИС ОГВ способны за редким исключением обеспечивать формальный контроль за эксплуатацией и развитием систем, не имея для этого в штате достаточного количества специалистов. В результате распространена практика, определения организации, осуществляющей работу по эксплуатации и развитию данных систем, что приводит к риску возникновению угроз ИБ связанных с 3й стороной. Сотрудники оператора имеют повышенные привилегии, а область их деятельности далеко не всегда четко определена политикой доступа к информационным ресурсам. Контроль за деятельностью операторов систем ИС ОГВ осуществляется от случая к случаю, в результате чего затруднено выявление инцидентов ИБ, связанных с операторской деятельностью. Также во многих случаях отсутствует описание критериев качества услуг в части ИБ.
Риски, связанные с разработчиками ПО	При разработке ИС ОГВ формируется логика реализации информационных процессов, обеспечивающих поддержку деятельности органов. При этом как требования, так и сами процедуры оценки уровня ИБ на различных стадиях жизненного цикла ИС отсутствуют.

Продолжение таблицы 2.7

1	2
Риски использования нелицензионного ПО	Использование нелицензионного ПО согласно общемировым практикам является нарушением авторских и смежных прав и влечет за собой административную и уголовную ответственность. Также данные риски связаны с разного рода угрозами ИБ, в том числе правовыми и техническими. Отсутствие регулирования авторского права на ряду с внешними военно-политическими факторами, а также отсутствием бюджетных ассигнований на приобретение лицензий максимально усложняют вопросы контроля за обеспечением ИБ.
Нормативно-правовые риски	
Отсутствие законов и НПА Коллизии в законодательстве Неоднозначное применение НПА	Связаны с правовым статусом различных категорий информации в ИС ОГВ, с правомерностью применения ограничений при создании и использовании систем, с ответственностью за нарушения функционирования данных систем и многим другим. В частности, законодательно не определены обязательства и требования по защите: коммерческой и служебной тайны; государственных ИС; информационных систем содержащих ПД; а также ИС, которые являются объектами критической информационной инфраструктуры ДНР.
Технологические риски	
Риски, связанные с уязвимостями на стороне пользователей	В настоящее время уровень защищенности пользователей, взаимодействующих с ИС ОГВ, неоднороден. При этом большинство пользователей не предпринимают действий по обеспечению ИБ, а какие-либо воздействия на них, жесткая регламентация их деятельности со стороны оператора затруднительна.
Риски совместимости	Использование в ИС ОГВ различных разнородных механизмов обеспечения ИБ, не систематизированных и не интегрированных между собой, в ряде случаев, не допускающих интеграцию со средствами защиты иных производителей, создает набор рисков ИБ, связанных с конкретными механизмами и технологиями ее обеспечения, что в ряде случаев приводит к необходимости дублирования средств защиты и увеличивает вероятность ошибочных действий администраторов, а также создает зоны, где средства ИБ конфликтуют между собой, взаимно блокируя действия друг друга.
Риски, связанные со встроенными средствами защиты	Реализация существенных механизмов обеспечения ИБ как встроенных средств прикладного ПО приводит к противоречию между изменчивостью прикладного ПО и необходимости проводить проверки соответствия требованиям ИБ. Кроме того, производители прикладного ПО могут не иметь в составе команды специалистов по ИБ, в результате чего реализация механизмов оказывается некорректной.
Риски импорто-зависимости	Данные риски чреваты возникновением недекларированных возможностей и угроз непрерывности процессов вследствие зависимости от правообладателей при развитии, обновлении и(или) поддержки систем.

Одной из ключевых проблем информатизации, в целом, и сферы обеспечения ИБ, в частности, является непризнанность ДНР, которая усложняет различные аспекты как закупки ИС и средств защиты информации в РФ, так и осуществления иных видов взаимодействия с российскими поставщиками/ вендорами/интеграторами. Учитывая этот факт, а также тренды импортозамещения в ОГВ РФ, импортозависимость ДНР, обусловленная недостатком необходимых компетенций, требует особого внимания со стороны уполномоченных органов.

Важно отметить, что несмотря на наличие массы существенных технологических угроз и рисков ИБ, приоритетность организационных и правовых реформ с учетом их важности для формирования системного подхода на общегосударственном уровне, а также всех сложностей и неопределенностей, связанных с функционированием информационного поля ОГВ ДНР, остается ключевой.

После определения основных проблем и направлений, нуждающихся в оптимизации, важно систематизировать показатели, на базе которых будут вырабатываться предложения по совершенствованию СОИБ в ОГВ и отслеживаться динамика выполнения поставленных задач. Данные критерии, в дальнейшем могут быть имплементированы в государственные программы и (или) иным способом использоваться как инструмент определения состояния показателей общегосударственной СОИБ.

Общемировые «лучшие практики» указывают на то, что СОИБ в ОГВ целесообразно строить на количественном понимании величины рисков, вытекающих из существующих подходов к правовому, организационному, техническому и иным аспектам обеспечения ИБ [72; 101; 201-204]. Поэтому, имея выстраиваемое на прозрачных многоуровневых показателях представление о настоящем состоянии общегосударственной СОИБ, у ОГВ появляется возможность управления зрелостью подходов к ее совершенствованию.

Методика расчета индекса GCI была выбрана как подходящая для настоящего исследования в рамках расчета эффективности общегосударственных подходов ДНР к обеспечению ИБ, т.к. методология ее расчета является признанной на общемировом уровне. Процесс оценки в рамках настоящего исследования состоит из следующих шагов:

1. Отбор экспертов, которыми являются юристы и аналитики, работающие в области информационного обеспечения ОГВ и обладающие знаниями общемировых тенденций и законодательства ДНР в сфере обеспечения ИБ.

2. Предоставление каждому члену группы экспертов материалов, а именно:

– опросных листов с таблицами для определения весовых показателей и оценок;

– руководства с пояснениями к показателям.

3. Каждый эксперт в индивидуальном порядке заполняет электронную таблицу со своими рекомендованными значениями весовых коэффициентов каждого показателя, субпоказателя и микропоказателя и предоставляет данные автору.

4. После присвоения оценок всеми членами группы экспертов, их значения усредняются и сводятся в единую таблицу весовых коэффициентов.

В рамках данного исследования автором привлечены эксперты в количестве 5 человек из Министерства связи ДНР, которые присвоили значения весовым показателям и выставили оценки согласно методике расчета, после чего данные значения были усреднены автором. Переходя к практической части оценки состояния СОИБ ДНР согласно методике GCIv4, стоит обозначить порядок расчета значений, входящих в состав индекса GCI, который основан на иерархической модели вложений, «ветви» которой именуются кластерами («-показателей», «-субпоказателей» и «-микропоказателей»), каждый из которых содержит в себе кластер ниже по уровню.

Вес основных составляющих, показателей, субпоказателей и микропоказателей определяется экспертами согласно иерархической модели вложенности. В каждом кластере экспертами на основании анализа существующих в мире и ДНР трендов, распределяется 10 баллов в пределах весового коэффициента каждого кластера показателей (X_{Π_i}), субпоказателей ($X_{C_{ij}}$) и микропоказателей ($X_{M_{ijz}}$), после чего определяется вес каждой меры (таблица 2.8).

Из таблицы 2.8 видно, что в рамках распределения весового коэффициента, показатель 1 имеет большее значение, поэтому ему присвоен больший вес. Аналогичным образом поступаем и с микропоказателями.

В свою очередь, показатели 1 и 2 содержат только по одному субпоказателю, поэтому им присуждается максимальное значение в 10 баллов. В результате весовой коэффициент позволяет присуждать большее значение

элементу внутри каждого кластера, имеющему большую значимость для государства с точки зрения эксперта [199].

Таблица 2.8 – Пример таблицы с распределением весового коэффициента, вычислением веса кластеров, экспертными оценками и оценками кластера согласно методике расчета GCI [составлено автором]

Кластеры	Весовой коэффициент	Вес	Экспертная оценка	Оценка кластера
1. Показатель 1	6	12	-	8,400
1.1. Субпоказатель 1	10	12	-	8,400
1.1.1. Микропоказатель 1	7	8,4	2	8,400
1.1.2. Микропоказатель 2	3	3,6	0	0,000
2. Показатель 2	4	8	-	4,000
2.1. Субпоказатель 2	10	8	1	4,000

Далее на основании определенных экспертами весовых коэффициентов, согласно формулам, представленным в таблице 2.9, вычисляется вес кластеров.

Таблица 2.9 – Формулы вычисления веса кластеров согласно методике расчета GCI [составлено автором на основе [200]]

Вес кластера	Формула
Показатель	$W_{\Pi_i} = \text{ОС} * X_{\Pi_i} / \sum_{i=1}^{k} X_{\Pi_i}$;
Субпоказатель	$W_{C_{ij}} = X_{C_{ij}} * W_{\Pi_i} / \sum_{j=1}^{l} X_{C_{ij}}$;
Микропоказатель	$W_{M_{ijz}} = X_{M_{ijz}} * W_{C_{ij}} / \sum_{z=1}^{m} X_{M_{ijz}}$,

Условные обозначения:

W_{Π_i} – вес показателей в рамках каждой меры;

$W_{C_{ij}}$ – вес субпоказателей в рамках каждой меры;

$W_{M_{ijz}}$ – вес микропоказателей в рамках каждой меры;

ОС – основная составляющая в рамках каждой меры;

X_{Π_i} – весовой коэффициент кластеров показателей;

$X_{C_{ij}}$ – весовой коэффициент кластеров субпоказателей;

$X_{M_{ijz}}$ – весовой коэффициент кластеров микропоказателей;

k – количество показателей в рамках каждой меры;

l – количество субпоказателей в рамках каждого показателя;

m – количество микропоказателей в рамках каждого субпоказателя;

i – порядковый номер показателей в рамках меры;

j – порядковый номер субпоказателей в рамках i-го показателя;

z – порядковый номер микропоказателей в рамках j-го субпоказателя.

После вычисления веса кластеров согласно 3-х бальной шкале выставляются экспертные оценки: 0 баллов присуждается соответствующим значениям кластеров, если мера отсутствует; 1 – если мера выполняются частично и 2 – если мера выполняются полностью. Формулы вычисления значений оценок кластеров по каждому из 5-ти направлений представлены в таблице 2.10.

Таблица 2.10 – Формулы вычисления оценок кластеров согласно методике расчета GCI [составлено автором на основе [200]]

Оценка кластера	Формула
Микропоказатель	$O_{M_{ijz}} = W_{M_{ijz}} * B_{M_{ijz}}/2;$
Субпоказатель (содержащий микропоказатели)	$O_{C_{ij}} = \sum_{z=1}^{m} O_{M_{ijz}};$
Субпоказатель (без микропоказателей)	$O_{C_{ij}} = W_{C_{ij}} * B_{C_{ij}}/2;$
Показатель	$O_{\Pi_i} = \sum_{j=1}^{l} O_{C_{ij}}$

Условные обозначения:

$O_{M_{ijz}}$ – оценка z-го микропоказателя в рамках j-го субпоказателя;

O_{Π_i} – оценка i-го показателя в рамках меры;

$O_{C_{ij}}$ – оценка j-го субпоказателя в рамках i-го показателя;

$B_{M_{ijz}}$ – оценка меры z-го микропоказателя в рамках j-го субпоказателя;

$B_{C_{ij}}$ – оценка меры j-го субпоказателя без микропоказателей в рамках i-го показателя.

Итоговые значения каждой меры (ПМ, ТМ, ОМ, РП, МС), входящей в индекс GCI, вычисляется как произведение суммы значений, входящих в нее показателей кластеров (O_{Π_i}), на коэффициент значимости меры (M_p) и отношение к основной составляющей (ОС) (таблица 2.11).

Таблица 2.11 – Вычисление итоговых значений мер индекса GCI [составлено автором]

№ меры (p)	Наименование меры	Формула	Основная составляющая	Коэффициент значимости
1	Правовые меры (ПМ)	$O_p = (\sum_{i=1}^{k_p} O_{\Pi_i}) * M_p/\text{ОС}$	ОС = 20	$M_{\text{ПМ}}$ = 0,22
2	Технические меры (ТМ)			$M_{\text{ТМ}}$ = 0,22
3	Организационные меры (ОМ)			$M_{\text{ОМ}}$ = 0,22
4	Развитие потенциала (РП)			$M_{\text{РП}}$ = 0,17
5	Меры в области сотрудничества (МС)			$M_{\text{МС}}$ = 0,17

Условные обозначения:

O_p – оценка p-й меры для индекса GCI;

O_{Π_i} – показатели кластеров, входящих в меру;

k_p – количество показателей кластеров p-ой меры;

M_p – коэффициент значимости p-ой меры.

Как видно из таблицы 2.11, p может принимать значения от 1 до 5. Коэффициент значимости отражает важность меры для итогового значения индекса GCI и определяется экспертами. Основная составляющая является максимальным значением веса каждого кластера и принимается равной 20.

Итоговое значение индекса GCI вычисляется как сумма полученных показателей по каждой мере (правовой, технической, организационной, развитию потенциала и мере в области сотрудничества) (формулы 2.1-2.7):

$$\text{G (2014 г.)} = \text{ПМ} + \text{ТМ} + \text{ОМ} + \text{РП} + \text{МС} = 0 + 0 + 0 + 0 + 0 = 0, \quad (2.1)$$

$$\text{G (2015 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}000 + 0{,}017 = 0{,}0907, \quad (2.2)$$

$$\text{G (2016 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}000 + 0{,}017 = 0{,}0907, \quad (2.3)$$

$$\text{G (2017 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}0085 + 0{,}017 = 0{,}0992, \quad (2.4)$$

$$\text{G (2018 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}0085 + 0{,}017 = 0{,}0992, \quad (2.5)$$

$$\text{G (2019 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}0085 + 0{,}017 = 0{,}0992, \quad (2.6)$$

$$\text{G (2020 г.)} = 0{,}033 + 0{,}0275 + 0{,}0132 + 0{,}0085 + 0{,}017 = 0{,}0992, \quad (2.7)$$

где ПМ – итоговое значение правовых мер;

ТМ – итоговое значение технических мер;

ОМ – итоговое значение организационных мер;

РП – итоговое значение развития потенциала;

МС – итоговое значение мер в области сотрудничества;

G – итоговое значение индекса GCI.

Итоговые значения адаптированного индекса GCI со значениями, определенными экспертами за 2014, 2016, 2018 и 2020 гг. (ключевыми изменениями), отражены в Приложении И. На рисунке 2.5 представлена динамика развития показателей GCI ДНР согласно экспертным оценкам.

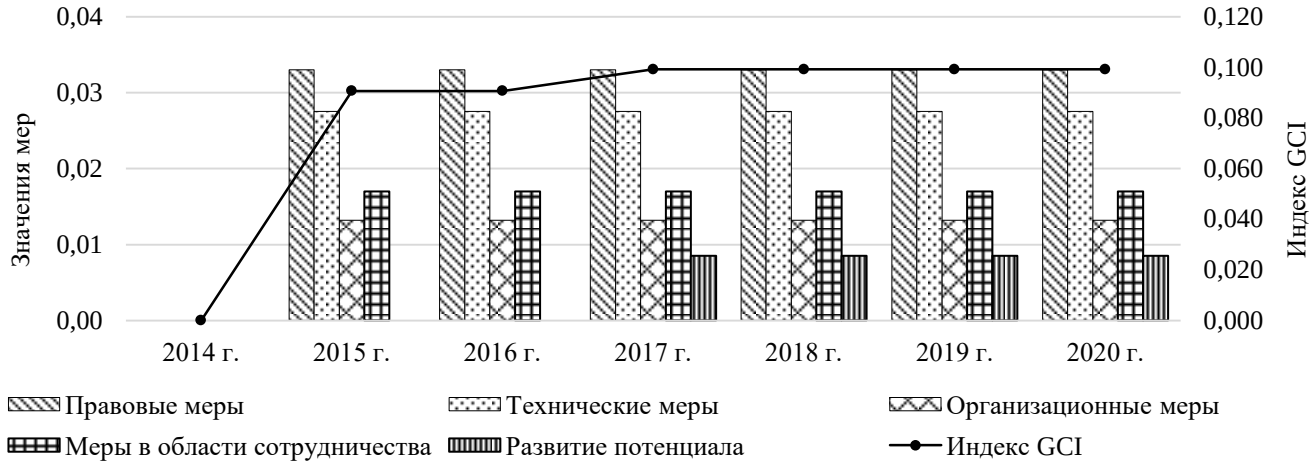

Рисунок 2.5 – Динамика развития Глобального индекса кибербезопасности (GCI) и его составляющих согласно экспертным оценкам, ДНР, 2014-2020 гг. [составлено автором]

Согласно адаптированной методике расчета, с 2016 г. по 2017 г., наблюдается прирост значения индекса GCI на 0,0085, при этом в период с 2017 г. по 2020 г. его прирост согласно экспертным оценкам не наблюдается. Указанная динамика с учетом низкого уровня индекса (0,0992 в 2020 г.) относительно нормативного значения, которое находится в интервале от 0 до 1, указывает на замедление роста и дает основание сделать вывод о том, что общегосударственные подходы к обеспечению информационной безопасности в ДНР недостаточно развиваются в связи со сложными политическими,

экономическими, кадровыми условиями и другими факторами, связанными с низким вниманием уполномоченных регуляторов к исследуемой сфере.

По результатам исследования определены основные направления совершенствования системы с наименьшим значением индекса – организационные меры, развитие потенциала и меры в области сотрудничества, при этом оптимизация указанных направлений на общегосударственном уровне возможна на основе совершенствования правовых и технических мер.

Стоит отметить, что по оценкам экспертов, общегосударственные подходы к указанным отраслям недостаточно наделены системностью, взаимодействия между ОГВ и регуляторами отлажены недостаточно эффективно. Каждый орган в исследуемой сфере действует на свое усмотрение, что приводит к падению уровня качества в применяемых подходах, сложностям в структурировании и совершенствовании государственного регулирования, отлаженности, скоординированности действий в инфокоммуникационной отрасли.

В результате системный подход к межведомственному электронному взаимодействию не сформирован, формирование электронного правительства не осуществляется, а качество и безопасность важнейших для государственного управления цифровых ресурсов в существующих условиях остаются сложно контролируемыми не только для уполномоченных структур, но и для руководства ОГВ. Указанные тенденции способствует всестороннему затруднению анализа, оценки и принятия стратегических решений в отрасли ИТ и сфере обеспечения ИБ, как для ОГВ, так и для высшего руководства ДНР.

Необходимо отметить, что без формирования направления защиты критической информационной инфраструктуры для государственных регуляторов становится максимально усложненным процесс обеспечения безопасности ключевых государственных информационных активов, т. к. не существует понимания важности данных, обрабатываемых в значимых для общегосударственной безопасности информационных системах, а также отсутствует государственное контрольно-надзорное направление за исполнением требований законодательства, состоянием и степенью защищённости указанных

объектов. Поэтому для ДНР представляется приоритетным направлением регулирование вопросов обеспечения безопасности критической информационной инфраструктуры.

Реализация данного направления должна происходить через принятие законодательного акта по указанным вопросам (по аналогии с российским ФЗ-187), способствующего систематизации структуры регулирования. Целесообразно предусмотреть конкретные обязанности по отнесению объектов к категориям значимости с определением перечня требуемых мер обеспечения ИБ через определения их минимального набора и общего правила о принятии разумных и достаточных мер по обеспечению ИБ даже если они не приведены в конкретном НПА, т.к. срок формирования зрелого нормативного поля в исследуемой области с учетом низкого уровня эффективности процедур согласования и принятия НПА в ДНР, определить сложно.

Основными функциями невластных субъектов критической информационной инфраструктуры можно назвать: осуществление категорирования объектов, принятие необходимых мер обеспечения ИБ, взаимодействие с уполномоченными ОГВ и информирование их об инцидентах. Относительно выбора соответствующих регуляторов в области критической информационной инфраструктуры для ДНР представляется перспективным создание единого органа, который будет обеспечивать работу по принципу «единого окна» и обладать следующими минимальными полномочиями: координация ОГВ при совершенствовании СОИБ; диагностика и оценка рисков ИБ в ОГВ; управление инцидентами ИБ в ОГВ; координация организаций в области защиты значимых объектов критической информационной инфраструктуры ДНР; распространение предупреждений об опасности угроз безопасности информации; подготовка методических рекомендаций об основных угрозах; содействие расследованию киберпреступлений.

Объектная модель регулирования области обеспечения безопасности критической информационной инфраструктуры наиболее подходит для ДНР. Формирование данной модели в существующих условиях должно производиться

с учетом установления соразмерно затратных требований к субъектам критической информационной инфраструктуры. Перспективным представляются: 1 – метод дифференциации и пропорциональности рискам (когда количество обязанностей при выполнении требований зависит от категории значимости и рисков на конкретном объекте), 2 – принцип содействия (при котором субъект критической информационной инфраструктуры может обратиться в уполномоченный орган за помощью на различных этапах защиты объектов), 3 – метод поощрения за выполнение экономически затратных требований субъекта критической информационной инфраструктуры путем предоставления экспертной помощи и субсидирования в разработке систем защиты информации, поддержке разработанных в соответствии с требованиями по ИБ систем и др. государственных преференциях [121, с. 66].

Целесообразно установить административную ответственность за неисполнение обязанностей субъектами критической информационной инфраструктуры. Уголовная ответственность, связанная с атаками на значимые объекты критической информационной инфраструктуры, должна предусматривать соразмерность штрафов и сроков заключения предполагаемым последствиям правонарушений. Дифференциация проводится в зависимости от категории значимости и от срока, в который не была исполнена обязанность.

2.3. Оценка рисков информационной безопасности в органе государственной власти

С учетом неопределенности в подходах к формированию СОИБ в ОГВ оценка мер, средств и процессов обеспечения ИБ, при наличии рисков, свойственных существующим подходам, является важнейшим инструментом

развития государственных ИС и ИТ-инфраструктур. В условиях функционирования ОГВ, сопровождающихся оттоком кадров и иными следствиями существующих проблем, особое значение приобретают методические подходы к оценке рисков, позволяющие стандартизировать процессы анализа СОИБ и оптимизировать затраты ресурсов на обеспечение ИБ. Парадигма риск-ориентированных подходов к обеспечению ИБ по мнению многих авторов является одним из ключевых факторов построения эффективной СОИБ, т.к. позволяет гибко оптимизировать распределение ресурсов, вкладываемых в формирование и поддержку процессов ИБ [72; 102; 201; 202]. Также эффективно проведенная оценка рисков, включающая выявление и оценку уязвимостей и угроз, позволяет обратить внимание на ключевые аспекты и каналы потенциально возможной компрометации информационных активов и выделить приоритетные направления для дальнейшей диагностики СОИБ.

Процесс расчета рисков ИБ актуален на всех этапах зрелости СОИБ и является полезным для руководства ОГВ, в первую очередь, с точки зрения оценки возможных экономических потерь от реализации существующих угроз безопасности информации. Чтобы применить к управлению рисками эффективный структурированный методический подход, необходимо объединить все требуемые аспекты данного подхода и описать их в рамках одной комплексной системы, предназначенной помочь ОГВ в оптимизации СОИБ. Поэтому крайне важным фактором для СОИБ в ОГВ является выбор эффективных методов оценки рисков ИБ [201-203].

Подходы к обеспечению ИБ, базирующиеся на риск-менеджменте, распространены в мировой и отечественной практике и используются в различных сферах и областях, поскольку оперируют широким понятием «активы». Автором проанализированы стандартизированные методики оценки и обработки рисков, подробно описанные в работах таких ученых, как В.В. Пугин, П.В. Плетнев, М.А. Одинцова, С.А. Глушенко, О.Ю. Губарева, Л.М. Ильченко и др. [204-209], однако, ни одна из них, по мнению автора, на современном этапе не является оптимальной для условий существования ОГВ ДНР с учетом тотальной

ограниченности в ресурсах и необходимости эффективной оптимизации СОИБ в ОГВ и ориентации на опыт РФ.

Целью управления рисками ИБ является поддержание их на приемлемом для ОГВ уровне. Для реализации данной цели необходим эффективный инструмент в виде методического подхода к оценке рисков ИБ, направленной на решение следующих задач:

– установка критериев оценки рисков и определения их приемлемости;

– гарантия обоснованности и непротиворечивости массивов рисков, актуальных для рассматриваемой системы;

– идентификация рисков, направленных на такие свойства информационных активов, как конфиденциальность, целостность и доступность;

– идентификация владельцев рисков – физических, юридических лиц или подразделений, отвечающих за управление риском и обладающих необходимыми для этого полномочиями руководителей, специалистов по ИБ и др. сотрудников ОГВ;

– оценка потенциальных потерь в случае реализации риска;

– опосредованное апостериорное определение вероятности реализации рисков и определение их величины;

– сопоставление рисков с установленными критериями, а также определение вектора приоритетных направлений по их обработке.

Переходя к практической части апробации методического подхода, стоит отметить, что отрасль ИТ является одной из наиболее приоритетных для развития современного общегосударственного благосостояния и одновременно одной из самых чувствительных к вопросам обеспечения ИБ. В настоящее время все ключевые информационно-коммуникационные взаимодействия: через сеть интернет, мобильную-, радиосвязь в ДНР так или иначе связаны с деятельностью Министерства связи ДНР.

Расследование преступлений в исследуемой отрасли также касается вопросов регулирования взаимодействия операторов связи и подведомственных Министерству связи ДНР предприятий с уполномоченными органами при

осуществлении оперативно-розыскных мероприятий. Поэтому можно констатировать, что Министерство связи ДНР является одним из системообразующих регуляторов как в отрасли ИТ, так и в сфере обеспечения ИБ в ДНР. Что обосновывает выбор указанного ОГВ в качестве объекта апробации методического подхода.

В процессе апробации методического подхода рассматривается корпоративная распределенная многопользовательская информационная среда ОГВ, имеющая подключение к сетям общего пользования, обрабатывающая информацию разного уровня конфиденциальности и не содержащая сведений, составляющих государственную тайну. Стоит отметить, что все процедуры оценки рисков ИБ выполняются экспертами, однако, в дальнейшем, с целью поддержания эффективного процессного подхода к ИБ согласно модели PDCA могут проводиться сотрудниками подразделений ОГВ, ответственных за ИБ.

Компетентность привлекаемых к апробации методического подхода экспертов была обоснована через предъявление к ним следующих профессиональных требований:

– наличие высшего образования в сфере обеспечения ИБ и (или) прохождение курсов профессиональной переподготовки по направлению «Информационная безопасность», и (или) имеющих не менее трех лет стажа практической работы в сфере обеспечения ИБ;

– знание законодательства и ключевых НПА ДНР и РФ в сфере обеспечения ИБ;

– знание международных стандартов и государственных стандартов РФ в сфере обеспечения ИБ;

– умение работать с технической документацией;

– знания о современных средствах и системах вычислительной и телекоммуникационной техники, операционных системах, системах управления базами данных, а также о конкретных способах обеспечения ИБ в них;

– знания о возможных источниках и способах реализации угроз безопасности информации (далее – УБИ);

– знания о способах обеспечения ИБ в информационных и телекоммуникационных системах ОГВ;

– понимание различных подходов к обеспечению ИБ, знание защитных мер, свойственных им ограничений;

– независимость, основанная на отсутствии коммерческого и финансового интереса и (или) иного давления, способного оказать влияние на принимаемые решения [55].

В рамках данного исследования апробация методического подхода осуществляется на основании экспертных оценок. Для этого автором привлечены эксперты в количестве 10 человек, 5 из которых являются специалистами Министерства связи ДНР и 5 – специалистами ГУП ДНР «Углетелеком».

Обобщенная модель структуры алгоритма методического подхода к оценке рисков ИБ в ОГВ представлена на рисунок 2.6. Первой стадией первого этапа «Идентификация и оценка значимости активов» является «Проведение опроса сотрудников», в результате которого посредством опросных листов определяются первичные сведения об информационных активах (их перечень и назначение). После этого, в результате выполнения стадии «Выявление ключевых активов и аспектов их функционирования» эксперты на основании уточнения и обработки полученной ранее информации формируют следующие сведения:

– перечень ключевых информационных активов, связанных с ними бизнес-процессов и границ ответственности за компоненты;

– сведения об архитектуре активов и условиях их функционирования;

– сведения о механизмах, мерах и средствах ИБ, связанных с ключевыми активами.

Выявление ключевых информационных активов позволяет определить их значимость, ограничить рамки оценки и сфокусировать ресурсы на обнаружении наиболее актуальных УБИ для информационной среды ОГВ.

Далее экспертами на основании анализа бизнес-процессов, сведений об архитектуре ключевых информационных активов и аспектах их функционирования, сведений о мерах и средствах ИБ в ОГВ, требований

законодательства, отраслевых и внутренних требований ОГВ, а также сведений о мерах и средствах обеспечения ИБ проводится оценка возможных негативных последствий для их функционирования.

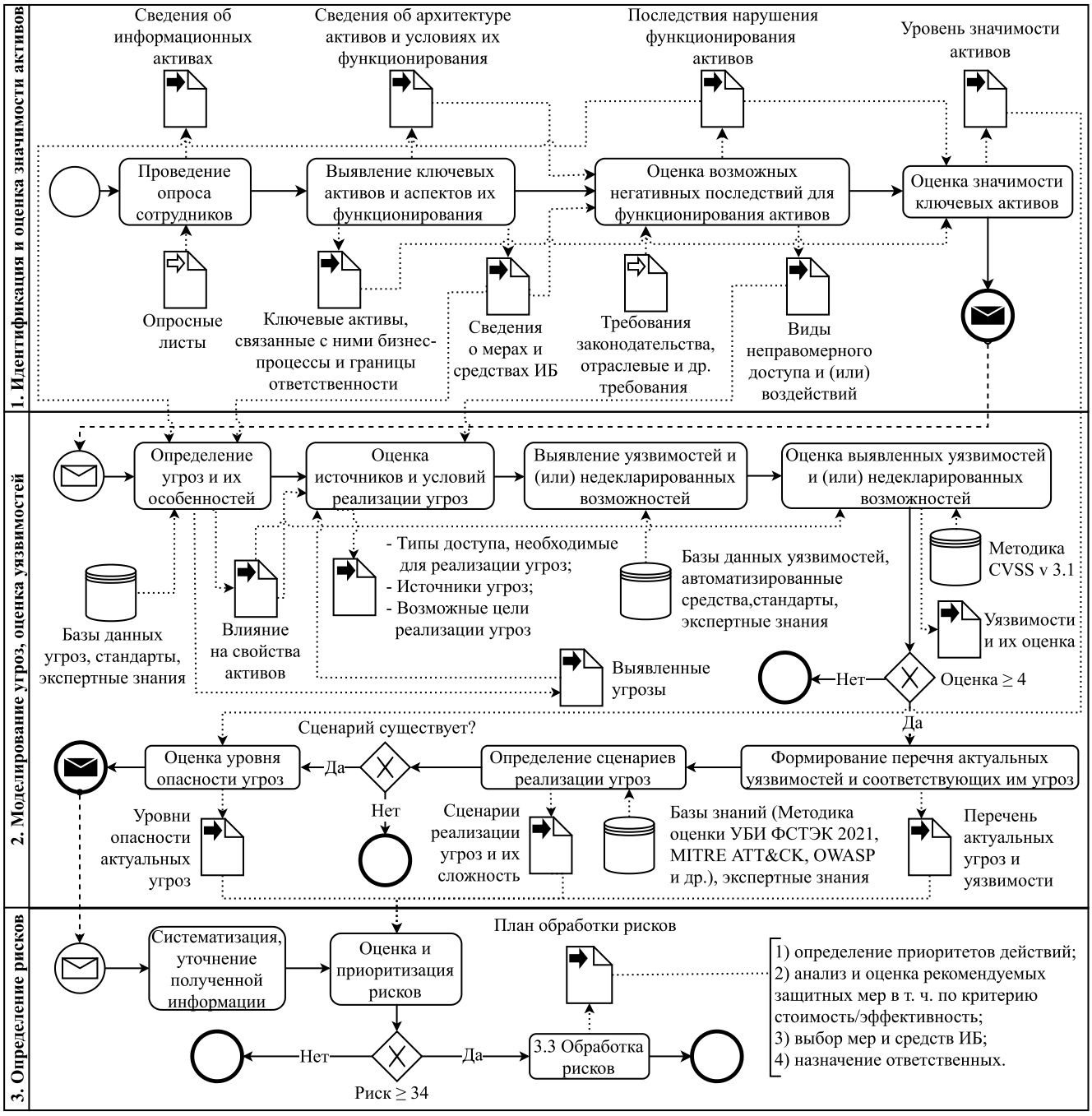

Рисунок 2.6 – Алгоритм оценки рисков информационной безопасности в ОГВ [составлено автором]

В результате реализации стадии 3 этапа 1 определяются:

1. Последствия нарушения функционирования активов, которые включают:

– степень влияния на непрерывность деятельности ОГВ;

– степень влияния на деловую репутацию;

– объем финансовых и материальных потерь;

– объем финансовых и материальных затрат, необходимых для восстановления свойств безопасности информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;

– количество человеческих ресурсов, необходимых для восстановления свойств безопасности для информационных активов рассматриваемого типа и ликвидации последствий нарушения ИБ;

– объем временных затрат, необходимых для восстановления свойств безопасности для информационных активов и ликвидации последствий нарушений;

– степень нарушения законодательных требований и (или) договорных обязательств ОГВ;

– степень нарушения требований, регулирующих и контролирующих (надзорных) органов в области обеспечения ИБ;

– данные о наличии у рассматриваемых типов сред активов защитных мер;

– объем хранимой, передаваемой, обрабатываемой и уничтожаемой информации, соответствующей рассматриваемой среде актива [55].

2. Виды неправомерного доступа и (или) воздействий на информационные активы, которые могут быть использованы злоумышленниками (таблица 2.12).

Таблица 2.12 – Виды неправомерного доступа и (или) воздействий на информационные активы [составлено автором на основе [210]]

Идентификатор	Виды неправомерного доступа
УКИ	Утечка защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение конфиденциальности)
НСД	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ОВО	Отказ в обслуживании компонентов и/или систем (нарушение доступности)
МЗИ	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
НИВ	Несанкционированное использование вычислительных ресурсов в интересах решения несвойственных им задач
НРС	Нарушение функционирования (работоспособности) программных и аппаратных средств обработки, передачи и хранения информации

На заключительной стадии первого этапа проводится оценка значимости выявленных ключевых информационных активов, которая определяется посредствам экспертных оценок (таблица 2.13).

Таблица 2.13 – Шкала определения значимости информационных активов ОГВ (S_j) [составлено автором на основе [210]]

Опасность	Описание	Значение, баллы
Низкая	Реализации УБИ, нарушит функциональную деятельность одного сотрудника ОГВ и (или) станет причиной выполнения возложенных на сотрудника функций с недостаточной эффективностью и (или) для выполнения функций, реализуемых активом, потребуется привлечение дополнительных ресурсов	1
Средняя	Реализация УБИ нарушит функциональную деятельность более чем одного сотрудника и (или) ОГВ не сможет выполнять хотя бы одну из возложенных на него функций	2
Высокая	Реализация УБИ нарушит функциональную деятельность всех сотрудников ОГВ и (или) нарушит выполнение нескольких функций	3

Определяются данные оценки на основании выявленной ранее информации, а именно: критичности бизнес-процессов, видов неправомерного доступа и(или) воздействий и последствий нарушения функционирования ключевых информационных активов, в результате чего определяется уровень значимости ключевых активов. В таблице 2.14 представлены основные результаты, полученные экспертами по итогам выполнения всех стадий 1-го этапа.

Первой стадией этапа 2 «Моделирование угроз, оценка уязвимостей» является «Определение угроз и их особенностей», осуществляемое экспертами с помощью открытых баз данных угроз и использованием автоматизированных средств моделирования угроз, а также стандартов и экспертных знаний. Здесь важно отметить, что «Методика оценки угроз безопасности информации» разработанная в 2021 г. ФСТЭК РФ содержит детали реализации этапа 2 и служит базой знаний настоящего этапа [210].

На стадии «Определение угроз и их особенностей» определяются:

– выявленные угрозы безопасности информации;

– влияние угроз на свойства активов (конфиденциальность, целостность, доступность) по шкале: 1 – оказывает влияние, 0 – не оказывает.

Таблица 2.14 – Результаты идентификации и оценки значимости ключевых информационных активов Министерства связи ДНР [составлено автором на основе [210]]

Информационный актив/ группа активов		Основные бизнес-процессы	Виды неправомерного доступа	Последствия нарушений функционирования актива	Значимость актива (S_j)
П1	Носители информации (электронные, бумажные)	Поддержка операционной и функциональной деятельности.	УКИ, НСД, МЗИ, НИВ	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	1
П2	Система электронного документооборота	– внутренняя деятельность, связанная с ВНД; – управление документами	УКИ, НСД, МЗИ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	3
П3	Локальная вычислительная сеть и промежуточные устройства	Передача информации между программными и техническими средствами ОГВ	УКИ, НСД, МЗИ, НРС	– нарушение конфиденциальности ПД; – непредоставление государственных услуг	3
П4	Система учета товарно-материальных ценностей	Поддержка и автоматизация процессов учета и хранения товарно-материальных активов ОГВ	УКИ, НСД, МЗИ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	1
П5	Система автоматизации работы кадровых операций	– формирование и управление кадровой политикой; – ведение кадрового делопроизводства; – обучение, развитие и оценка кадров; – формирование кадрового резерва	УКИ, НСД, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	2
П6	Система бухгалтерского и финансового учета	– бюджетирование деятельности; – управленческий и бухгалтерский учет, управление денежными средствами, задолженностями, издержками и др.	УКИ, НСД, МЗИ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	2
П7	Удаленное хранилище данных	Хранение данных для операционной и функциональной деятельности	УКИ, НСД, МЗИ, НИВ, НРС	– нарушение производственной деятельности; – нарушение конфиденциальности ПД	2
П8	Система электронной почты	Поддержка операционной и функциональной деятельности	УКИ, НСД, ОВО, НИВ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	2
П9	Информационный сайт	– мониторинг медиапространства; – взаимодействие со СМИ; – реализация социальных проектов	НСД, ОВО, МЗИ, НРС	– утрата доверия (нарушение репутации); – публикация недостоверной социально значимой информации; – увеличение количества жалоб в ОГВ; – появление негативных публикаций СМИ	2
П10	Мобильные и переносные устройства	Коммуникационные взаимодействия в рамках функциональной деятельности.	УКИ, НСД, МЗИ, НИВ, НРС	– утечка информации ограниченного доступа	2
П11	Система управления учетными данными и доступом к информационным системам	– учет пользователей и их прав доступа; – управление правами доступа и учетными записями; – аудит прав доступа с помощью встроенных отчетов.	УКИ, НСД, НРС	– нарушение конфиденциальности ПД; – непредоставление государственных услуг; – утечка информации ограниченного доступа	3
П12	Автоматизированное рабочее место пользователя	Обеспечение операционной и функциональной деятельности	УКИ, НСД, МЗИ, НИВ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	1
П13	Автоматизированное рабочее место администратора	Обеспечение операционной и функциональной деятельности	УКИ, НСД, МЗИ, НИВ, НРС	– нарушение конфиденциальности ПД; – утечка информации ограниченного доступа	1

В ходе реализации данной стадии, эксперты, базируясь на данных предыдущего этапа, проводят первоначальное определение УБИ, свойственным существующим активам. В последующем, данный список будет сокращаться в случае отсутствия актуальных уязвимостей и (или) сценариев их реализации.

В ходе выполнения второй стадии второго этапа «Оценка источников и условий реализации угроз» эксперты, пользуясь базами данных угроз, автоматизированными средствами моделирования угроз, стандартами и общими экспертными знаниями проводят анализ угроз и создается модель нарушителя (определяют категории, виды и возможности нарушителей) на основе предположений о потенциале атакующих, т.е. о мере усилий, затрачиваемых нарушителем при реализации УБИ, при этом выявляются:

– возможные цели для реализации УБИ;

– источники УБИ (характеристика и потенциал нарушителей);

– типы доступа к активу, необходимые для реализации УБИ по шкале представленной в таблица 2.15 [211].

Таблица 2.15 – Шкала определения типа доступа необходимого для сценария реализации угрозы (D_j) [составлено автором на основе [210]]

Опасность	Описание	Значение, баллы
Физический	Сценарий реализации УБИ предусматривает физический доступ нарушителя к активам ОГВ	1
Локальный	Сценарий реализации УБИ предусматривает локальный доступ нарушителя к системе или сети	2
Удаленный	Сценарий реализации УБИ предусматривает сетевой удаленный доступ нарушителя к активу	3

Третья стадия этапа 2 – «Выявление уязвимостей и (или) недекларированных возможностей» также осуществляется экспертами посредством инструментальной, методической поддержки и экспертных знаний (баз данных, стандартов, автоматизированных средств анализа поиска и анализа уязвимостей и др.). Осуществляется данная процедура в очном формате экспертами, получившими допуск и доступ к ключевым информационным активам ОГВ.

Далее производится «Оценка выявленных уязвимостей и (или) недекларированных возможностей» посредством методической базы, в качестве которой используется Общая система оценки уязвимостей (Common Vulnerability Scoring System – CVSS v3.1). Шкала определения уровня уязвимости представлена в таблице 2.16.

Таблица 2.16 – Шкала определения уровня уязвимости (U_i) [составлено автором на основе [213]]

Количественная оценка, баллы	Качественная оценка	Экспертное решение
0,1-0,9	Ничтожно малая	Уязвимость не актуальна
1,0-3,9	Низкая	Уязвимость не актуальна на данном этапе
4,0-6,9	Средняя	Уязвимость рекомендуется к анализу на предмет возможности реализации УБИ
7,0-8,9	Высокая	Уязвимость требует анализа на предмет возможности реализации УБИ
9,0-10,0	Критическая	

Расчет осуществляется посредством калькулятора расчета значений уязвимостей ФСТЭК [212]. При проведении анализа уязвимостей применяются следующие способы их выявления:

– анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности;

– анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации;

– анализ состава установленного ПО и обновлений безопасности ключевых активов с применением средств анализа защищенности.

После выявления актуальных угроз, уязвимостей и определения их оценок экспертами осуществляется формирование итогового перечня. Результаты оценки уровня уязвимостей, определяемые экспертами в ходе анализа их реквизитов по методике CVSS v.3.1 усредняются. Итоговые экспертные оценки уязвимостей, соответствующих выявленным угрозам для ключевых информационных активов Министерства связи ДНР, представлены в таблице 2.17. Приведенный перечень с учетом малого количества уязвимостей высокого уровня и отсутствия критических свидетельствует об относительно высоком уровне технической защищенности ключевых информационных активов исследованного ОГВ.

Таблица 2.17 – Перечень актуальных технических угроз безопасности и усредненных экспертных оценок уязвимостей ключевых информационных активов Министерства связи ДНР, баллы [составлено автором на основе [211]]

Угрозы безопасности информации		Оценка выявленных уязвимостей (U_i)												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		П1	П2	П3	П4	П5	П6	П7	П8	П9	П10	П11	П12	П13
У1	Угроза утраты носителей информации	3,2	-	-	-	-	-	-	-	-	-	-	-	-
У2	Угроза несанкционированного восстановления удалённой защищаемой информации	4,2	-	-	-	-	-	-	-	-	4,3	-	4,1	4,3
У3	Угроза восстановления и/или повторного использования аутентификационной информации	-	5,3	-	-	-	-	-	5,4	5,8	-	-	-	-
У4	Угроза форматирования носителей информации	5,3	-	-	-	-	-	-	-	-	6,9	-	6,4	6,9
У5	Угроза неправомерного ознакомления с защищаемой информацией	4,2	-	-	-	-	-	-	-	-	4,4	-	4,4	4,8
У6	Угроза преодоления физической защиты	5,1	-	-	-	-	-	-	-	-	7,4	-	7,3	7,4
У7	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	4,3	-	-	-	-	-	-	-	-	-	-	5,5	5,9
У8	Угроза загрузки нештатной операционной системы	-	-	-	-	-	-	-	-	-	6,8	-	6,2	6,8
У9	Угроза злоупотребления доверием потребителей облачных услуг	-	-	-	-	-	-	-	-	6,2	-	-	-	-
У10	Угроза изменения компонентов информационной (автоматизированной) системы	-	-	6,9	6,2	6,1	6,5	-	-	-	-	-		
У11	Угроза физического устаревания аппаратных компонентов	-	-	-	-	-	-	-	-	-	3,9	-	3,3	3,9
У12	Угроза хищения средств хранения, обработки и (или) ввода/вывода/ передачи информации	6,2	-	-	-	-	-	-	-	-	7,5	-	6,8	7,5
У13	Угроза использования механизмов авторизации для повышения привилегий	-	5,9	-	4,2	4,8	5,3	4,4	4,8	-	-	-	-	-
У14	Угроза исследования механизмов работы программы	-	-	-	4,2	4,3	4,8	-	4,8	4,8	-	-	-	-
У15	Угроза нарушения доступности облачного сервера	-	-	-	-	-	-	-	6,1	5,3	-	-	-	-
У16	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия	-	3,9	-	-	-	-	-	3,1	-	-	-	-	-
У17	Угроза невозможности восстановления сессии работы на персональном компьютере при выводе из промежуточных состояний питания	-	-	-	-	-	-	-	-	-	3,1	-	2,9	3,2
У18	Угроза некорректного использования функционала программного и аппаратного обеспечения	-	5,4	-	-	-	-	-	5,1	-	-	-	5,1	-
У19	Угроза неопределённости ответственности за обеспечение безопасности облака	-	-	-	-	-	-	-	4,1	4,2		-	-	-
У20	Угроза неправомерных действий в каналах связи	-	-	6,5	-	-	-	-	-	-	-	-	-	-
У21	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	-	-	6,7	-	-	-	-	-	-	-	-	-	-
У22	Угроза несанкционированного доступа к аутентификационной информации	-	-	-	-	-	-	4,2	-	5,3	-	-	-	-
У23	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	-	-	-	-	-	-	3,3	-	-	-	-	-	-

Продолжение таблицы 2.17

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
У24	Угроза несанкционированного изменения аутентификационной информации	-	-	-	-	-	-	4,2	-	-	-	-	-	-
У25	Угроза несанкционированного копирования защищаемой информации	5,1	-	-	-	-	-	5,3	-	-	-	-	5,1	5,9
У26	Угроза несанкционированного удаления защищаемой информации	4,9	-	-	-	-	-	5,4	-	-	-	-	5,3	6,2
У27	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	-	-	5,9	-	-	-	-	-	4,1	-	-	-	-
У28	Угроза перебора всех настроек и параметров приложения	-	3,9	-	-	-	-	3,3	3,5	3,9	-	-	-	-
У29	Угроза перехвата данных, передаваемых по вычислительной сети	-	3,5	-	-	-	-	-	-	-	-	-	-	-
У30	Угроза повышения привилегий	-	6,3	-	-	-	-	5,1	-	-	-	-	-	-
У31	Угроза подмены содержимого сетевых ресурсов	-	-	-	-	-	-	-	5,7	-	-	5,1	-	-
У32	Угроза приведения системы в состояние «отказ в обслуживании»	-	-	-	-	-	-	-	-	6,1	-	-	-	-
У33	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	-	-	-	-	-	-	-	-	5,3	-	-	-	-
У34	Угроза включения в проект недостоверно испытанных компонентов	-	3,9	-	3,1	3,3	3,3	-	-	-	-	-	-	-
У35	Угроза распространения «почтовых червей»	-	-	-	-	-	-	-	4,9	-	-	-	-	-
У36	Угроза несанкционированного использования привилегированных функций мобильного устройства	-	-	-	-	-	-	-	-	-	3,7	-	-	-
У37	Угроза несанкционированного использования системных и сетевых утилит	-	-	-	-	-	-	-	-	-	4,2	-	-	-
У38	Угроза несанкционированной модификации защищаемой информации	5,1	-	-	-	-	-	5,3	-	-	-	-	5,1	5,9
У39	Угроза использования уязвимых версий программного обеспечения	-	4,8	-	-	-	-	4,2	4,3	-	-	-	-	-
У40	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере	-	6,4	-	-	-	-	-	6,2	-	-	7,1	-	-
У41	Угроза межсайтового скриптинга	-	-	-	-	-	-	-	-	5,1	-	-	-	-
У42	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	5,1	-	-	-	-	-	-	-	-	5,9	-	5,3	5,9
У43	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	-	3,8	-	3,3	3,5	3,9	-	3,5	3,9	-	3,3	-	-
У44	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы на события безопасности	-	5,5	5,9	5,1	5,1	5,3	5,1	5,3	-	-	5,9	-	-
У45	Угроза несанкционированной установки приложений на мобильные устройства	-	-	-	-	-	-	-	-	-	4,1	-	-	-
У46	Угроза внедрения вредоносного кода через рекламу, сервисы и контент	-	-	-	-	-	-	-	-	-	3,7	-	3,1	3,4
У47	Угроза деструктивного использования декларированного функционала BIOS	-	-	-	-	-	-	-	-	-	4,8	-	4,2	4,8
У48	Угроза программного сброса пароля BIOS	-	-	-	-	-	-	-	-	-	4,3	-	4,1	4,3
У49	Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации	3,9	-	-	-	-	-	3,1	3,3	-	-	-	-	-

После оценки выявленных уязвимостей производится корреляция определенных угроз и выявленных уязвимостей ключевых информационных активов. При необходимости список актуальных угроз дополняется либо из него исключаются угрозы, для которых не была обнаружена уязвимость. Также из списка исключаются уязвимости с низкой оценкой, после чего формируется перечень актуальных уязвимостей и соответствующих им угроз. Стоит отметить, что выявленные угрозы во многих случаях могут быть реализованы через разные уязвимости и способы их эксплуатации, однако, для упрощения использования методического подхода и оптимизации имеющихся на апробацию ресурсов выбрана схема: одна уязвимость – одна угроза – один сценарий ее реализации. Также для апробации список выявленных угроз был ограничен только техническими угрозами.

На стадии 6 этапа 2 настоящего методического подхода производится определение сценариев реализации УБИ, в ходе которого эксперты пользуются следующими базами знаний: MITRE ATT&CK, OWASP, Методикой оценки УБИ 2021 ФСТЭК РФ и др., а также экспертными знаниями, определяя актуальные сценарии, техники, тактики и процедуры реализации выявленных УБИ через соответствующие им уязвимости. Целью данного этапа является выявление сценариев реализации угроз и определения их сложности с применением шкалы, представленной в таблице 2.18, а также формирование понимания актуальности и способов реализации УБИ.

Таблица 2.18 – Шкала определения уровня сложности сценария реализации УБИ (P_j) [составлено автором на основе [210]]

Опасность	Описание	Значение, баллы
Высокий	Сценарий реализации УБИ может быть реализован нарушителем с высоким потенциалом	1
Средний	Сценарий реализации УБИ может быть реализован нарушителем со средним потенциалом	2
Повышенный	Сценарий реализации УБИ может быть реализован нарушителем с базовым повышенным потенциалом	3
Умеренный	Сценарий реализации УБИ может быть реализован нарушителем с базовым потенциалом	4

Основными факторами для оценки уровня сложности сценария реализации УБИ (P_j) являются:

– данные о расположении источника угрозы относительно соответствующих типов объектов среды;

– информация о мотивации источника угрозы (для источников угроз антропогенного характера);

– предположения о квалификации и (или) ресурсах источника угрозы;

– статистические данные о частоте реализации угрозы ее источником в прошлом;

– информация о способах реализации УБИ;

– информация о сложности обнаружения реализации УБИ рассматриваемым источником;

– данные о наличии у рассматриваемых типов объектов среды ОГВ, технических и прочих априорных защитных мер [55].

Важно отметить, что УБИ является актуальной для информационного актива, если: имеются источник угрозы; условия для ее реализации; существует хотя бы один сценарий ее реализации, а воздействие на информационный актив может привести к негативным последствиям. В свою очередь, условиями, необходимыми для реализации УБИ, являются:

– наличие актуальных уязвимостей и (или) недекларированных возможностей активов, использование которых возможно нарушителем;

– наличие доступа к компонентам активов для реализации УБИ.

Из ранее сформированного списка исключаются угрозы, для которых обоснована неприменимость за счет отсутствия сценариев, условий реализации или негативных последствий, в том числе, за счет обоснованной достаточности мер и средств защиты информации от данной угрозы. В результате определяются актуальные угрозы и оценка соответствующих им уязвимостей.

В ходе реализации заключительной стадии второго этапа «Оценка уровня опасности УБИ» на основе показателей, выявленных на предыдущих стадиях в

отношении каждой i-ой угрозы с j-м сценарием ее реализации, определяется уровень опасности УБИ (W_i) для каждого актива (формула 2.8):

$$W_i = \sum_{j=1}^{k}(D_j + P_j + S_j), \quad (2.8)$$

где W_i – уровень опасности УБИ для информационного актива;

D_j – оценка типа доступа необходимого для реализации j-го сценария УБИ;

P_j – оценка уровня сложности реализации j-го сценария УБИ;

S_j – оценка уровня значимости актива для j-го сценария УБИ;

k – количество сценариев реализации данной УБИ.

В том случае, если для одной УБИ определено несколько сценариев ее реализации, оценка уровня ее опасности проводится для каждого сценария и предусматривать оценку сложности ее реализации для рассматриваемой архитектуры, анализ условий функционирования систем и сетей, а также определение возможного масштаба негативных последствий (ущерба) в случае успешной ее реализации. Заключительной стадией настоящего методического подхода является «Определение рисков».

В ходе реализации стадии «Систематизация, уточнение полученной информации» уточняются полученные на предыдущих этапах данные, после чего проводится «Оценка и приоритизация рисков». Здесь стоит указать на актуальность отмеченного И.В. Аникиным использования трехфакторного подхода определения уровня риска ИБ, используемого в стандартах и научных работах [215-218], согласно которому уровень риска ИБ определяется по следующей формуле [214, с. 27] (формула 2.9):

$$R(V,T) = PossV(V) * PossT(T) * Impact(T), \quad (2.9)$$

где $PossV(V)$ – возможность использования уязвимости;

$PossT(T)$ – возможность реализации угрозы, используя уязвимость (V);

$Impact(T)$ – ущерб от реализации указанной угрозы.

Указанная выше трехфакторная оценка является востребованной, однако с учетом современных реалий, с точки зрения автора, требует уточнения. Ущерб от реализации УБИ является показателем, аналогичным значимости информационных активов (S_j), входящей в значение уровня опасности угрозы (W_i). В свою очередь, возможность использования уязвимости и реализации угрозы, согласно настоящему методическому подходу, определяется показателями, входящими в оценку уязвимости и уровень опасности УБИ.

Важным фактором, определяющим уровень риска ИБ, является вероятность реализации УБИ. Однако, с точки зрения многих ученых и экспертов расчет значения вероятности наступления события или инцидента ИБ крайне затруднен в условиях высокой неопределенности аспектов, влияющих на СОИБ ОГВ. С учетом наличия других показателей (уровень опасности актуальной УБИ и оценка уязвимости), приведенных в настоящем методическом подходе, расчет значения вероятности, по мнению автора, не рационален. Поэтому вероятность наступления риска целесообразно определять его уровнем (чем больше риск, тем больше вероятность его наступления).

В результате, автором принята итоговая формула расчета уровня риска ИБ (формула 2.10):

$$K_i = U_i * W_i, \tag{2.10}$$

где U_i – оценка уязвимости информационного актива;

W_i – уровень опасности актуальной угрозы для информационного актива;

K_i – уровень риска реализации угрозы через заданную уязвимость.

Показатель уровня риска ИБ реализации угрозы (K_i) служит приоритизирующим фактором при оптимизации мер и средств ИБ – чем риск выше, тем приоритетнее последовательность его обработки. Шкала определения уровня рисков ИБ, представлена в таблице 2.19.

Таблица 2.19 – Шкала определения уровня рисков ИБ (K_i) [составлено автором]

Количественная оценка, баллы	Экспертное решение
0-11	Риск не актуален
12-33	Риск низкий и не требует обработки на данном этапе
34-55	Риск средний и рекомендуется к обработке
56-77	Риск значителен и требует обработки
78-100	Риск критичен и требует обработки

При определении последовательности обработки в случае совпадения значений рисков для разных активов приоритет отдается активу с наибольшим общим риском (формула 2.11):

$$O_i = \sum_{i=1}^{m} K_i, \qquad (2.11)$$

где K_i – уровень риска реализации угрозы через заданную уязвимость;

m – количество угроз, соответствующих уязвимости;

O_i – общий риск реализации УБИ для актива.

В таблице 2.20 представлены итоговые результаты вычисления актуальных рисков ИБ в Министерстве связи ДНР согласно определенных экспертами значений.

Таблица 2.20 – Результирующая таблица оценки рисков ИБ в Министерстве связи ДНР [составлено автором]

Актив	Оценка актуальных уязвимостей (U_i)	УБИ	Показатели опасности угроз			Уровень опасности актуальных угроз (W_i)	Уровень риска реализации угроз (K_i)	Общий риск для актива (O_i)
			D_j	P_j	S_j			
1	2	3	4	5	6	7	8	9
П1	4,2	У2	1	4	1	6	25,2	277,6
	5,3	У4	1	4	1	6	31,8	
	4,2	У5	1	4	1	6	25,2	
	5,1	У6	1	2	1	4	20,4	
	4,3	У7	1	3	1	5	21,5	
	6,2	У12	1	4	1	6	37,2	
	5,1	У25	1	4	1	6	30,6	
	4,9	У26	1	3	1	5	24,5	
	5,1	У38	1	4	1	6	30,6	
	5,1	У42	1	4	1	6	30,6	

Продолжение таблицы 2.20

1	2	3	4	5	6	7	8	9
П2	5,3	У3	2	3	3	8	42,4	293,7
	5,9	У13	2	2	3	7	41,3	
	5,4	У18	2	2	3	7	37,8	
	6,3	У30	2	2	3	7	44,1	
	4,8	У39	2	3	3	8	38,4	
	6,4	У40	1	4	3	8	51,2	
	5,5	У44	2	2	3	7	38,5	
П3	6,9	У10	1	3	3	7	48,3	235,7
	6,5	У20	2	3	3	8	52	
	6,7	У21	2	2	3	7	46,9	
	5,9	У27	2	3	3	8	47,2	
	5,9	У44	2	2	3	7	41,3	
П4	6,2	У10	1	3	1	5	31	98,5
	4,2	У13	2	2	1	5	21	
	4,2	У14	2	2	1	5	21	
	5,1	У44	2	2	1	5	25,5	
П5	6,1	У10	1	3	2	6	36,6	121,8
	4,8	У13	2	2	2	6	28,8	
	4,3	У14	2	2	2	6	25,8	
	5,1	У44	2	2	2	6	30,6	
П6	6,5	У10	1	3	2	6	39	131,4
	5,3	У13	2	2	2	6	31,8	
	4,8	У14	2	2	2	6	28,8	
	5,3	У44	2	2	2	6	31,8	
П7	4,4	У13	2	3	2	7	30,8	292,2
	4,2	У22	1	4	2	7	29,4	
	4,2	У24	2	3	2	7	29,4	
	5,3	У25	1	4	2	7	37,1	
	5,4	У26	2	3	2	7	37,8	
	5,1	У30	2	2	2	6	30,6	
	5,3	У38	1	4	2	7	37,1	
	4,2	У39	2	3	2	7	29,4	
	5,1	У44	2	2	2	6	30,6	
П8	5,4	У3	2	3	2	7	37,8	407
	4,8	У13	2	2	2	6	28,8	
	4,8	У14	2	2	2	6	28,8	
	6,1	У15	2	3	2	7	42,7	
	5,1	У18	2	2	2	6	30,6	
	4,1	У19	1	4	2	7	28,7	
	5,7	У31	2	3	2	7	39,9	
	4,9	У35	3	3	2	8	39,2	
	4,3	У39	2	3	2	7	30,1	
	6,2	У40	1	4	2	7	43,4	
	5,3	У44	2	2	2	6	31,8	
	4,2	У45	2	2	2	6	25,2	
П9	5,8	У3	3	2	2	7	40,6	386,5
	6,2	У9	2	3	2	7	43,4	
	4,8	У14	2	2	2	6	28,8	
	5,3	У15	3	3	2	8	42,4	
	4,2	У19	1	4	2	7	29,4	
	5,3	У22	1	4	2	7	37,1	
	4,1	У27	3	3	2	8	32,8	
	6,1	У32	3	3	2	8	48,8	
	5,3	У33	3	3	2	8	42,4	
	5,1	У41	3	3	2	8	40,8	

Продолжение таблицы 2.20

1	2	3	4	5	6	7	8	9
П10	4,3	У2	1	4	2	7	30,1	393,5
	6,9	У4	1	4	2	7	48,3	
	4,4	У5	1	4	2	7	30,8	
	7,4	У6	1	2	2	5	37	
	6,8	У8	1	4	1	6	40,8	
	7,5	У12	1	4	2	7	52,5	
	4,2	У37	2	3	2	7	29,4	
	5,9	У42	1	4	2	7	41,3	
	4,1	У45	1	4	2	7	28,7	
	4,8	У47	1	3	2	6	28,8	
	4,3	У48	1	3	2	6	25,8	
	4,3	У2	1	4	2	7	30,1	
П11	5,1	У31	2	3	2	7	35,7	133,8
	7,1	У40	1	4	3	8	56,8	
	5,9	У44	2	2	3	7	41,3	
П12	4,1	У2	1	4	1	6	24,6	415,9
	6,4	У4	1	4	1	6	38,4	
	4,4	У5	1	4	1	6	26,4	
	7,3	У6	1	2	1	4	29,2	
	5,5	У7	1	3	1	5	27,5	
	6,2	У8	1	4	1	6	37,2	
	6,8	У12	1	4	1	6	40,8	
	5,1	У18	2	2	1	5	25,5	
	5,1	У25	1	4	1	6	30,6	
	5,3	У26	2	3	1	6	31,8	
	5,1	У38	1	4	1	6	30,6	
	5,3	У42	1	4	1	6	31,8	
	4,2	У47	1	3	1	5	21	
	4,1	У48	1	3	1	5	20,5	
П13	4,3	У2	1	4	1	6	25,8	423,9
	6,9	У4	1	4	1	6	41,4	
	4,8	У5	1	4	1	6	28,8	
	7,4	У6	1	2	1	4	29,6	
	5,9	У7	1	2	1	4	23,6	
	6,8	У8	1	4	1	6	40,8	
	7,5	У12	1	4	1	6	45	
	5,9	У25	1	4	1	6	35,4	
	6,2	У26	2	3	1	6	37,2	
	5,9	У38	1	4	1	6	35,4	
	5,9	У42	1	4	1	6	35,4	
	4,8	У47	1	3	1	5	24	
	4,3	У48	1	3	1	5	21,5	

Стоит отметить, что, несмотря на наличие рисков ИБ, большинство из них являются низкими либо средними, что говорит о достаточно высоком организационно-техническом уровне обеспечения ИБ в Министерстве связи ДНР, т.к. несмотря на наличие выявленных экспертами уязвимостей и угроз, значительное их количество купировано мерами и средствами обеспечения ИБ.

По результатам оценки и приоритизации, риски обрабатываются экспертами и распределяются на принятые и те, для которых формируется план обработки, формируемый на заключительной стадии настоящего методического подхода, который содержит:

– определение приоритетных действий по купированию рисков;

– анализ и оценку рекомендуемых защитных мер, в т. ч. по критерию «стоимость/эффективность»;

– выбор мер и средств ИБ, компенсирующих выявленные риски;

– назначение ответственности за проведение определенных работ.

В результате приоритизации рисков ответственные за ИБ подразделения ОГВ на основании полученных от экспертов рекомендаций по купированию существующих рисков производят оптимизацию мер и средств ИБ.

Таким образом, сформированный методический подход к оценке рисков ИБ в ОГВ позволил решить следующие задачи:

– определить актуальные уязвимости и угрозы безопасности информации ОГВ, вероятность реализации которых необходимо уменьшить или исключить;

– оценить и приоритизировать риски ИБ ОГВ;

– оценить общую защищенность СОИБ в ОГВ;

– выработать рекомендации по оптимизации СОИБ в ОГВ.

Стоит отметить, что решение указанных задач является важным для настоящего исследования, т.к. позволяет оценить состояние защищенности ключевых информационных активов. При этом с целью повышения уровня качества данных при получении комплексной оценки уровня мер, средств, и, главным образом, процессов СМИБ, на базе которых существует возможность эффективной оптимизации подходов к формированию и развитию СОИБ в ОГВ, необходимо осуществить более глубокий и комплексный анализ системы.

Выводы к главе 2

1. Выявление и анализ ключевых информационных систем ОГВ и ведомств ДНР, а также аспектов, связанных с их функционированием, позволили определить фрагментарность подходов к разработке, внедрению и сопровождению государственных информационных систем. Исследованы функциональные области электронного правительства и определено их состояние в ДНР.

2. Проведен анализ динамики развития Индекса телекоммуникационной инфраструктуры (TII) в ДНР, являющегося одним из трех составных компонентов Индекса развития электронного правительства (EGDI). Выявлена положительная динамика, указывающая на интенсивное развитие телекоммуникационной инфраструктуры ДНР, сопровождающееся приростом числа пользователей сети интернет и числа абонентов мобильной связи. Выявленная тенденция указывает на то, что на настоящем этапе уровень готовности информационно-телекоммуникационной инфраструктуры ДНР позволяет говорить о наличии технической возможности поступательного перехода на предоставление государственных услуг в электронном виде.

3. Обобщены и систематизированы существующие проблемы развития информационного обеспечения системы публичного управления ДНР и определены способы их решения, главным из которых является формирование единого информационного пространства органов государственной власти.

4. Проведенный анализ современного состояния правового и организационного обеспечения позволил выделить ключевые регуляторные и структурные проблемы ОГВ в отрасли ИТ и сфере обеспечения ИБ. Систематизация факторов, а также определение актуальных типов угроз, влияющих на безопасность государственных ИС, позволили выделить основные группы рисков безопасности, свойственных информационным средам ОГВ ДНР.

5. Исследование современных тенденций развития сферы обеспечения ИБ в ДНР позволило установить, что согласно адаптированной методике расчета с 2016 г. по 2017 г., наблюдается прирост значения индекса GCI на 0,0085, при этом в период с 2017 г. по 2020 г. его прирост не наблюдается. Указанная динамика с учетом низкого уровня индекса (0,0992 в 2020 г.) относительно нормативного значения, которое находится в интервале от 0 до 1, указывает на замедление роста и дает основание сделать вывод о том, что общегосударственные подходы к обеспечению ИБ в ДНР недостаточно развиваются, в связи со сложными политическими, экономическими, кадровыми условиями и другими факторами, связанными с низким вниманием уполномоченных регуляторов к исследуемой сфере. По результатам исследования определены основные направления совершенствования исследуемой сферы с наименьшим значением индекса – организационные меры, развитие потенциала и меры в области сотрудничества. При этом оптимизация указанных направлений на общегосударственном уровне возможна только с учетом и на основе совершенствования правовых и технических мер.

6. Определено, что в существующих условиях важнейшими становятся 2 направления – формирование области обеспечения безопасности критической информационной инфраструктуры через осуществление организационно-правовых реформ и реализация организационных изменений в структуре регулирующих органов государственной власти ДНР посредством создания единого органа, в полномочия которого входят функции, определенные законодательством в данной сфере.

7. Усовершенствован методический подход к оценке рисков ИБ в ОГВ. Предложенный подход предусматривает алгоритм, базирующийся на моделировании угроз безопасности информации и оценке уязвимостей информационных активов ОГВ, и позволяет определить способы реализации выявленных угроз, уровень рисков, связанный с каждой угрозой и приоритизировать последовательность их обработки.

8. Выявлено, что усовершенствованный автором методический подход к оценке рисков позволяет решить важные задачи и является необходимым для данного исследования, однако, применяемый инструментарий не обеспечивает достаточный уровень качества данных, на базе которых определяется зрелость процессов СОИБ, в связи с чем целесообразно провести комплексную диагностику, включающую анализ и оценку процессов СМИБ.

9. В результате аналитического исследования определены ключевые направления, способы и ориентиры для разработки комплекса рекомендаций по совершенствованию существующих подходов к обеспечению ИБ в ОГВ ДНР.

Основные результаты главы опубликованы в научных трудах автора [183; 203].

ГЛАВА 3. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО СОВЕРШЕНСТВОВАНИЮ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

3.1. Концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти

Как было определено в теоретическом и обосновано в аналитическом разделах, эффективный, релевантный и комплексный подход к обеспечению ИБ в ОГВ базируется на нормативно-правовом поле, в котором четко определены полномочия ответственных регуляторов, требования, порядки, процедуры, санкции за неисполнение требований законодательства и многое другое. Поэтому ключевым этапом, инициирующим оптимизацию сферы обеспечения ИБ в ОГВ, является формирование эффективной организационно-правовой базы, заключающееся в разработке, принятии и имплементации в практическую плоскость положений НПА.

В данном исследовании разработаны направления поддержки и развития СОИБ в ОГВ, которые разделены по уровню их реализации на государственный – верхний уровень и уровень ОГВ – нижний, что обусловлено существующим состоянием развития институциональной и законодательной базы, а также невозможностью провести определенные реформы непосредственно в ОГВ без создания поддерживающих данные мероприятия условий на государственном уровне. Под условиями необходимо понимать обеспечение профильными ОГВ стабильной институциональной структуры с прозрачной правовой базой, эффективным распределением функций и полномочий в сфере обеспечения ИБ,

регуляторными механизмами и иными областями, необходимыми для оптимизации процесса информатизации ОГВ.

Структуризация направлений, способствующая систематизации процессов по оптимизации вышеперечисленных условий, представлена в виде концепции совершенствования СОИБ в ОГВ (далее – Концепция) (рисунок 3.1). Предложенная Концепция представляет собой комплексный подход к проведению эффективных преобразований в ОГВ с использованием инструментария совершенствования нормативного правового поля, оценки рисков, диагностики и стандартизации процессов обеспечения ИБ, направленных на повышение зрелости информационных сред ОГВ. Реализуется Концепция, главным образом, за счет разработки нормативно-правового поля, распределения и перераспределения функций и полномочий в сфере обеспечения ИБ, а также на базе существующего законодательства ДНР.

Для достижения поставленной цели в представленной Концепции разработан комплекс мероприятий по реализации структурных изменений нормативного правового, организационного и технического характера, что обеспечит инициацию формирования системных подходов к обеспечению ИБ на государственном уровне, а также создаст условия по развитию существующих подходов к обеспечению ИБ в ОГВ.

Важнейшим направлением на общереспубликанском уровне, по мнению автора, является разработка и принятие законов и подзаконных НПА, касающихся обеспечения безопасности критической информационной инфраструктуры, т.к. формирование и развитие данной области позволит создать системы безопасности наиболее значимых для ОГВ объектов критической информационной инфраструктуры, а также обеспечить возможность реализации контрольно-надзорных функций и полномочий за формированием и развитием СОИБ в ОГВ. Одновременно с этим, как было отмечено в аналитическом разделе, крайне важным для развития процесса информатизации ОГВ, является разработка и принятие недостающих законов и подзаконных НПА в рамках существующего законодательства в области создания и обеспечения безопасности государственных ИС.

Рисунок 3.1 – Концепция совершенствования СОИБ в ОГВ [разработано автором]

Первоочередным мероприятием, необходимым для формирования и развития системного подхода к обеспечению ИБ в ОГВ и нормативного закрепления указанных на рисунке 3.1 принципов и задач при определении основ развития исследуемой сферы, в рамках исполнения положений, указанных в Законе ДНР «О безопасности» № 04-IНС от 12.12.2014, а также гармонизации нормативного правового поля ДНР и РФ, является разработка и принятие Стратегии национальной безопасности ДНР и Доктрины информационной безопасности ДНР.

Отсутствие эффективных подходов к регулированию и контрольно-надзорной деятельности за обеспечением безопасности государственных ИС обуславливает необходимость формирования центра компетенций в сфере обеспечения ИБ, в задачи которого будет входить экспертная координация и поддержка процессов при совершенствовании СОИБ в ОГВ. Поэтому инициация реформ, способствующих внедрению комплексного подхода к обеспечению ИБ в ОГВ, включающего диагностику, оценку рисков, управление инцидентами безопасности, а также эффективный контроль за обеспечением ИБ в ОГВ, требует создания специального Единого государственного центра координации ОГВ в сфере обеспечения ИБ (далее – ЕГЦК).

Также, важно отметить, что, одним из ключевых прогнозируемых результатов настоящей Концепции является создание условий для формирования единого информационного пространства ОГВ ДНР и государственной системы управления ИБ, что позволит стандартизировать, унифицировать и повысить общегосударственный уровень обеспечения ИБ при оптимизации ресурсных затрат на создание, развитие и обеспечение безопасности информационных сред ОГВ. Как было отмечено, формирование и развитие области обеспечения безопасности критической информационной инфраструктуры охватывает все наиболее значимые объекты информационных сред ОГВ. Поэтому именно данная область, по мнению автора, должна стать краеугольной при совершенствовании СОИБ в ОГВ. В таблице 3.1 представлен комплекс базовых мероприятий по совершенствованию СОИБ в ОГВ в рамках реализации настоящей Концепции.

Таблица 3.1 – Комплекс базовых мероприятий по совершенствованию СОИБ в ОГВ ДНР в рамках реализации Концепции [разработано автором]

Мероприятие	Задачи	Ожидаемый эффект
Общегосударственный уровень		
Разработка Стратегии безопасности и Доктрины ИБ ДНР	1. Разработка и принятие Стратегии безопасности ДНР. 2. Разработка и принятие Доктрины информационной безопасности ДНР.	Инициация реформ в сфере обеспечения ИБ, создание условий для развития законодательства
Создание Единого государственного координационного центра ОГВ в сфере обеспечения ИБ	1. Разработка и принятие постановления Правительства ДНР «О Едином государственном центре координации органов государственной власти в сфере обеспечения информационной безопасности». 2. Выделение финансирования на создание ЕГЦК из Республиканского бюджета.	Инициация формирования системного подхода к обеспечению ИБ в ОГВ
Разработка и принятие ряда подзаконных нормативных правовых актов и законов	1. Разработка и принятие подзаконных НПА, для Законов: «Об информации и информационных технологиях» № 71- IНС, «Об электронной подписи», № 60- IНС, «О персональных данных» № 61- IНС от 19.06.2015 и др. 2. Разработка недостающих законов в сфере обеспечения ИБ, в частности: Закона «О коммерческой тайне», «О техническом регулировании», «О лицензировании отдельных видов хозяйственной деятельности и др.	Совершенствование процессов регулирования области создания и обеспечения безопасности государственных ИС и информатизации в целом.
Разработка и принятие ряда законов и подзаконных нормативных правовых актов ДНР в области обеспечения безопасности критической информационной инфраструктуры ОГВ	1. Разработка и принятие Закона ДНР «О безопасности критической информационной инфраструктуры ДНР». 2. Разработка и принятие Закона «О внесении изменений в отдельные законодательные акты ДНР в связи с принятием Закона «О безопасности критической информационной инфраструктуры ДНР». 3. Разработка и принятие Закона «О внесении изменений в УК ДНР и УПК ДНР в связи с принятием Закона «О безопасности критической информационной инфраструктуры». 4. Разработка и принятие ряда подзаконных НПА к Закону ДНР «О безопасности критической информационной инфраструктуры ДНР»	1. Формирование системы регулирования области обеспечения безопасности критической информационной инфраструктуры в ОГВ ДНР. 2. Распределение необходимых полномочий и функций в области обеспечения безопасности критической информационной инфраструктуры ОГВ ДНР. 3. Формирование СОИБ значимых объектов критической информационной инфраструктуры в ОГВ ДНР.
Уровень органов государственной власти		
Оценка рисков ИБ в ОГВ	Выявление и приоритизация актуальных угроз и рисков ИБ в ОГВ.	Оценка ключевых активов, мер и средств обеспечения ИБ
Диагностика СОИБ в ОГВ	Анализ состояния ключевых процессов СОИБ в ОГВ, выработка рекомендаций по оптимизации существующих подходов.	1. Оценка процессов ИБ в ОГВ. 2. Формирование планов по оптимизации СОИБ в ОГВ.
Создание систем безопасности критической информационной инфраструктуры ОГВ	1. Совершенствование процессов защиты критической информационной инфраструктуры ДНР на основе вышеуказанных процедур и требований законодательства. 2. Осуществление контроля степени защищенности значимых ИС в ОГВ 3. Формирование системы управления инцидентами значимых объектов критической информационной инфраструктуры ОГВ.	1. Создание систем безопасности значимых объектов критической информационной инфраструктуры в ОГВ. 2. Создание системы управления инцидентами ИБ в ОГВ.

Необходимость принятия Закона «О безопасности критической информационной инфраструктуры» обусловлена отсутствием единых требований ИБ к значимым объектам информационных сред ОГВ, а также отсутствием единой государственной системы управления ИБ в ОГВ. В рамках устранения существующих проблем в сфере обеспечения ИБ необходимо привести основные цели принятия Закона ДНР «О безопасности критической информационной инфраструктуры ДНР», которыми должны стать: обеспечение единой политики в сфере обеспечения ИБ, установление обязательных требований к системам безопасности значимых объектов информационных сред ОГВ, подтверждение соответствия выполнения требований законодательства, стандартизация и совершенствование подходов к обеспечению ИБ в ОГВ.

Наряду с указанным Законом предлагается разработать и принять также Законы:

– Закон ДНР «О внесении изменений в отдельные законодательные акты ДНР в связи с принятием Закона ДНР «О безопасности критической информационной инфраструктуры ДНР»;

– Закон ДНР «О внесении изменений в Уголовный кодекс ДНР и Уголовно-процессуальный кодекс ДНР в связи с принятием Закона «О безопасности критической информационной инфраструктуры ДНР».

Целесообразность разработки данных Законов обусловлена необходимостью создания уголовных и административных санкционных механизмов за неисполнение требований законодательства, а также ужесточения режима секретности сведений о мерах по обеспечению безопасности критической информационной инфраструктуры. Принятие Закона ДНР «О безопасности критической информационной инфраструктуры», а также указанных выше Законов будет способствовать совершенствованию подходов к обеспечению ИБ и гармонизации нормативных правовых полей ДНР и РФ.

Формированию и развитию систем безопасности критической информационной инфраструктуры в ОГВ способствует разработка и принятие комплекса подзаконных НПА, которые образуют систему организации и

стандартизации процессов, методов, инструментов и подходов, обеспечивающих разработку, ввод в действие, контроль исполнения, поддержание в актуальном состоянии, совершенствование, оценку эффективности мер и средств обеспечения ИБ значимых объектов критической информационной инфраструктуры в ОГВ (Приложение К).

Глава ДНР по аналогии с Президентом РФ может определять: основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры; уполномоченные органы в области защиты критической информационной инфраструктуры и иных задач, связанных с системой управления инцидентами ИБ значимых объектов в исследуемой области. Правительство ДНР по аналогии с Правительством РФ может устанавливать: показатели критериев значимости объектов критической информационной инфраструктуры, сроки категорирования и порядок осуществления государственного контроля в указанной области.

Согласно проведенному анализу, выбор важнейших отраслей критической информационной инфраструктуры может включать в себя следующие: государственное управление, здравоохранение, науку, энергетическую, металлургическую, оборонную, транспортную, горнодобывающую, пищевую промышленность, агропромышленную, отрасль коммуникаций и связи и финансово-бюджетную.

Субъектами критической информационной инфраструктуры являются государственные органы, государственные учреждения, юридические лица и (или) индивидуальные предприниматели ДНР, которым принадлежат объекты критической информационной инфраструктуры, функционирующие в вышеуказанных отраслях. В свою очередь, объектами критической информационной инфраструктуры являются: информационные системы, информационно-телекоммуникационные сети, а также автоматизированные системы управления субъектов критической информационной инфраструктуры.

Важно отметить, что общемировые «лучшие практики» создания эффективных СОИБ подразумевают разбиение информационных активов на

категории с целью надлежащего (достаточного и не избыточного) определения комплекса требований для данных активов. С этой целью предлагается внедрить в ОГВ процедуру категорирования информационных активов. Модель определения категорий значимости в рамках гармонизации нормативного поля ДНР целесообразно определить аналогичной модели РФ.

Первоочередные меры, направленные на защиту критической информационной инфраструктуры ОГВ ДНР, позволяющие сформировать базовое понимание наличия в ОГВ значимых объектов, а также угроз и рисков ИБ, связанных с возможным нарушением их функционирования должны включать мероприятия по инвентаризации и категорированию при дальнейшем создании и обеспечении функционирования систем безопасности значимых объектов.

В рамках категорирования объекту критической информационной инфраструктуры присваивается категория значимости, являющаяся характеристикой, позволяющей отделить объекты, для которых требования законодательства в указанной области не являются обязательными (не отнесенные к значимым), от тех, для которых, возможное наступление негативных последствий может привести к значимым для государства последствиям (значимые объекты). Данные последствия определяются на основе показателей критериев, связанных с воздействием на:

– социальную значимость: возможность нанесения ущерба жизни и здоровью людей; прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи; отсутствие доступа к государственной услуге;

– политическую значимость: возможность причинения ущерба интересам ДНР в вопросах внутренней и внешней политики);

– экономическую значимость: возможность причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам ДНР;

– экологическую значимость: воздействие на окружающую среду;

– значимость для обороны, безопасности государства и правопорядка.

Здесь стоит отметить, что для ОГВ характерна социальная, политическая и экономическая значимость, однако, в рамках выполнения контрольных и надзорных функций за деятельностью подведомственных государственных предприятий, могут быть определены и другие категории объектов, свойственные субъектам критической информационной инфраструктуры.

Предлагается определить следующие категории значимости объектов: минимальный, базовый и усиленный. В соответствии с разрабатываемым законодательством присваивание категорий зависит от степени возможных последствий в результате инцидентов ИБ для значимых объектов. В том случае, если объекту критической информационной инфраструктуры присвоена одна из установленных категорий, он переходит в разряд значимых и к нему должны быть применены установленные законодательством требования.

При категорировании выявляются объекты критической информационной инфраструктуры, определяются риски для данных объектов и определяется необходимость создания систем безопасности для них. Категория значимости, определяющая целевой уровень безопасности объектов, устанавливается субъектом критической информационной инфраструктуры, который образует постоянно действующую комиссию по категорированию с пересмотром процедуры раз в 5 лет. По окончанию категорирования в ОГВ начинается этап создания систем безопасности значимых объектов критической информационной инфраструктуры. Комплекс мероприятий, направленных на создание и развитие систем обеспечения безопасности критической информационной инфраструктуры в ОГВ, приведен в Приложении Л.

Как было отмечено, современное общество находится на беспрецедентном уровне развития и проникновения в жизнь человека технологической составляющей, при котором особое значение имеет упорядочивание механизмов государственного управления с целью устранения угроз и минимизации рисков ИБ. В связи с этим, с учетом имеющегося массива правовых и организационных проблем целесообразность структурных реформ видится автору оптимальным решением.

Этап создания ЕГЦК, напрямую подчиненному Администрации Главы ДНР, является одной из важнейших предлагаемых реформ в рамках настоящей Концепции. Главной задачей данного органа является координация и экспертная поддержка ОГВ в вопросах обеспечения ИБ [221]. Принимая во внимание вышеизложенное, с учетом анализа нормативного правового поля ДНР, а также проведения сравнительного анализа в рамках изучения полномочий регуляторов РФ в сфере обеспечения ИБ, основные направления деятельности ЕГЦК представлены в таблице 3.2.

Таблица 3.2 – Основные направления деятельности и задачи ЕГЦК [разработано автором]

Направление	Основные задачи
Разработка проектов НПА в сфере обеспечения ИБ	– формирование концепций по гармонизации законодательства в сфере обеспечения ИБ; – разработка проектов НПА в сфере обеспечения ИБ (в частности, касающихся обеспечения безопасности критической информационной инфраструктуры).
Анализ и оценка СОИБ в ОГВ	– проведение диагностики СОИБ в ОГВ; – проведение оценки рисков ИБ в ОГВ;
Контроль, повышение качества	– контроль ОГВ на предмет соответствия законодательству в области обеспечения безопасности критической информационной инфраструктуры. – координация вопросов создания, поддержки и развития СОИБ в ОГВ.
Управление инцидентами ИБ в ОГВ	– координация ОГВ в области управления инцидентами ИБ; – осуществление организационных и технических работ по обнаружению, предотвращению и реагированию на инциденты ИБ в ОГВ.
Экспертная поддержка	– помощь правоохранительным органам в расследовании инцидентов ИБ; – экспертная помощь в вопросах обеспечения ИБ ОГВ, организациям и гражданам.
Защита цифровых прав граждан	– защита ПД граждан (консультативная юридическая помощь); – юридическая помощь в области защиты авторских прав, консультативная и иная юридическая помощь, сопровождение процессов, связанных с защитой ПД.
Повышение квалификации	– создание системы повышения квалификации для ответственных за ИБ сотрудников ОГВ; – создание обучающих курсов для граждан ДНР.
Развитие образовательных подходов	– взаимодействие с учебными заведениями ДНР по формированию образовательных программ; – проведение семинаров, конференций, мастер-классов и др.
Научные исследования	– написание научных работ в сфере обеспечения ИБ; – взаимодействие с учеными ДНР и РФ в рамках совершенствования подходов к обеспечению ИБ в ДНР.

Указанные функции могут быть эффективно реализованы с учетом наличия профильных компетенций и четкого распределения функциональных обязанностей ЕГЦК. Поэтому, с целью систематизации функционала и выполнения указанных выше задач, предлагается следующая организационная структура ЕГЦК и основные функции его подразделений (рисунок 3.2).

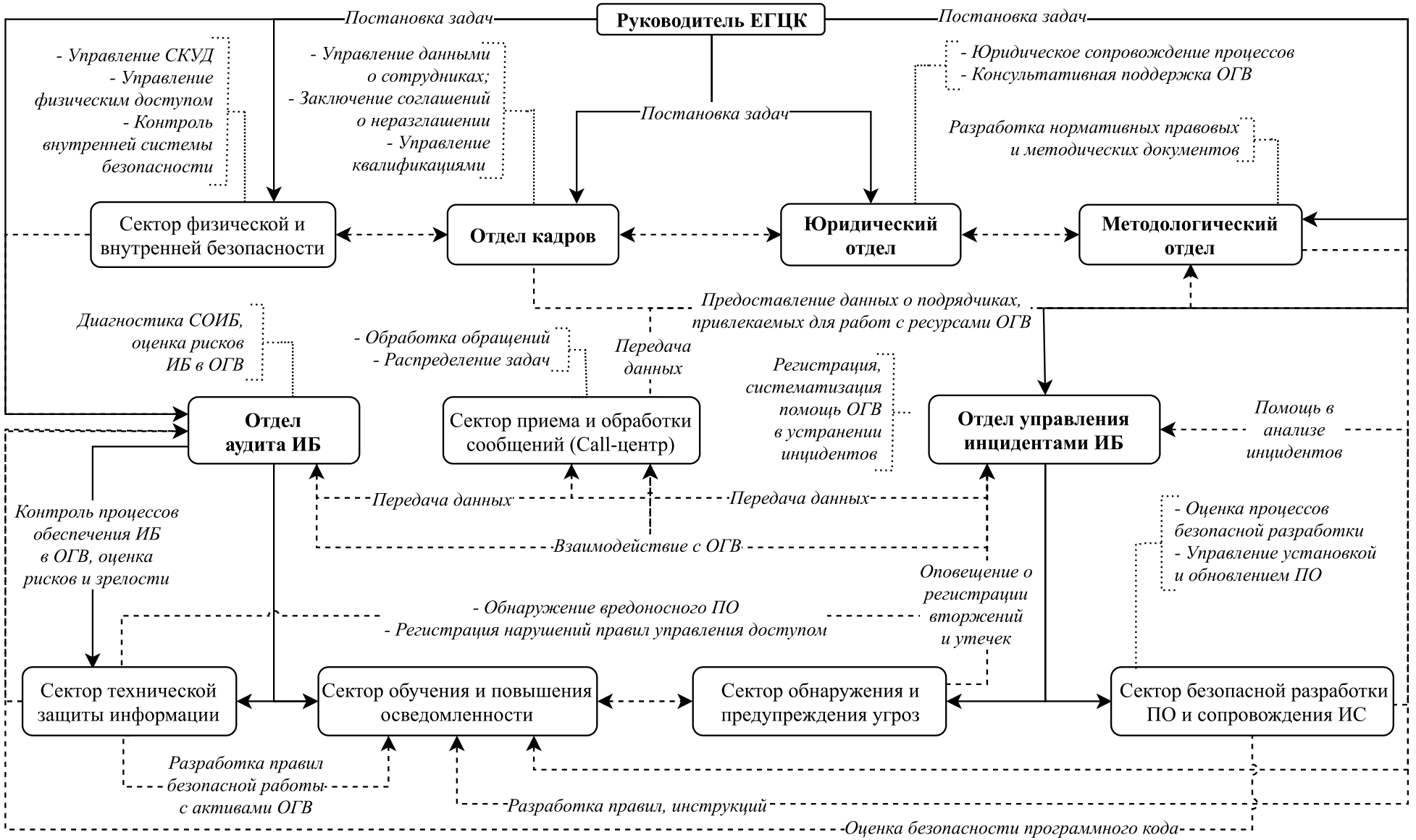

Рисунок 3.2 – Организационная структура ЕГЦК и основные функции его подразделений [разработано автором]

В рамках функционального взаимодействия ЕГЦК с субъектами ИБ ДНР предполагается развитие подходов к обеспечению ИБ всех субъектов за счет систематизации функций в рамках единой организации, предполагающей скоординированное с вышестоящими структурами сотрудничество в рамках обеспечения ИБ ОГВ и других субъектов взаимодействия (рисунок 3.3).

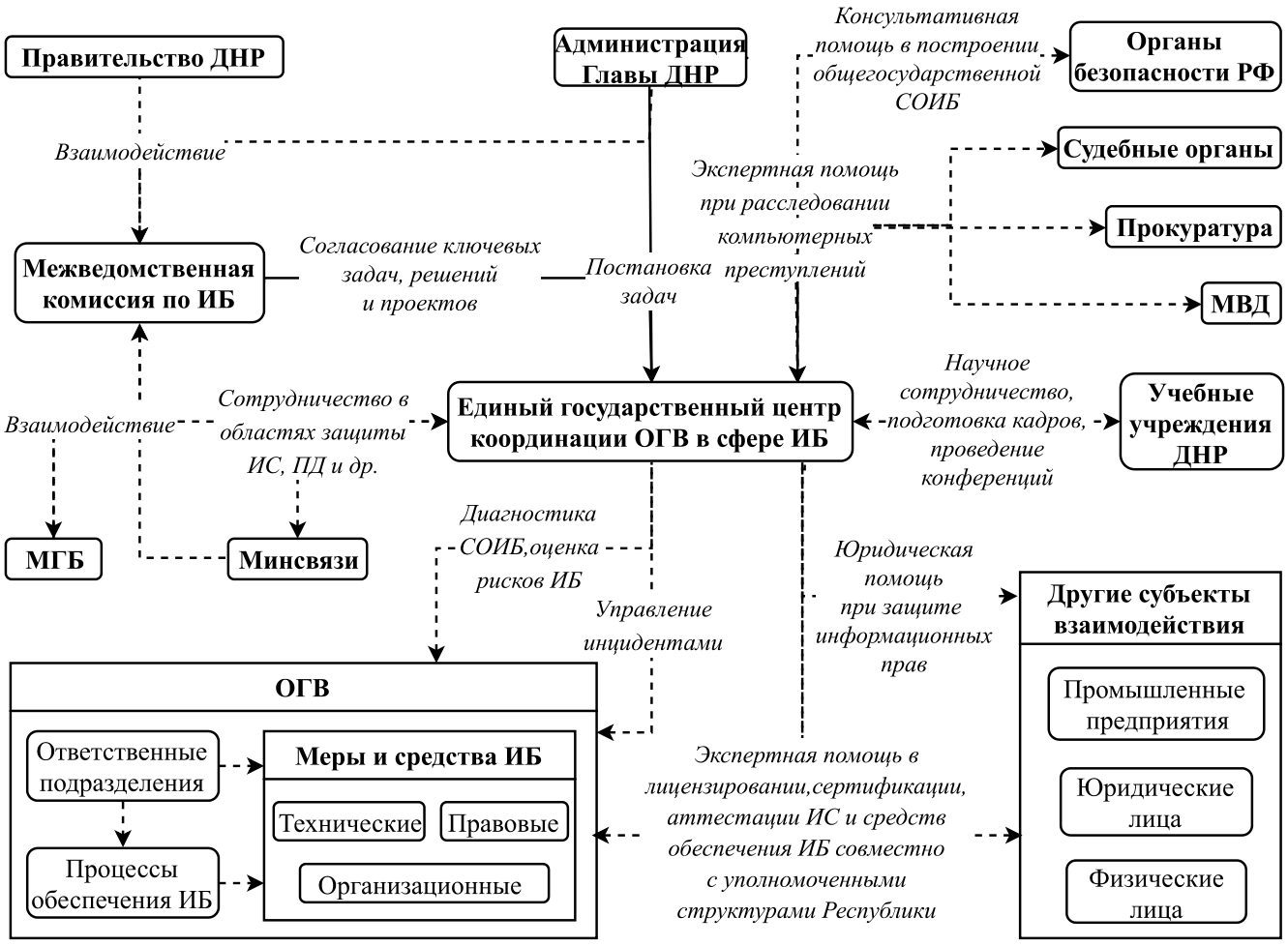

Рисунок 3.3 – Схема функционального взаимодействия ЕГЦК с ключевыми субъектами обеспечения ИБ в ДНР [разработано автором]

Межведомственная комиссия по ИБ ДНР, созданная в 2019 г., может стать координационной платформой по выработке согласованных решений, синхронизирующей стратегическое видение развития сферы обеспечения ИБ на уровне ключевых государственных регуляторов (Администрации Главы ДНР, Правительства ДНР, МГБ ДНР и Министерства связи ДНР). В дальнейшем

согласованные в Межведомственной комиссией по ИБ ДНР решения формализуются указанными регуляторами в рамках реализации своих функций и полномочий [192].

При выработке комплексного подхода к установлению информационного взаимодействия по вопросам обеспечения ИБ между образовательными учреждениями, государством и бизнесом, ЕГЦК может выступать эффективным посредником, выделяющим целевые группы участников, формирующим совокупность требований, организуя конференции, занимаясь переподготовкой кадров, разрабатывая целевые программы и др.

Все документы, формируемые ЕГЦК, согласовываются с Администрацией. Главы ДНР и при необходимости обсуждаются на Межведомственной комиссии по ИБ ДНР. Важно также конкретизировать функции ЕГЦК по разработке методического обеспечения, в число основных направлений которого входят:

– политики и регламенты организации СМИБ в ОГВ;

– политики и регламенты организации систем безопасности значимых объектов критической информационной инфраструктуры;

– политики и регламенты, способствующие систематизации порядка управления инцидентами ИБ в ОГВ;

– политики и регламенты выполнения основных функций по обеспечению ИБ структурными подразделениями ОГВ в рамках управления инцидентами ИБ;

– меры и способы обеспечения ИБ, способствующие предотвращению и (или) снижению негативного воздействия от инцидентов ИБ в ОГВ;

– порядок скоординированного взаимодействия работников ответственных структурных подразделений ОГВ по управлению инцидентами ИБ в ОГВ;

– порядок скоординированного взаимодействия ОГВ и ЕГЦК;

– признаки, на основе которых производится обнаружение угроз безопасности информации, атак и (или) регистрация инцидентов ИБ, связанных с их проведением;

– порядок действий ответственных за ИБ подразделений ОГВ, связанных с обеспечением ИБ при ликвидации последствий инцидентов ИБ (регламенты обработки инцидентов) и др.

Главной задачей ЕГЦК является способствование совершенствованию СОИБ в ОГВ, поэтому важно сформировать перечень предоставляемых органом сервисов (услуг), которые можно разбить на 3 группы:

1. Сервисы управления инцидентами ИБ – разработаны для ответов на запросы о помощи, создания отчётов об инцидентах ОГВ и реагирования на любые угрозы атаки на СОИБ в ОГВ, а также обработки инцидентов и факторов их возникновения, где факторами могут выступать: сведения о процессах или произошедших событиях, полученные от ОГВ, а также файлы или объекты, найденные в ИС ОГВ, которые могли быть вовлечены в исследование или атаку на информационные активы, или использовались для компрометации мер и (или) средств обеспечения ИБ. Главной целью данной группы сервисов является совершенствование подходов по обнаружению, предотвращению и реагированию на инциденты ИБ.

2. Профилактические сервисы – услуги по улучшению состояния инфраструктуры ОГВ и процессов СОИБ прежде, чем произойдет или будет зафиксирован инцидент или любое другое событие. Главными целями данной группы сервисов является: поддержка уровня СОИБ в ОГВ, повышение осведомленности ответственных за обеспечение ИБ в ОГВ подразделений, избежание инцидентов ИБ и снижение ущерба от их последствий.

3. Сервисы управления зрелостью СОИБ – сервисы, предназначенные для комплексного анализа и совершенствования мер, средств и процессов ИБ в ОГВ. Главными целями данных сервисов являются: организация процессов диагностики, оценки рисков ИБ и др. процессов, способствующих анализу и оптимизации СОИБ в ОГВ.

Формирование комплекса сервисов является частью процесса совершенствования СОИБ в ОГВ. Указанные сервисы с учетом должной компетенции кадров ЕГЦК помогут заложить прочный фундамент для

оптимизации СОИБ в ОГВ. Здесь важно конкретизировать перечень сервисов, предоставляемых в рамках указанных групп (таблица 3.3).

Таблица 3.3 – Сервисы, предоставляемые ЕГЦК [разработано автором]

Сервис	Описание
1	2
Сервисы управления инцидентами ИБ	
Анализ инцидентов ИБ	Мониторинг, анализ и оценка всей доступной информации и вспомогательных доказательств или особенностей, связанных с инцидентами ИБ с целью определения масштаба инцидентов, объёма причиненного ущерба, их природы, а также формирования рекомендации для реагирования на них. ЕГЦК может использовать результаты анализа уязвимостей или факторов инцидентов, для того чтобы понять и предоставить наиболее полный и своевременный анализ инцидентов, анализируя действия по их осуществлению и последствий их реализации для определения взаимосвязей, тенденций, шаблонов, или следов злоумышленников.
Обработка инцидентов ИБ	Получение, сортировка и определение приоритетов при обработке инцидентов, реагирование на запросы и отчёты, а также анализ инцидентов, а также осуществление следующих действий: – принятие мер по защите атакованных систем и сетей; – предоставление решения и стратегии уменьшения рисков ИБ; – поиск результатов и особенностей деятельности злоумышленников; – анализ сетевого трафика; – исправление или восстановление систем и др.
Сбор юридической информации	Сбор, сохранение, документирование и анализ сведений о рисках ИБ для информационных активов ОГВ проводимые с целью определения их изменений и содействия в сборе и анализе цепочек событий, приведших к инцидентам ИБ. Проводится с учетом документирования цепочки доказательств сохранности информации, с целью допуска ее законного предоставления в суде.
Отслеживание, трассировка, определение сценариев реализации	Отслеживание источника проникновения злоумышленника или определение систем, к которым он имеет доступ. Даная работа может осуществляться ЕГЦК совместно с правоохранительными органами, интернет-провайдерами и другими организациями и включает в себя, в частности: отслеживание или трассировку путей проникновения злоумышленника в поражённую систему и относящуюся к ней сеть, анализ использованных систем для получения доступа и источников возникновения инцидентов, а также определение других сетей и систем, через которые возможен данный доступ. Данный сервис также может включать установление личности злоумышленника.
Сервисы обнаружения и предотвращения вторжений	Подразделения ЕГЦК, предоставляющие эту услугу, анализируют существующие журналы систем обнаружения и предотвращения вторжений, оценивают и применяют ответные действия, на события, произошедшие в результате их срабатывания, распространяют оповещения в соответствии с составленным заранее Соглашениям (SLA), или требованиями законодательства.
Реагирование на инциденты	Содействие и консультация ОГВ, потерпевших от атак, с целью восстановления после инцидентов ИБ. Предоставление непосредственной поддержи для реагирования и восстановления после инцидентов, анализ и организация восстановления и исправления поражённых систем. Данный сервис включает полный комплекс мероприятий, которые необходимы в случае возникновения инцидента.
Профилактические сервисы	
Анализ развития технологий, техник и тактик осуществления атак	Отслеживание появления и наблюдение за развитием новых технических средств, деятельностью злоумышленников и за новыми тенденциями в сфере обеспечения ИБ. Исследования включают судебные постановления и законодательные акты, информацию о социальных или политических угрозах в сфере обеспечения ИБ, технологиях, взаимодействие с полномочными органами в сфере обеспечения ИБ, с отраслью науки. В результате ЕГЦК разрабатывает методические и рекомендательные документы по совершенствованию СОИБ в ОГВ.
Разработка средств ИБ	Разработка и внедрение новых, специфичных для конкретной области деятельности, инструментов (систем и сервисов), направленных на совершенствование СОИБ в ОГВ.

Продолжение таблицы 3.3

1	2
Настройка и сопровождение инструментария, приложений, инфраструктуры и сервисов ИБ	Выдача рекомендаций о том, как с точки зрения ИБ лучше настроить и поддерживать функциональность сервисов ИБ, приложений, операционных систем и всей информационной инфраструктуры ОГВ. Кроме выдачи рекомендаций, ЕГЦК по запросу проводит обновление настроек и поддержку инструментов и сервисов ИБ (систем обнаружения и предупреждения вторжений, систем сканирования и мониторинга, сетевых экранов, виртуальных частных сетей, систем аутентификации и др.).
Оповещение и предупреждение	Оповещение о вторжениях, предупреждения об уязвимостях и рекомендации по обеспечению ИБ в ОГВ, а также распространение информации описывающей атаки злоумышленников, уязвимости ИБ, попытки вторжения, компьютерные вирусы и рекомендованные действия для реагирования. Оповещение, предупреждение, или рекомендации отсылаются, как реакция на конкретную проблему с целью оповещения ОГВ о данной деятельности и предоставления инструкций по защите или восстановлению их систем.
Распространение информации, связанной с ИБ	Повышение осведомлённости, в частности распространения: 1. Рекомендаций по совершенствованию СОИБ в ОГВ. 2. Шаблонов документации, способствующей внедрению «лучших практик» организации ИБ. 3. Информации о разработке и распространении обновлений. 4. Информации о современных уязвимостях, угрозах и связанных с ними рисков ИБ. 5. Глобальной статистики и тенденций по направлению управления инцидентами ИБ 6. Общих рекомендации по обеспечению ИБ и др.
Сервисы управления зрелостью СОИБ	
Разработка проектов НПА в сфере обеспечения ИБ	Взаимодействие с ответственными регуляторами на предмет необходимости разработки НПА, методических, др. документов и их содержания с последующим формирование необходимых проектов документов, и передачей их на согласование.
Оценка рисков ИБ, диагностика СОИБ	Диагностика, оценка рисков ИБ в ОГВ, способствующая повышению способности ОГВ по оценке реальных угроз безопасности информации и позволяющая максимально точно получить оценку мер, средств и процессов обеспечения ИБ, основываясь на «лучших практиках», требованиях законодательства, стандартах РФ в сфере обеспечения ИБ.
Консультирование, экспертная поддержка	Выдача рекомендаций ОГВ и др. субъектам критической информационной инфраструктуры по внедрению мер, средств и процессов обеспечения ИБ. Подготовка методических рекомендаций. Выдача рекомендаций и помощь в разработке процессов менеджмента ИБ (СМИБ). Консультирование по иным вопросам обеспечения ИБ.
Инвентаризация значимых объектов ОГВ	Сбор сведений о результатах присвоения объектам критической информационной инфраструктуры категорий значимости, либо обоснований отсутствия их присвоения. Ведение реестра значимых объектов критической информационной инфраструктуры.
Обучение и подготовка	Предоставление ОГВ информации о проблемах обеспечения ИБ на семинарах, конференциях, курсах повышения переквалификации, и др. формах взаимодействия.
Научные исследования	Взаимодействие с научными учреждениями ДНР, а также учеными в отрасли ИТ и сфере обеспечения ИБ на предмет написания аналитических статей, монографий, диссертаций и др. научных работ.
Оценка зрелости информационных систем	Оценка систем, приложений и других ресурсов на предмет обеспечения необходимого уровня обеспечения ИБ. Сервис может представлять собой процесс оценки, аттестации или сертификации (совместно с профильными организациями), в зависимости от стандартов и норм, применяемых в ОГВ или устанавливаемых уполномоченными регуляторами.

По итогам ликвидации последствий инцидентов ОГВ своими силами либо с помощью сил специалистов ЕГЦК проводит оценку эффективности мер и средств ИБ в порядке, определенном соответствующими методическими рекомендациями через диагностику, оценку рисков или иной инструмент, и, при необходимости,

дорабатывает внедренные подходы к обеспечению ИБ и реагированию на инциденты безопасности. Также по результатам ликвидации последствий инцидентов безопасности, вызванных компьютерными атаками, силами ответственных подразделений ЕГЦК совместно с ответственными сотрудниками ОГВ при необходимости проводится анализ способов проведения атаки, уязвимостей, использованных злоумышленником, и, при необходимости, дополнительные исследования, способствующие уточнению аспектов совершившегося инцидента. На основе результатов проведенного анализа, вид выявленной атаки и аспекты ее реализации включаются в число типовых с последующей разработкой соответствующих методических рекомендаций либо обновления существующих.

В рамках взаимодействия ОГВ с ЕГЦК осуществляется обмен сведениями о присвоении категорий значимости объектам критической информационной инфраструктуры, о защищенности данных объектов и иных информационных систем, а также об инцидентах безопасности, признаках угроз безопасности информации и иными сведениями, необходимыми для систематизации данных о состоянии СОИБ в ОГВ и повышении осведомленности сотрудников ответственных подразделений ОГВ. Этапы создания ЕГЦК представлены в таблице 3.4.

Таблица 3.4 – Этапы создания ЕГЦК [разработано автором]

Этап	Содержание
1	2
Разработка концепции создания и развития ЕГЦК	Формирование стратегического плана, содержащего цели, задачи и поэтапный план развития.
Разработка операционной и организационной модели ЕГЦК	Формирование операционной и организационной модели (в т.ч. организационно-штатной структуры) с учетом требований, заложенных в законодательстве ДНР.
Разработка архитектуры центра ЕГЦК	1. Формирование, согласование и утверждение архитектуры ЕГЦК (информационной инфраструктуры, инструментов, ресурсов для обеспечения функциональной деятельности и др. 2. Разработка сервисов, предоставляемых ЕГЦК с привязкой к бизнес-процессам, системам и ИТ-инфраструктуре.
Определение списка предоставляемых сервисов	На начальном этапе целесообразно оптимизируя штат ЕГЦК предоставлять только некоторые из основных сервисов. После пилотного запуска список может быть расширен.

Продолжение таблицы 3.4

1	2
Формализация процессов, процедур, систематизация функциональной деятельности	1. Определение последовательности технологических процессов, порядка действий и технических процедур. 2. Разработка необходимой нормативной и правовой документации для создания ЕГЦК.
Разработка и принятие стратегии развития	1. Финансовая модель (электронные сервисы ОГВ – в т. ч. государственные услуги должны работать круглосуточно, что говорит о необходимости предоставления в рабочие часы ЕГЦК услуг в полном объеме, а в нерабочее время услуги должны предоставляться по требованию. Услуги для ОГВ будут предоставляться бесплатно, а возможность предоставления услуг иным потребителям будет рассмотрена в течение пилотного и оценочного этапов). 2. Модель доходов (во время пилотного этапа ЕГЦК может финансироваться из Республиканского бюджета. С пилотного этапа по оценочный будет рассмотрен вопрос привлечения дополнительного финансирования, включая возможность продажи услуг внешним потребителям). 3. Организационная модель, штат сотрудников (определение организационной модели, штата сотрудников и уровня их подготовки). 4. Создание, согласование и принятие стратегии развития (подготовка экономического обоснования и плана проекта, а также расчет затрат на наладочные работы и расчет эксплуатационных расходов).
Разработка ключевых показателей эффективности	1. Разработка и согласование с уполномоченными регуляторами показателей (факторов) для оценки эффективности процессов и сервисов ЕГЦК. 2. Внедрение показателей в систему оценки процессов.
Формирование инфраструктуры ЕГЦК	Формирование ИТ-инфраструктуры, систем и ресурсов, обеспечивающих процессы ЕГЦК.
Внедрение разработанных процессов	Начало функционирования ЕГЦК. Реализация функций и полномочий организации.
Внедрение организационных и технических средств управления инцидентами	Внедрение средств мониторинга, средств взаимодействия, средств создания виртуальных частных сетей между ОГВ и ЕГЦК и др. средств, способствующих оптимизации процессов обнаружения, реагирования и устранения инцидентов ИБ в ОГВ.
Контроль эффективности внедренных процессов	1. Разработка показателей оценки эффективности. 2. Формирование отчетов в соответствии с разработанными показателями.
Подготовка, переподготовка кадров	Совершенствование уровня подготовки ответственных сотрудников ЕГЦК и ОГВ

Создание ЕГЦК в рамках реализации настоящей Концепции, позволит оптимизировать процессы взаимодействия органов-регуляторов в сфере обеспечения ИБ, Правительства ДНР и других ОГВ, повысить эффективность, зрелость и оперативность принятия управленческих решений при обеспечении ИБ

в ОГВ, а также в целом повысит уровень зрелости подходов к обеспечения ИБ в ОГВ.

Настоящая Концепция поможет заложить прочный фундамент в совершенствование СОИБ в ОГВ и позволит начать решать следующие задачи:

– координация и помощь ОГВ в сфере обеспечения ИБ;

– оценка и поддержание уровня обеспечения ИБ в ОГВ;

– систематизация государственных подходов к обеспечению ИБ.

– упрощение правовой и организационной интеграции общегосударственных СОИБ ДНР и РФ;

– разработка и совершенствование НПА в сфере обеспечения ИБ;

– помощь ОГВ, гражданам и бизнесу в вопросах обеспечения ИБ;

– выявление признаков, предупреждение и ликвидация последствий инцидентов безопасности, определение их источников, методов, способов, средств осуществления и векторов направленности, а также разработка мер, способов и средств детектирования и минимизации рисков ИБ от указанных угроз безопасности информации;

– формирование и поддержание в актуальном состоянии детализированной информации о значимых объектах критической информационной инфраструктуры ОГВ ДНР;

– прогнозирование ситуации и предупреждение инцидентов в сфере обеспечения ИБ в ДНР, выявление, оценка и прогнозирование рисков ИБ;

– формирование системы взаимодействия ЕГЦК с ОГВ и иными организациями при управлении инцидентами ИБ;

– организация и проведение научно-исследовательских работ по разработке и применению мер, средств и методов управления инцидентами ИБ в ОГВ;

– осуществление мероприятий по обеспечению подготовки и повышению квалификации кадров в сфере обеспечения ИБ в ОГВ;

– мониторинг и анализ степени защищенности значимых ИС ОГВ на всех этапах их создания, функционирования и модернизации;

– разработка проектов НПА и методических документов в сфере обеспечения ИБ;

– совершенствование оперативно-тактического взаимодействия сил и средств ОГВ в сфере обеспечения ИБ на общегосударственном уровне.

Таким образом, автором разработан теоретико-методический подход к совершенствованию СОИБ в ОГВ ДНР за счет разработки концепции совершенствования системы, которая, в отличие от существующих, базируется на системных процессно-ориентированных принципах управления, повышении эффективности применения комплексного подхода к обеспечению ИБ в ОГВ, инструментарии оценки рисков и диагностики, объектной модели регулирования и оптимизации механизмов государственного управления в исследуемой сфере.

Предлагаемый концептуальный подход представляет собой эффективные преобразования общегосударственной СОИБ через формирование системного подхода к обеспечению общегосударственной ИБ ДНР и процессного подхода к развитию СОИБ в ОГВ. Формирование предложенных регуляторных и организационных требований и механизмов совершенствования СОИБ в ОГВ обеспечит создание комплексного подхода к обеспечению ИБ в ОГВ, а также создаст условия, способствующие развитию информатизации и созданию единого информационного пространства ОГВ.

3.2. Формирование архитектуры единого информационного пространства органов государственной власти

Формирование единого информационного пространства ОГВ ДНР является одной из важнейших задач информатизации ОГВ, т.к. способствует всесторонней оптимизации имеющихся ресурсов и возможностей, и позволяет максимально

эффективно обеспечить внедрение комплексного подхода к обеспечению ИБ в ОГВ. Данная задача должна реализовываться через централизацию ключевых государственных ИС, повышение уровня их функциональной совместимости, внедрение в рамках единой инфраструктуры стандартизированных процессов управления ИБ, унификации технологической политики ДНР, а также формирования регламентов взаимодействия и методических рекомендаций, способствующих гармонизации процессов формирования единого информационного пространства ОГВ ДНР.

Под Единым информационным пространством ОГВ ДНР (далее – ЕИП), понимается совокупность информационных систем и элементов ИТ-инфраструктур ОГВ, позволяющих на основе единых принципов и правил обеспечивать безопасное информационное взаимодействие ОГВ, организаций и граждан при их равнодоступности к открытым информационным ресурсам, а также максимально полного удовлетворения их информационных потребностей и защиты информационных прав на всей территории государства.

По сравнению с действующим в настоящий момент порядком, при котором каждое ведомство самостоятельно решает задачи в отрасли ИТ и сфере обеспечения ИБ, применяя свой набор решений, предлагаемый подход позволяет минимизировать описанные в аналитическом разделе риски ИБ, уменьшить затраты на формирование государственных ИС и ИТ-инфраструктур, улучшить их качество, а также обеспечить прозрачные механизмы реализации технологической политики государства.

Ключевыми целями создания ЕИП является формирование:

– единых механизмов взаимодействия ОГВ, граждан и др. субъектов информационного пространства, при предоставлении государственных услуг и реализации функций;

– единой технологической политики в ОГВ;

– единой архитектуры информационного пространства ОГВ;

– единых механизмов функционирования государственных ИС;

– единой государственной системы управления ИБ в ОГВ.

Основными задачами создания ЕИП являются:

1. Создание единой методологической базы через:

– формирование единых правил, стандартов, концепций, моделей, методических рекомендаций и руководств развития ИС и ИТ-инфраструктур ОГВ;

– формирование законодательства, необходимого для создания государственных ИС и инфраструктурных элементов ЕИП;

– разработку единых методологий оценок качества государственных ИС;

– разработку единых методологий оценки ИБ в ОГВ.

2. Создание единых процессов разработки, создания, эксплуатации и обеспечения безопасности ИС и ИТ-инфраструктур ОГВ через:

– разработку высокоуровневой целевой и функциональной архитектуры ЕИП;

– разработку архитектуры основных систем и субъектов ЕИП;

– разработку информационной и процессной архитектуры ЕИП;

– разработку интеграционной и межведомственной архитектуры ЕИП;

– разработку архитектуры каждой информационной системы электронного правительства, включенной в ЕИП;

– разработку архитектуры государственной системы управления ИБ в ОГВ;

– разработку архитектуры безопасности ЕИП.

3. Обеспечение организационной поддержки через:

– разработку ключевых субъектов информационного взаимодействия ЕИП;

– формирование организационной структуры для управления процессами создания и функционирования ЕИП;

– определение и реализацию финансовой поддержки деятельности, направленной на создание и функционирование ЕИП;

– расчет ожидаемых экономических выгод и рисков от создания ЕИП.

4. Создание единой информационно-технологической инфраструктуры через:

– разработку ключевых ИС и инфраструктурных элементов электронного правительства, входящих в ЕИП;

– разработку и внедрение единых правил и технологий, способствующих созданию и функционированию ИС и ИТ-инфраструктур ОГВ.

– разработку и внедрение единых правил и технологий, способствующих обеспечению интероперабельности ИС и ИТ-инфраструктур ОГВ;

Достижение приведенных целей через реализацию указанных задач позволит:

– создать условия для разработки и внедрения ключевых ИС и инфраструктурных элементов электронного правительства;

– оптимизировать затраты на разработку, внедрение и поддержку ИС и инфраструктурных элементов в ОГВ (за счет сокращения и структуризации затрачиваемых ресурсов, использования свободного ПО и др.);

– повысить отказоустойчивость ИТ-инфраструктур ОГВ;

– унифицировать архитектурные подходы, методики и инструменты создания и развития ИС и ИТ-инфраструктур ОГВ;

– сократить сроки создания и повысить качество функционирования ИС и ИТ-инфраструктур ОГВ;

– повысить уровень технической поддержки и обслуживания государственных ИС и ИТ-инфраструктур (за счет открытости технологий, использования облачных технологий и др.);

– обеспечить соответствие ИС и ИТ-инфраструктур ОГВ единым требованиям и правилам обеспечения ИБ;

– создать единые процессы и автоматизированные механизмы обеспечения ИБ в ОГВ.

В рамках реализации подготовительных мероприятий по созданию ЕИП важно сформировать архитектуру основных субъектов информационного взаимодействия, их функций и ключевых систем данного пространства, обобщенная схема которой приведена на рисунке рисунок 3.4.

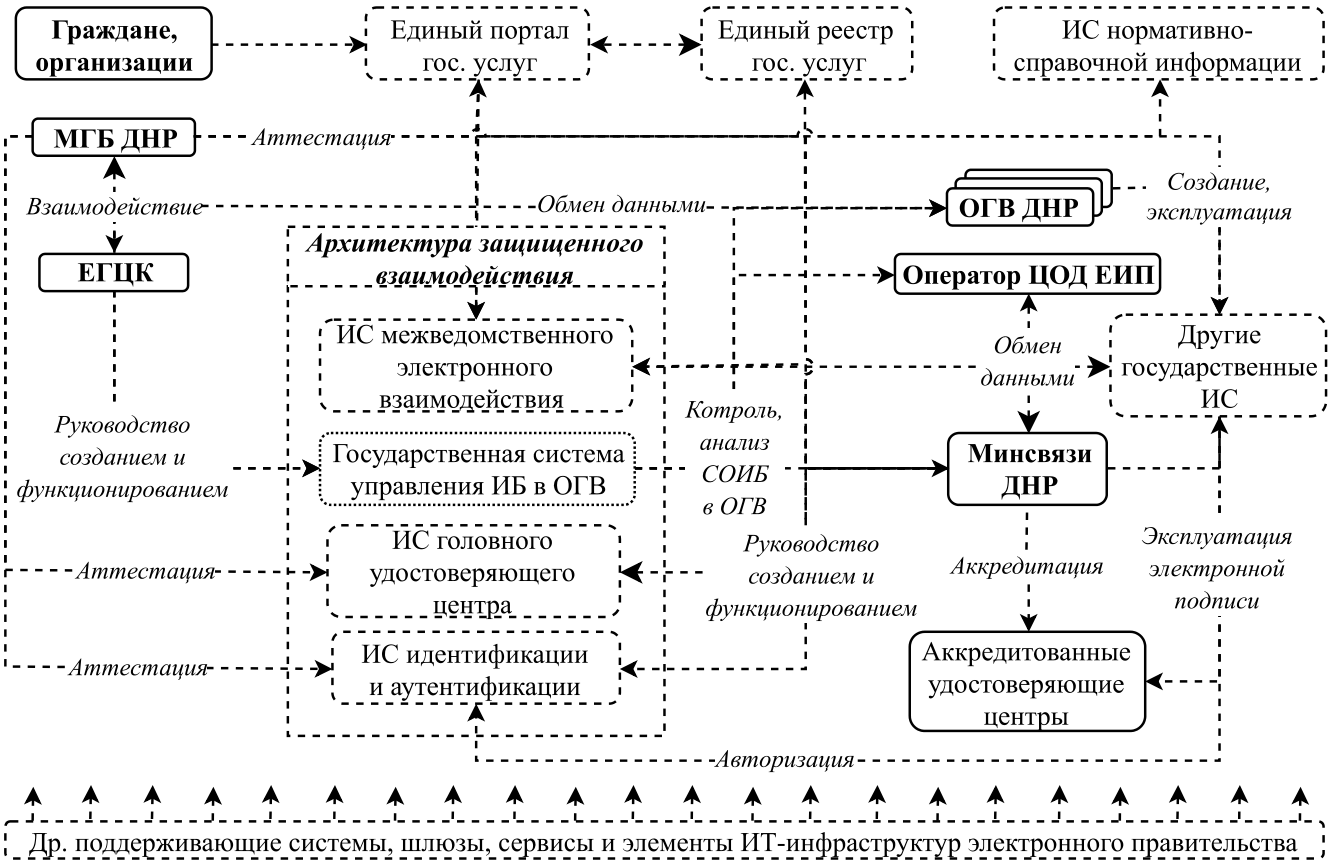

Рисунок 3.4 – Архитектура основных систем и субъектов ЕИП [разработано автором]

Предложенная архитектура учитывает важнейшие системы электронного правительства, обеспечивающие защищенный централизованный обмен данными между ОГВ и гражданами, позволяя создать единый механизм предоставления государственных услуг в электронном виде.

Ключевым элементом ЕИП является ИС головного удостоверяющего центра, позволяющая использовать электронную подпись в рамках взаимодействия между ОГВ, бизнесом и гражданами, обеспечивая юридическую значимость документов, циркулирующих в ИС, входящих в ЕИП. Главной задачей ИС головного удостоверяющего центра является обеспечение информационно-технологической поддержки отношений при использовании электронных подписей, возникающих между субъектами ЕИП в процессах формирования и оказания государственных услуг в электронном виде и

осуществления межведомственного взаимодействия. Реализуется данная задача путем предоставления субъектам ЕИП и ИС ОГВ совокупности сервисов проверки и подтверждения аутентичности и достоверности электронных подписей с использованием аккредитованных удостоверяющих центров.

В рамках ЕИП применяется квалифицированная электронная подпись, предоставляющая унифицированный механизм формирования единого набора мер, реализуемых с целью обеспечения равного уровня доверия вне зависимости от того, какая организация из числа участников ЕИП предоставляла услуги электронной подписи и какими технологиями она при этом пользовалась. Данный набор мер в рамках ЕИП реализуется Министерством связи ДНР с помощью ИС головного удостоверяющего центра, а также множеством аккредитованных удостоверяющих центров, обеспечивающих поддержку процессов управления сертификатами ключей проверки электронной подписи.

Также одной из важнейших систем ЕИП должна стать ИС идентификации и аутентификации, предоставляющая пользователям единый механизм авторизации в различных государственных ИС, обеспечивая централизованный контроль использования ПД и их актуальности в различных ИС, что значительно повышает общегосударственный уровень обеспечения ИБ. Функции основных систем целевой архитектуры ЕИП представлены в таблице 3.5.

Важнейшей системой, обеспечивающей информационное взаимодействие между ОГВ в целях предоставления государственных услуг, исполнения государственных функций в электронной форме, а также защищенного автоматизированного обмена данными в рамках ЕИП является ИС межведомственного электронного взаимодействия, позволяющая кратно увеличить качество всех процессов обмена данными. Помимо функционирования в рамках выполнения задач электронного правительства, данная система должна стать ключевой платформой, позволяющей осуществлять межведомственное взаимодействие между ОГВ и ЕГЦК в рамках единой государственной системы управления ИБ.

Таблица 3.5 – Ключевые системы единого информационного пространства ОГВ ДНР [разработано автором]

Системы	Основные задачи	Основные функции	Положительный эффект от внедрения
1	2	3	4
Единый портал государственных услуг	1. Обеспечение доступа к государственным и муниципальным услугам в электронной форме	Доступ к предназначенным для распространения с использованием сети интернет сведениям о государственных услугах, размещенным в государственных ИС	Обеспечение возможности предоставления государственных услуг и реализации функций ОГВ в электронном виде в формате «одного окна»
Единый реестр государственных услуг	2. Обеспечение субъектов ЕИП консолидированной, актуальной и достоверной информацией о предоставляемых государственных услугах	Сбор и хранение информации о порядке предоставления государственных услуг, а также обеспечения единства и непротиворечивости нормативно-справочной информации	
ИС межведомствен-ного электронного взаимодействия	Обеспечение защищенного обмена данными между ОГВ в электронном виде	Передача документов, сведений, запросов и информации о ходе выполнения запросов между государственными ИС	1.Повышение качества государственных услуг и функций. 2.Обеспечение единого механизма информационного взаимодействия субъектов ЕИП в электронной форме. 3.Оптимизация процессов обработки данных.
ИС головного удостоверяющего центра	Создание инфраструктуры, позволяющей осуществлять выдачу сертификатов ключей квалифицированной электронной подписи	1. Создание, выдача, контроль, и проверка сертификатов ключей проверки электронных подписей аккредитованных удостоверяющих центров. 2. Обеспечение осуществления подтверждения подлинности квалифицированных электронных подписей. 3. Ведение реестров квалифицированных сертификатов ключей проверки электронных подписей.	Создание единого пространства доверия, позволяющего осуществлять юридически значимый обмен документами и данными между субъектами ЕИП
ИС нормативно-справочной информации	Обеспечение формирования, хранения актуализации, и единообразного представления данных, содержащихся в государственных ИС и использующихся ОГВ, в т.ч. при межведомственном взаимодействии	1. Формирование единого каталога нормативно-справочной информации (наборов справочников, словарей, классификаторов, стандартов, регламентов и др.). 2. Формирование единого реестра базовых государственных информационных ресурсов. 3. Предоставление пользователям системы инструментов поиска сведений в различных государственных ИС за счет обеспечения информационного взаимодействия с ИС электронного правительства.	Обеспечение единообразного представления данных, содержащихся в государственных ИС и использующихся в деятельности ОГВ при исполнении государственных функций и предоставлении государственных услуг в электронном виде

Продолжение таблицы 3.5

1	2	3	4
ИС идентификации и аутентификации	Обеспечение единого унифицированного санкционированного способа авторизации при осуществлении доступа субъектов информационного взаимодействия к информации, содержащейся в государственных и иных ИС	1. Обеспечение идентификации, аутентификации и авторизации субъектов ЕИП в государственных ИС. 2. Управление идентификационными данными (ведение регистров физических, юридических лиц, ОГВ, организаций, ИС должностных и др. лиц). 3. Предоставление в государственные ИС идентификационных данных (в том числе сведений о полномочиях по доступу к ресурсам государственных ИС) субъектов ЕИП. 4. Поддержка различных уровней достоверности идентификации пользователей системы: упрощённая, стандартная, или подтвержденная учетные записи. 5. Поддержка различных методов аутентификации: по паролю, по электронной подписи, двухфакторная аутентификация.	1.Сокращение времени разработки государственных ИС и затрат, связанных с обеспечением сервисов идентификации и аутентификации пользователей, созданием и поддержкой пользовательской базы. 2.Обеспечение единого уровня безопасности пользовательских данных в государственных ИС, контроль использования ПД. 3.Повышение качества доступа к государственным ИС. 4.Повышение эффективности межведомственного взаимодействия за счет единых стандартов, форматов и сервисов осуществления авторизации. 5.Эволюционное развитие инфраструктуры доступа ЕИП, не затрагивающее жизненный цикл подключенных государственных ИС.
Государственная система управления ИБ в ОГВ	Создание единой организационно-технической системы централизованного управления СОИБ в ОГВ на базе ЕГЦК	1. Мониторинг и анализ защищенности ИС и ИТ-инфраструктур ЕИП (анализ сетевого трафика потоков данных для поиска сведений, которые могут быть полезны для выявления неисправностей и отклонений от штатного функционирования указанных элементов ЕИП). 2. Идентификация уязвимостей и угроз безопасности ИС и ИТ-инфраструктур ОГВ. 3. Сбор и систематизация аналитических данных, используемых для управления рисками ИБ. 4. Обработка данных о событиях/инцидентах ИБ с непрерывной обратной связью. 5. Сбор свидетельств компьютерных преступлений для реконструкции инцидентов ИБ, произошедших с государственными ИС.	Создание единого централизованного автоматизированного механизма управления событиями, уязвимостями инцидентами ИБ, рисками, диагностикой и иными процессами управления ИБ в ОГВ, способствующего всестороннему совершенствованию процессов координации, взаимодействия и обеспечения ИБ в ОГВ и повышению уровня защищенности государственных ИС и ИТ-инфраструктур

Указанные системы, при эффективном их использовании, позволяют обеспечивать единые правила и требования, предъявляемые к разработке, описанию и взаимодействию информационных ресурсов государства, а также доступность актуальной и достоверной информации для внешних систем, в том числе для эффективного решения аналитических и управленческих задач, предоставления государственных услуг и выполнения функций ОГВ.

Стоит отметить, что одним из ключевых элементов обеспечения безопасности государственных ИС является их аттестация. С учетом этого факта, важно отметить, что большинство сервисов ИБ центра обработки данных ЕИП должно быть выведено за пределы прикладного ПО и может быть аттестовано отдельно от него, поэтому изменения в прикладном ПО (в рамках выполнения требований, необходимых для прохождения аттестации) будут необходимы только при его существенной переработке, при этом объем испытаний в данном случае будет минимальным, что прямо влияет на оптимизацию всех видов ресурсов как при аттестации, так и при проведении иных видов оценок защищенности ИС и ИТ-инфраструктур, входящих в ЕИП.

Важнейшим преимуществом в рамках предложенной архитектуры является возможность сегментации соответствующих контуров безопасности инфраструктуры центра обработки данных ЕИП таким образом, чтобы определенному сегменту соответствовала определенная категория государственных ИС с обеспечением доступа определенным категориям пользователей. Данная возможность существенно оптимизирует процессы аттестации уполномоченными регуляторами государственных ИС, снижая ресурсы на проведение испытаний и повышая уровень доверия уполномоченных структур к интегрированным в ЕИП системам.

Особый интерес для настоящего исследования представляет организация процессов управления и взаимодействия субъектов ЕИП. Обобщенная схема организации процесса управления ЕИП, приведенная на рисунок 3.5, предполагает выделение центра обработки данных ЕИП, который выполняет инфраструктурную функцию электронного правительства и, в него в

последующем может быть осуществлена поступательная миграция ключевых государственных ИС.

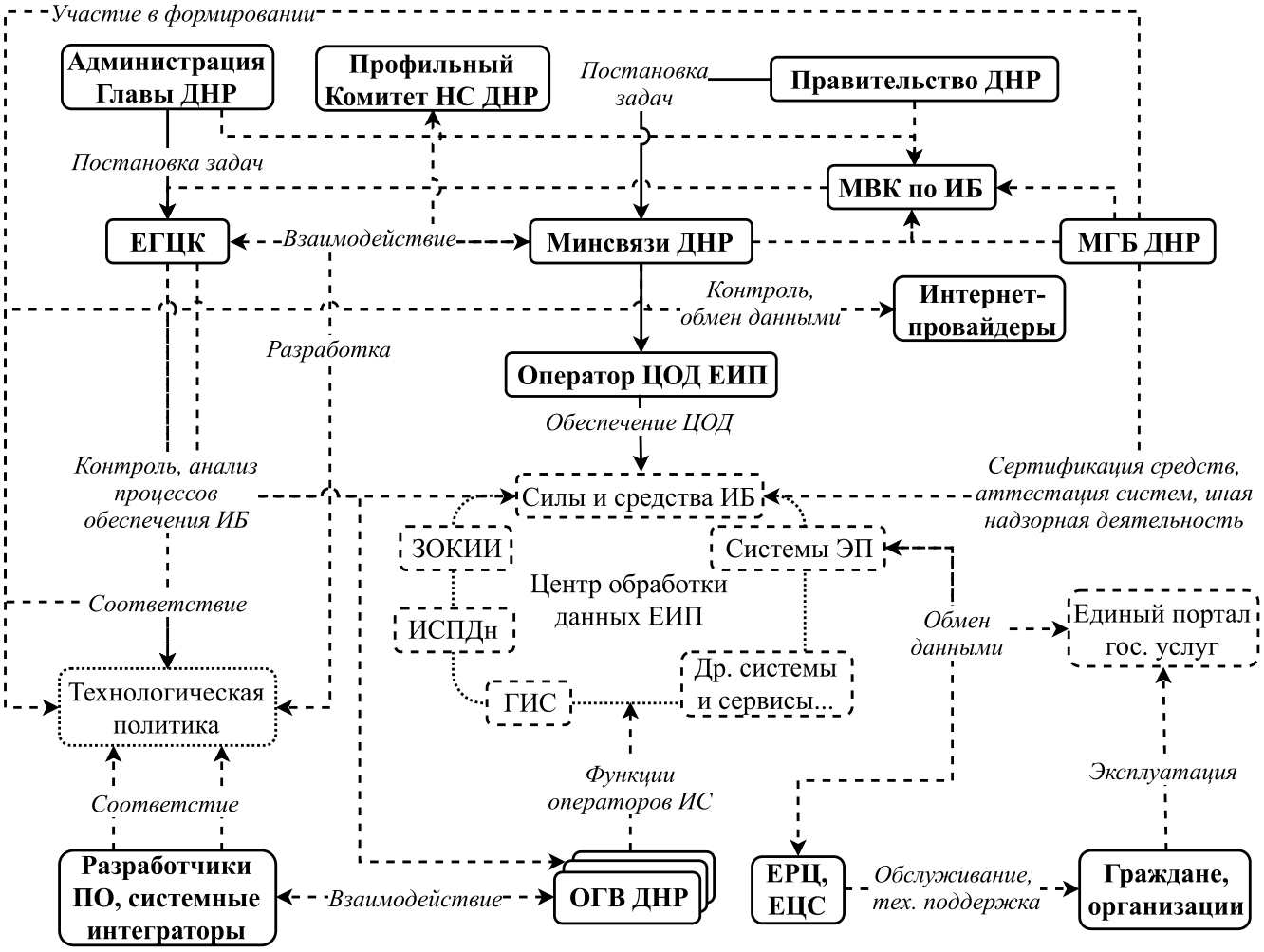

Рисунок 3.5 – Организация процесса управления ЕИП [разработано автором]

С учетом того, что Министерство связи ДНР является уполномоченным органом по реализации ключевых направлений развития информатизации и формирования электронного правительства, данный орган должен стать ключевым субъектом управления ЕИП, ответственным за формирование и развитие входящих в него ИС с последующим определением ответственных разработчиков и подведомственного Оператора центра обработки данных ЕИП, обеспечивающего поддержку функционирования интегрированных в данное

пространство систем. Также Министерство связи ДНР должно стать ответственным органом за формирование технологической политики, которой необходимо соответствовать всем разработчикам государственных ИС, системным интеграторам и иным субъектам ЕИП. Однако, комплексный подход к формированию и развитию ЕИП может быть обеспечен исключительно с задействованием всех субъектов информационного пространства ДНР (МГБ ДНР, Правительства ДНР, Главы ДНР, Народного Совета ДНР, ЕГЦК и др. ОГВ).

В рамках работы Межведомственной комиссии по ИБ ДНР, Глава ДНР, Правительство ДНР, МГБ и Минсвязи ДНР формируют стратегические согласованные решения, цели, задачи и сроки их исполнения, а также определяют ответственных за формирование и развитие правового и организационного обеспечения ИБ в ЕИП. Помимо этого, Комитетом Народного Совета ДНР по внешней политике, международным связям, информационной политике и информационным технологиям при взаимодействии с Министерством связи ведется разработка нормативного правового обеспечения, необходимого для развития ЕИП. Единые регистрационные центры и Единые центры связи ДНР могут стать платформой для обслуживания и технической поддержки граждан при предоставлении государственных услуг.

Ключевые системы ЕИП по мере их разработки интегрируются в Центр обработки данных ЕИП с целью обеспечения единого уровня безопасности, качества ИС и оптимизации ресурсов, затрачиваемых на их поддержку. Политики обеспечения качества и безопасности ИС и ИТ-инфраструктуры центра обработки данных ЕИП реализуются Оператором данного центра и должны контролироваться с помощью набора стандартизированных показателей, разрабатываемых ЕГЦК совместно с Министерством связи ДНР. При этом другими ОГВ могут формироваться корректировки политик и показателей в отрасли ИТ и сфере обеспечения ИБ, а также вноситься предложения по изменению в существующие НПА.

Как было отмечено, ответственным за обеспечение ИБ ЕИП должен стать Оператор центра обработки данных, подведомственный Министерству связи

ДНР, однако, контроль за обеспечением ИБ в рамках регулярных комплексных аудитов ИБ, оценки рисков и иных процессов, связанных с формированием, поддержкой и развитием систем безопасности государственных ИС проводят специалисты ЕГЦК. Помимо этого, ЕГЦК исполняет экспертно-консультативную роль в вопросах обеспечения ИБ и осуществляет координационные функции в ЕИП, формируя общегосударственную систему управления ИБ, а также платформу для координации и взаимодействия всех субъектов ЕИП по вопросам регистрации, расследования и обработки инцидентов ИБ в ОГВ.

Специалистами ЕГЦК совместно с Оператором центра обработки данных ЕИП и ответственными подразделениями ОГВ проводится мониторинг, регистрация инцидентов и скоординированное взаимодействие в сфере обеспечения ИБ. В рамках технологического сотрудничества осуществляемого через средства взаимодействия ЕГЦК обеспечивает доступ к методической базе, основным типам угроз безопасности информации, сценариям и способам реализации компьютерных атак, характерных для ИС ОГВ, а также к мерам, средствам и способам, способствующим предупреждению, обнаружению и ликвидация инцидентов ИБ. Инфраструктура ЕИП в рамках ролевой модели должна предоставлять сервисы для разных типов пользователей с разным уровнем доступа и набором полномочий, среди которых можно выделить категории, представленные в таблице 3.6.

В соответствии со своим ролями субъекты, включенные в ЕИП, получают доступ к различным системам, сервисам, сегментам сети и контурам передачи данных. Все уровни доступа, полномочия и порядки их реализации и контроля за процессами управления доступом подробно регламентируются во внутренних нормативных и организационно-распорядительных документах Оператора центра обработки данных, надзор за выполнением положений которых осуществляет Министерство связи ДНР. При разработке требований к ИС и ИТ-инфраструктуре ЕИП предлагается разделить сервисы ИБ на: локальные – реализуемые в каждой из ИС ОГВ в соответствии с едиными правилами и политиками и глобальные – предоставляемые инфраструктурой центра обработки данных и ЕГЦК.

Таблица 3.6 – Категории пользователей центра обработки данных [разработано автором]

Пользователи	Задача	Описание	Уровень доступа	Набор полномочий
Провайдеры данных	Обеспечение наличия в системе базовой справочной информации и ее своевременной актуализации	Сотрудники ОГВ, отвечающие за предоставление исходных данных в систему (государственные справочники, реестры и классификаторы и др. ключевые данные), а также участвующие в обмене данными	Доступ к данным соответствующих ИС на уровне чтения и записи данных в соответствии с закрепленными полномочиями с возможностью чтения и записи	Актуализация ключевых данных. Разработка, дополнение изменение моделей ключевых данных реестров и систем
Провайдеры сервисов	Поддержка сервисов предоставления услуг пользователям систем ЕИП	Разработчики государственных ИС, ответственные за обновление и поддержку сервисов систем, интегрированных в Центр обработки данных ЕИП	Доступ к сервисам и данным соответствующих ИС на уровне чтения и записи данных и приложений в соответствии с закрепленными полномочиями	Управление сервисами ЕИП (актуализация, добавление, обновление Систем на уровне приложений)
Служба поддержки инфраструктуры	Обеспечение непрерывности работы систем и сервисов ЕИП	Сотрудники оператора центра обработки данных ЕИП, осуществляющие функции мониторинга, резервного копирования, обновление систем, и др. функции, поддерживающие непрерывность работы ЕИП	Доступ к управлению инфраструктурой на физическом и сетевом уровне в соответствии с закрепленными полномочиями	Управление инфраструктурой, обработка логов, доступ к системе мониторинга инфраструктуры и сервисов
Служба обеспечения ИБ	Формирование и развитие СОИБ центра обработки данных ЕИП	Сотрудники оператора центра обработки данных ЕИП, отвечающие за внутренние процессы ИБ и взаимодействие с ЕГЦК	Доступ к специализированным средствам защиты информации (средствам обнаружения и предотвращения вторжений, защиты от утечек и др.)	Внутренний анализ уязвимостей, оценка рисков ИБ, моделирование угроз, расследование инцидентов и др. процессы обеспечения ИБ
Контролеры ИБ	Обеспечение анализа СОИБ, управление инцидентами ИБ	Сотрудники ЕГЦК, отвечающие за процессы взаимодействия с Оператором центра обработки данных при управлении инцидентами ИБ, диагностике СОИБ и иных процессов контроля ИБ	Доступ к средствам защиты информации, включенным в инфраструктуру центра обработки данных ЕИП на уровне чтения данных	Анализ средств, мер и процессов обеспечения ИБ, оценка рисков, экспертная поддержка при оптимизации СОИБ Оператора ЕИП
Аналитики данных	Проведение анализа данных, находящихся в государственных ИС	Сотрудники ОГВ или уполномоченных за надзор структур, получившие доступ к ИС с целью анализа данных в рамках выполнения функций и полномочий своего ведомства	Доступ к соответствующим ИС (на уровне данных) в соответствии с закрепленными полномочиями с возможностью чтения	Анализ, выгрузка ключевых данных. Составление аналитических отчетов в соответствии со своими функциями
Конечные пользователи	Получение доступа к государственным услугам	Граждане и организации, получающие конечный результат работы ИС в виде государственных услуг	Доступ к получению государственных услуг	Запрос государственных услуг и информации, обратная связь

Ответственные подразделения Оператора центра обработки данных ЕИП и ЕГЦК становятся в данном случае ключевыми субъектами обеспечения ИБ в ОГВ, осуществляя мониторинг соответствия требованиям ИБ и предоставляя сервисы, применяемые в рамках всех государственных ИС. В рамках описанной архитектуры формируется набор сервисов ИБ, предоставляемых ЕГЦК. Сервисы управления инцидентами ИБ, управления уязвимостями, контроля соответствия требованиям безопасности, оценки рисков ИБ и др. используют информацию на различных уровнях и являются единой системой защиты, обеспечивающей формирование комплексного подхода к совершенствованию СОИБ в ОГВ.

Приведенная система управления доступом позволяет минимизировать требования к ИБ для ИС центра обработки данных Оператора ЕИП, поскольку на прикладном уровне остается исключительно реализация логики разграничения доступа, что также крайне положительно влияет на оптимизацию ресурсов.

Важнейшим элементом предлагаемых в рамках ЕИП изменений является государственная система управления ИБ в ОГВ, архитектура которой предполагает формирование механизмов скоординированного централизованного взаимодействия ключевых субъектов обеспечения ИБ ДНР в рамках единых механизмов, которые функционируют в трех форматах: 1 – автоматизированные (через ИС межведомственного электронного взаимодействия); 2 – через телефонные линии связи; и 3 – через специальные почтовые сервера, доступ к которым имеют только уполномоченные лица субъектов ЕИП (рисунок 3.6).

Данный подход исключает необходимость вручную искать, собирать, оценивать, классифицировать, анализировать и, в конечном счете, дифференцировать и связывать с ИБ данные, полученные из многочисленных гетерогенных источников в ИТ-инфраструктуре и ИС ОГВ, с учетом автоматизации, централизации и унификации ключевых процессов, связанных с мониторингом и другими процессами обеспечения ИБ в ОГВ. Также предложенная архитектура позволяет эффективно выявлять и анализировать атаки на ключевые системы ОГВ, осуществляя непрерывный контроль безопасности через специальные выделенные каналы связи.

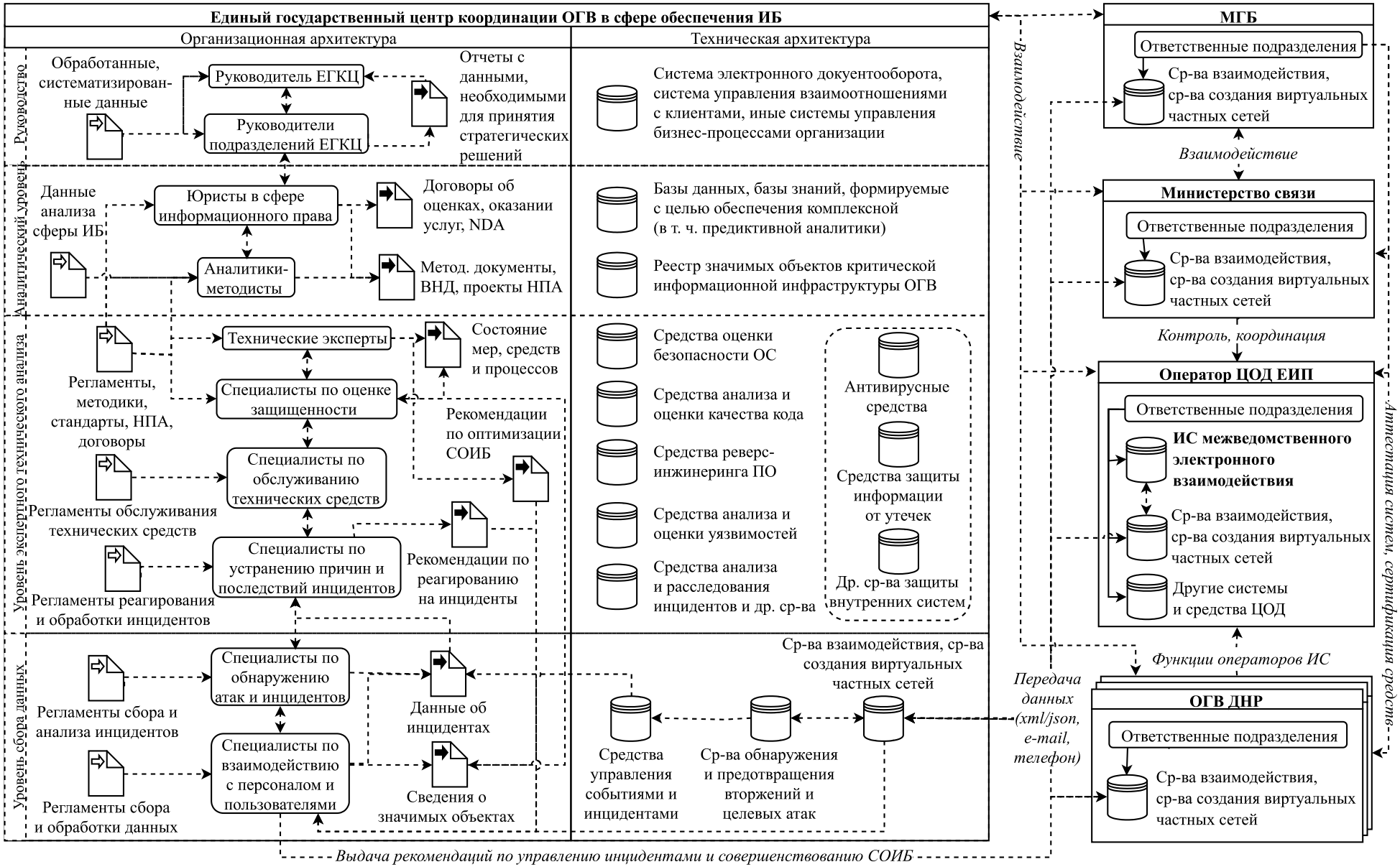

Рисунок 3.6 – Архитектура государственной системы управления ИБ в ОГВ [разработано автором]

Среда информационного взаимодействия ЕИП, формируемая информационной системой межведомственного электронного взаимодействия, а также подключенными к ней средствами взаимодействия и средствами создания виртуальных частных сетей позволяет создать платформу для защищенного автоматизированного обмена данными. Данная платформа в совокупности со средствами обнаружения и предотвращения вторжений и целевых атак, средствами управления событиями и средствами анализа, расследования инцидентов и другими средствами позволяет решить одну из основных задач комплексного обеспечения ИБ в ОГВ – задачу превентивного аудита, когда уязвимости систем к определенному типу информационно-технического воздействия будут обнаруживаться до того, как это воздействие осуществлено злоумышленниками. При этом данные процессы производятся в автоматизированном виде и на регулярной основе. Помимо этого, предложенная архитектура предполагает возможность прогнозирования и анализа рисков ИБ за счет сбора аналитических данных в рамках мониторинга и проведения оценок защищенности ИС и ИТ-инфраструктур ОГВ, что позволяет выстраивать эффективную систему управления зрелостью.

Для объединения ключевых элементов инфраструктуры ЕИП создаются коммуникационные сегменты на выделенных каналах связи, через которые ОГВ в рамках выполнения функций операторов ИС подключаются к системам центра обработки данных ЕИП через защищенные каналы связи. Формируются данные каналы связи за счет установки в инфраструктуры ОГВ и Оператора центра обработки данных ЕИП выделенных VPN-серверов, что влияет на затрату ресурсов, однако, с учетом критичности систем ЕИП, фактор минимизации рисков компрометации VPN-ключей является приоритетным.

На рисунке 3.7 представлен алгоритм взаимодействия ОГВ с ЕГЦК в рамках государственной системы управления ИБ при управлении событиями, уязвимостями и инцидентами ИБ. Приведенный алгоритм позволяет усовершенствовать ключевые процессы управления ИБ в ОГВ, оптимизируя взаимодействие органов в рамках указанных процессов.

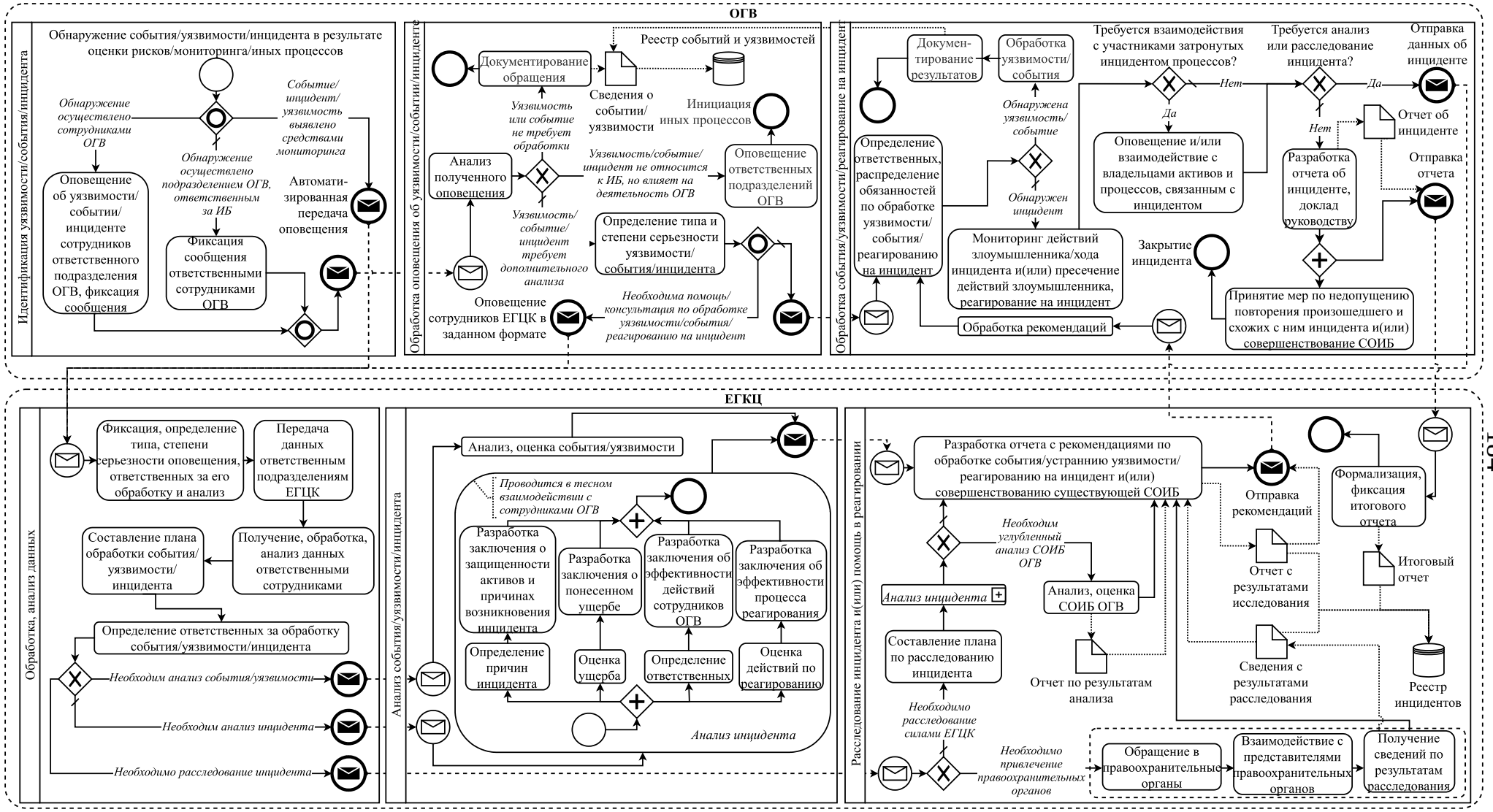

Рисунок 3.7 – Алгоритм взаимодействия ОГВ с ЕГЦК при управлении событиями, уязвимостями и инцидентами ИБ в рамках государственной системы управления ИБ [разработано автором]

Наиболее эффективное взаимодействие в рамках приведенного алгоритма возможно только при поступательном объединении ключевых объектов ЕИП. Для этого в рамках формирования ЕИП необходимо учесть следующие базовые требования к информационным средам ОГВ:

– наличие технической возможности интеграции государственных ИС с внешними сервисами: идентификации и аутентификации, криптографическими сервисами, сервисами электронной подписи и системой межведомственного электронного взаимодействия через программный интерфейс приложения (API);

– наличие технических средств мониторинга ИТ-инфраструктуры ОГВ, средств создания виртуальных частных сетей (VPN) и средств автоматизированного взаимодействия с ЕГЦК в информационной среде ОГВ;

– обеспечение организационных и технических возможностей передачи данных в ИС межведомственного электронного взаимодействия в форматах XML/JSON через каналы связи, формируемые средствами взаимодействия и средствами создания виртуальных частных сетей.

Данные, передаваемые ОГВ в ЕГЦК через ИС межведомственного электронного взаимодействия, перед конвертацией в указанные форматы должны формироваться в виде специальных карточек инцидентов, требования к структуре которых разрабатывает ЕГЦК. С целью отладки и систематизации механизмов взаимодействия ЕГЦК и Оператора центра обработки данных ЕИП обмен данными, разработка систем, интеграция, техническая поддержка и иные процессы ЕИП осуществляются в рамках, зон ответственности, определенных в договорах и регламентах взаимодействия.

В результате тесного сотрудничества ОГВ, ЕГЦК и др. субъектов ЕИП в рамках государственной системы управления ИБ в ОГВ достигается наиболее эффективная синергия, способствующая обеспечению комплексного подхода к обеспечению ИБ в ОГВ за счет совместного применения правовых, организационных мер, инструментальных средств и единых процессов. При этом предлагаемые подходы содержат следующие возможности:

– эффективная и централизованная структура управления ИБ в ОГВ;

– централизованное управление и анализ конфигурационных настроек сетевых устройств и средств защиты информации информационных сред ОГВ;

– ситуационная осведомленность уполномоченных регуляторов и ОГВ в рамках системного мониторинга государственных ИС и ИТ-инфраструктур;

– мониторинг состояния процессов обеспечения ИБ в режиме реального времени, интегрированный с требованиями по обеспечению ИБ и включающий автоматизированный контроль за состоянием информационных сред ОГВ с оповещением, уведомлением, отчетностью о выполнении требований ИБ, службой технической поддержки и другими сервисами;

– совершенствование процессов управления изменениями в информационных средах ОГВ в рамках автоматизации, централизации и унификации процессов;

– автоматизированный анализ состояния ИБ в ОГВ (сбор, агрегирование, корреляция событий и потоков данных), использование сервисов расширенной аналитики, способствующих оптимизации процессов работы с данными;

– риск-ориентированная приоритезация оповещений об опасности угроз безопасности в информационных средах ОГВ в соответствии с наиболее вероятными событиями, которые могут привести к наиболее негативным последствиям;

– совершенствование процессов обнаружения уязвимостей, событий и инцидентов ИБ, а также их анализа и расследования (за счет сокращения времени обнаружения и реагирования, интеграции с различными средствами и сервисами и др.);

– улучшенное планирование и реализация мер обеспечения ИБ при управлении рисками, соблюдении соответствия, а также при идентификации и устранение причин возникновения инцидентов ИБ;

– регулярный анализ безопасности информационных сред ОГВ, проведение оценок с предоставлением различных форм отчетов и аналитики;

– улучшенный обмен информацией в рамках единой системы управления ИБ в ОГВ, учитывающей использование синтезированных знаний и процедуры повышения осведомленности о существующих системах и процессах ИБ;

– измерение ключевых показателей эффективности СОИБ в ОГВ на основе контроля эффективности процессов управления ИБ;

– целостный подход, позволяющий комплексно рассматривать каждый элемент СОИБ в ОГВ, не фокусируясь исключительно на снижении рисков ИБ путем устранения уязвимостей, но учитывая системный анализ мер и средств обеспечения ИБ за счет непрерывного мониторинга и тесного взаимодействия всех субъектов ЕИП;

– непрерывное понимание общей ситуации с обеспечением ИБ в ОГВ, сочетающее в себе наблюдения в рамках мониторинга ИБ, внешнюю ИБ-аналитику, а также регулярный поиск уязвимостей и угроз ИБ;

– фокусный и целевой подход к формированию и развитию СОИБ в ОГВ, способствующий повышению зрелости процессов ИБ на основе системного понимания всех аспектов, связанных с функционированием информационных сред ОГВ и оптимизации расходования требуемых для обеспечения ИБ ресурсов, с учетом установленных приоритетов;

– формирование подхода к совершенствованию СОИБ в ОГВ, основанного на единых показателях ИБ, позволяющих создавать механизмы принятия быстрых, эффективных и обоснованных решений по оптимизации мер, средств и процессов ИБ;

– экспертное независимое использование информации об угрозах и уязвимостях ИБ из открытых внешних источников при анализе СОИБ в ОГВ, способствующее формированию объективного анализа и оценки мер и средств обеспечения ИБ на основе «лучших практик»;

– комплексный анализ состояния мер и средств обеспечения ИБ в ИС и ИТ-инфраструктурах ОГВ, согласованный с едиными, прозрачно интерпретируемыми регуляторами и ОГВ показателями ИБ и др.

Указанные возможности в рамках предложенных подходов могут быть обеспечены с учетом формирования эффективного плана создания ЕИП (таблица 3.7).

Таблица 3.7 – Обобщенный план создания ЕИП [разработано автором]

Стадия	Детализация
1	2
1. Разработка Концепции формирования ЕИП	Установка плана развития, целей, задач, принципов, областей действия субъектов ЕИП, зон ответственности, др. основ форсирования ЕИП.
2. Согласование	Согласование со всеми заинтересованными сторонами видения внедряемых реформ, которое соответствует и согласуется с целями всех участников ЕИП.
3. Финансирование	Определение источников, выделение финансирования из Республиканского бюджета.
4. Разработка и принятие необходимых Законов и НПА	1. Разработка и принятие Закона о внесении изменений в Закон «Об информации, информационных технологиях». 2. Разработка и принятие Закона «О государственных и муниципальных услугах». 3. Разработка и принятие приказа Министерства связи ДНР о внесении изменений в приказ Министерства связи ДНР от 16.10.2015 № 85 «Об утверждении Требований к организации мероприятий создания, развития, эксплуатации и вывода из эксплуатации государственных ИС, и дальнейшего хранения содержащейся в их базах данных информации». 4. Разработка и принятие других недостающих подзаконных НПА в отрасли ИТ и сфере обеспечения ИБ.
5. Назначение организации-Центра компетенции ЕИП	Разработка и принятие приказа Министерства связи ДНР «О создании Центра компетенций по формированию технологической архитектуре единого информационного пространства органов государственной власти ДНР»
6. Определение Оператора центра обработки данных ЕИП	Определение ответственного Оператора центра обработки данных ЕИП в соответствии с имеющимися ресурсами, поставленными целями и необходимыми к выполнению задачами.
7. Утверждение архитектурных процессов ЕИП	Разработка и принятие приказа Министерства связи ДНР «Об утверждении архитектурных процессов единого информационного пространства органов государственной власти ДНР»
8. Разработка Дорожных карт разработки ИС, включенных в ЕИП	1. Определение разработчиков ИС, включенных в ЕИП и подрядчиков, необходимых для реализации всех этапов разработки и внедрения систем. 2. Формализация этапов, сроков, ответственных за разработку и внедрения ИС, включенных в ЕИП.
9. Разработка технической документации	Разработка технических заданий, технических требований и иной сопроводительной документации для каждой ИС, включенной в архитектуру ЕИП
10. Разработка и внедрение информационных систем, входящих в электронное правительство	1. Реализация всех этапов разработки, создания и введение в эксплуатацию каждой ИС, включенных в архитектуру ЕИП. 2. Разработка соответствующей пользовательской и эксплуатационной документации и регламентов работы ответственных подразделений ЕИП. 3. Сопровождение, обеспечение функционирования инфраструктуры центра обработки данных ЕИП.
11. Доработка государственных ИС	Доработка существующих государственных ИС с целью обеспечения возможности их интеграции с ИС идентификации и аутентификации и ИС межведомственного электронного взаимодействия.
12. Обеспечение процессов интеграции ИС ЕИП в центр обработки данных	1. Разработка внутренних нормативных документов Оператора центра обработки данных ЕИП, определение и формализация ключевых процессов управления ИБ и стандартных операционных процедур, необходимых для поддержки ЕИП. 2. Выделение мощностей Оператором центра обработки данных ЕИП. 3. Интеграция ИС ЕИП в центр обработки данных.
13. Формирование среды взаимодействия в рамках ЕИП	Внедрение средств взаимодействия и средств создания виртуальных частных сетей в ИТ-инфраструктуры ОГВ с целью их интеграции в ЕИП

Продолжение таблицы 3.7

1	2
14. Внедрение государственной системы управления ИБ в ОГВ	1. Разработка плана организационных и технологических процедур по внедрению централизованной системы управления ИБ в ОГВ. 2. Внедрение государственной системы управления ИБ в ОГВ в рамках функционирования отладки организационно-технических механизмов взаимодействия всех субъектов ЕИП.
15. Оценка состояния мер, средств и процессов обеспечения ИБ в ОГВ	1. Разработка дорожной карты диагностики СОИБ и оценки рисков ИБ в ОГВ, формализация процедур. 2. Оценка рисков ИБ в ОГВ силами внутренних подразделений. 3. Диагностика СОИБ в ОГВ силами ЕГЦК.
16. Формирование системы повышения квалификации	1. Формирование системы повышения квалификации в сфере обеспечения ИБ на базе ЕГЦК. 2. Прохождение обучения ответственных сотрудников Оператора ЕИП на базе ЕГЦК. 3. Прохождение обучения ответственных сотрудников ОГВ.
17. Развитие СОИБ в ОГВ	Выполнение выданных рекомендаций ответственными подразделениями ОГВ в рамках проведенных оценок состояния СОИБ.

Ожидаемый социально-экономический эффект от создания ЕИП для граждан и ОГВ представлен на рисунке 3.8.

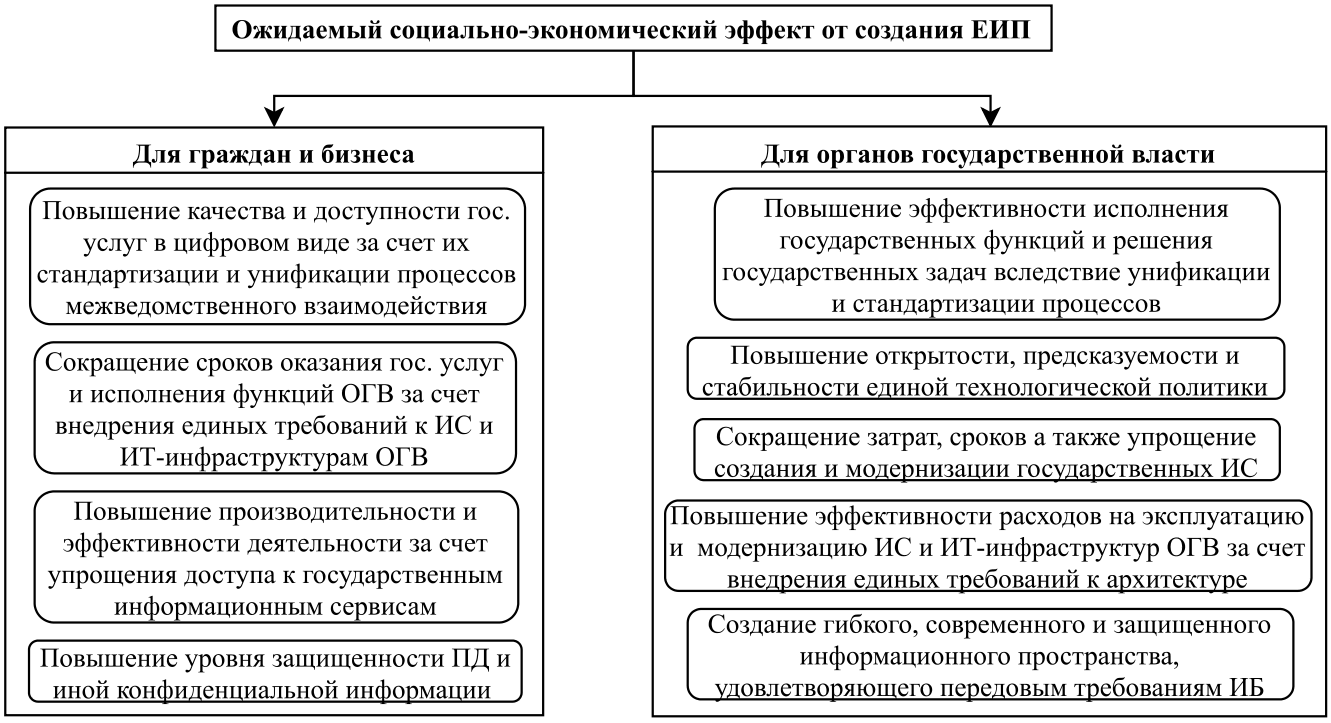

Рисунок 3.8 – Ожидаемый социально-экономический эффект от создания ЕИП [разработано автором]

В результате проведенного исследования предложены организационные подходы к формированию архитектуры единого информационного пространства

органов государственной власти за счет создания системы управления информационной безопасностью в ОГВ, что, в отличие от существующей структуры управления, позволит стандартизировать, унифицировать и обеспечить единство механизмов развития СОИБ в публичном управлении, а также оптимизировать процессы взаимодействия ОГВ в сфере обеспечения ИБ.

Указанные подходы позволят усовершенствовать процессы взаимодействия всех субъектов информационного пространства ДНР, реализуя подход, базирующийся на формировании ключевых систем электронного правительства, повышении функциональной совместимости государственных информационных систем и формировании комплексной системы управления информационной безопасностью в органах государственной власти, что позволяет усовершенствовать и стандартизировать подходы к информатизации и обеспечению информационной безопасности в органах государственной власти, а также повысить эффективность системы публичного управления и создать условия, способствующие обеспечению устойчивого развития ДНР в цифровую эпоху.

3.3. Разработка методического подхода к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти

В связи с низким уровнем зрелости общегосударственных подходов к обеспечению ИБ в ДНР необходимо решать сложности, связанные с формированием комплексного подхода к обеспечению ИБ в ОГВ. Одним из ключевых направлений совершенствования СОИБ в ОГВ является контроль за состоянием системы и оценка ее эффективности. Контроль и эффективная оценка СОИБ в ОГВ является основополагающим процессом, способствующим

оптимизации системы. Наиболее подходящим для данной оценки инструментом, позволяющим осуществлять регулярный контроль и оценку состояния мер, средств и процессов обеспечения ИБ, надзор за выполнением требований законодательства, а также позволяющим выработать эффективный поэтапный подход к совершенствованию СОИБ в ОГВ, по мнению автора, является регулярная комплексная экспертная диагностика системы, что обуславливает необходимость в разработке методического подхода.

Качественный процесс комплексной диагностики СОИБ представляет собой многоуровневый, поэтапный подход, зависящий от множества аспектов, факторов и свойств информационных сред обследуемого объекта. Поэтому с целью построения модели комплексной диагностики СОИБ в ОГВ в рамках разработки методического подхода целесообразно применить системное моделирование процессов, позволяющее обобщить и структурировать необходимые стадии проведения диагностики, выделить основные этапы, элементы и функции, а также оптимизировать качество осуществляемых при его реализации работ [222].

Цель системного моделирования процессов диагностики СОИБ заключается в проведении систематизации процессов и этапов диагностики, выявлении их взаимосвязей, определении требований к средствам, мерам и критериям принятия экспертных решений, определении требований к компетенциям и распределении обязанностей экспертов, осуществляющих диагностику. По результатам проведенного анализа предметной области сформулированы следующие ключевые задачи комплексной диагностики СОИБ в ОГВ:

– анализ уязвимостей, моделирование угроз безопасности информации;

– выявление, анализ и оценка рисков ИБ;

– оценка соответствия применяемых мер, средств и процессов обеспечения ИБ заданным требованиям законодательства и «лучших практик»;

– оценка процессов обеспечения ИБ ИТ-инфраструктуры, а также защищенности и эффективности процессов управления жизненным циклом ИС;

– оценка системы менеджмента ИБ;

– оценка процессов защиты ПД;

– формирование комплексных рекомендаций по совершенствованию мер, средств и процессов обеспечения ИБ.

В ходе анализа «лучших практик» выделены направления, позволяющие провести оценку ключевых процессов обеспечения ИБ в ОГВ. С целью формирования релевантной модели комплексной диагностики СОИБ в ОГВ использованы корреляционные связи выделенных направлений и высокоуровневых процессов обеспечения ИБ, определенных через анализ и отбор данных процессов из «лучших практик» с учетом специфики функционирования ОГВ (рисунок 3.9).

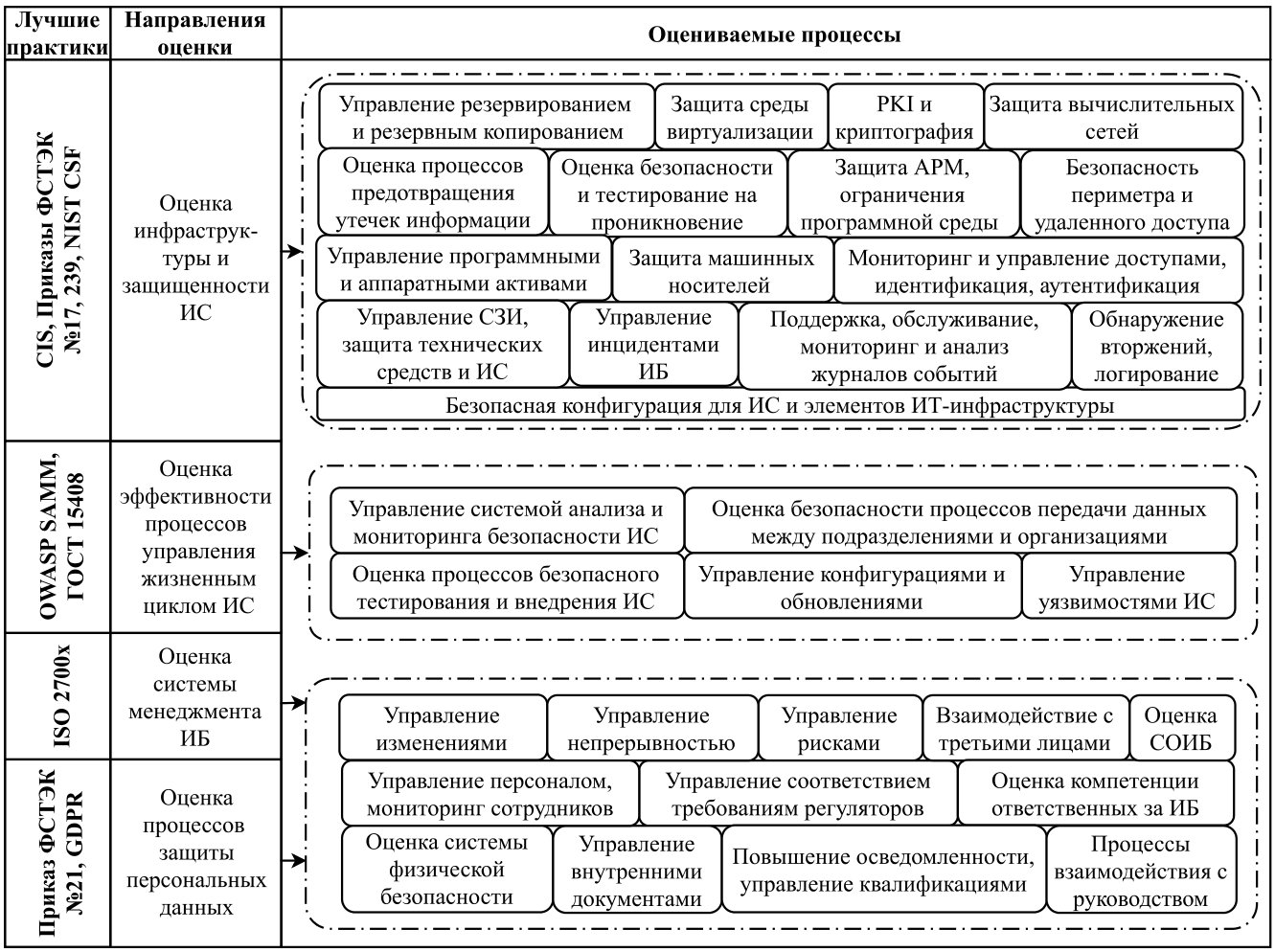

Рисунок 3.9 – Модель выборок процессов из «лучших практик» [разработано автором на основе [51; 52; 77; 83; 86; 223-225]]

Предлагается следующий перечень экспертов, привлекаемых для проведения комплексной диагностики СОИБ в ОГВ в рамках выявленных процессов:

1. Эксперт-аналитик в сфере обеспечения ИБ – специалист по формированию СМИБ, специализирующийся в организационных и управленческих процессах ИБ.

2. Эксперт-системный администратор – специалист по защите ИТ-инфраструктуры, техническим мерам и средствам обеспечения ИБ.

3. Эксперт-юрист в области информационного права – специалист, занимающийся нормативно-правовым регулированием в сфере обеспечения ИБ, защитой ПД и иными правовыми вопросами.

4. Эксперт-технический писатель – специалист, занимающийся анализом технической документации, фокусирующийся на деталях стандартов и требований законодательства в данной области.

5. Эксперт-разработчик ПО – специалист по анализу программного кода.

6. Эксперт по проведению тестирования на проникновение – специалист по практическому анализу защищенности ИС и ИТ-инфраструктур.

Также определены дополнительные (необходимые в случае проведения углубленного анализа и оценки процессов и технических аспектов) специалисты:

1. Эксперт по расследованию инцидентов (форензике) – специалист в области осуществления организационно-технических мероприятий, направленных на поиск и выстраивание цепочек возникновения событий и хронологии возникновения инцидентов ИБ (расследование киберпреступлений).

2. Эксперт по реверс-инжинирингу – специалист с навыками глубокого анализа программного кода, занимающийся обратной разработкой, анализом информационных систем для определения безопасности их функциональных характеристик (внутренней архитектуры, функций, алгоритмов).

Для отображения основных компонентов диагностики СОИБ в ОГВ, а именно, функциональных элементов, необходимых для выполнения процессов диагностики, их характеристик и взаимосвязей между ними с учетом требований

отобранных из проанализированных «лучших практик» процессов была построена информационная модель элементов диагностики СОИБ (рисунок 3.10).

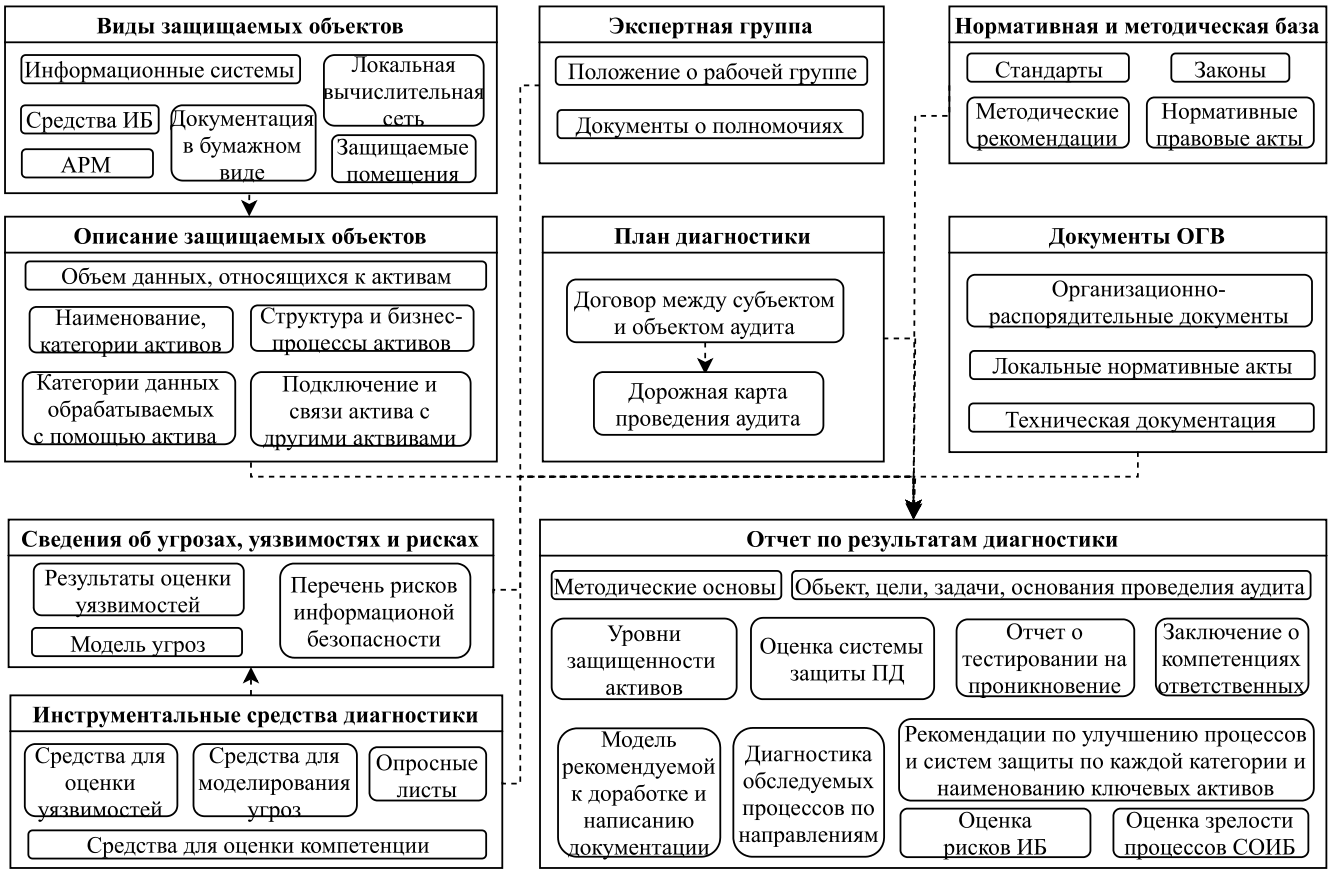

Рисунок 3.10 – Информационная модель элементов комплексной диагностики СОИБ в ОГВ [разработано автором]

Широта охвата и разветвленность структурных элементов информационной модели диагностики СОИБ говорит о количестве затрагиваемых вопросов: бизнес-процессы организации, документация, уровень подготовки сотрудников, оценка уязвимостей, моделирование угроз, оценка рисков ИБ и др. С учетом обозначенных целей, разработанной модели выборок процессов из «лучших практик», а также сформированной информационной модели, выделены ключевые этапы, необходимые для разработки эффективного методического подхода к комплексной диагностике СОИБ в ОГВ:

1. Инициирование процедуры диагностики, сбор информации.

2. Очная оценка процессов на соответствие требованиям.

3. Тестирование на проникновение.

4. Оценка защищенности и технического состояния ИТ-инфраструктуры.

5. Оценка защищенности и качества информационных систем.

6. Оценка защищенности зданий и помещений.

7. Оценка уровня подготовки сотрудников.

8. Оценка системы защиты персональных данных.

9. Оценка эффективности СОИБ. Формирование заключения.

В результате проведенного исследования сформирована поэтапная схема реализации методического подхода к комплексной диагностике СОИБ в ОГВ, где определены основные процессы этапов диагностики, порядок реализации которых оптимизирован и конкретизирован на рисунке 3.11). Каждый из указанных этапов, в свою очередь, включает в себя перечень ключевых процессов в обобщенной форме. Выделенные процессы позволяют не только осуществить комплексный анализ деталей эффективности СОИБ в ОГВ, но и сформировать полноценную структуру и последовательность оптимизации максимального количества «узких» мест на основании данных, полученных в результате диагностики, формируя зрелый подход к поступательной оптимизации системы. Результатом отчета по результатам комплексной диагностики является оценка и детальное описание уязвимостей, угроз рисков ИБ, свойственных информационной среде обследуемого ОГВ, а также анализ зрелости и детальное описание процессов, отображенных на рисунке 3.9.

Стоит отметить, что проведение комплексной диагностики является ресурсоемкой процедурой, с учетом глубины знаний специалистов, необходимых для ее осуществления и требуемых для выполнения всех этапов диагностики временных затрат. При этом, необходимо указать на важность оценки на соответствие требованиям регуляторов и «лучшим практикам» через диагностику на соответствие требованиям ИБ для ОГВ, т. к. данный способ позволяет как провести анализ уровня мер, средств и процессов обеспечения ИБ в ОГВ с оптимальной затратой ресурсов, так и выстраивать общегосударственную СОИБ через количественную оценку и контроль уровня зрелости СОИБ в ОГВ.

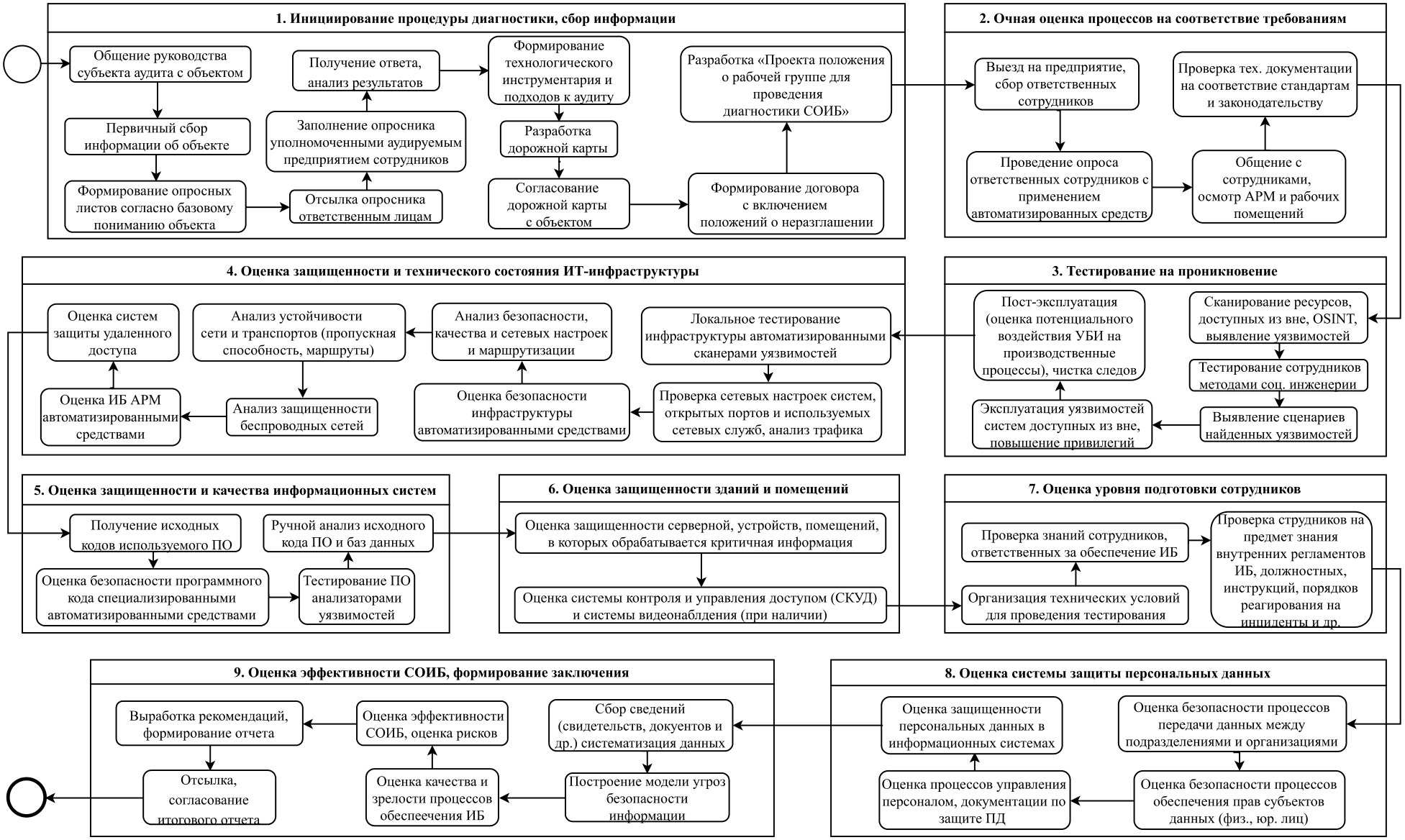

Рисунок 3.11 – Обобщенная схема процессов методического подхода к комплексной диагностике СОИБ в ОГВ [разработано автором]

Поэтому в существующих условиях существования ДНР, с учетом особой важности оптимизации ресурсов, затрачиваемых на осуществление диагностики и необходимости количественной оценки уровня зрелости процессов ИБ в ОГВ целесообразно проводить диагностику СОИБ на соответствие требованиям (этап 2, рисунок 3.11), а дальнейшее исследование целесообразно построить с точки зрения детализации и декомпозиции данного этапа.

Особую важность при этом занимает выбор стандарта/фреймворка/НПА, которому необходимо соответствовать органам государственной власти. Здесь важно отметить, что на современном этапе финансовую и банковскую, в частности, сферы можно назвать одними из наиболее передовых в области разработки и реализации релевантных методологий и стандартов обеспечения ИБ, учитывающих актуальные современные угрозы и содержащие цикличные риск-ориентированные подходы к оценке и совершенствованию СОИБ.

Происходит это по причине того, что формирование эффективной СОИБ является безальтернативно необходимым компонентом выживания финансовых учреждений, как с учетом критичности циркулирующих в их ИС данных, так и с учетом того, что все ключевые услуги данных организаций строятся на безопасных, отказоустойчивых и отлаженных автоматизированных процессах. Поэтому, несмотря на разницу между банковской сферой и сферой государственного управления для настоящего исследования выбраны, по мнению автора, передовые с точки зрения охвата и релевантности затрагиваемых при анализе мер, средств и процессов обеспечения ИБ стандарты РФ:

– ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [219];

– ГОСТ Р 57580.2-2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [220].

Целями данных стандартов является:

1. Определение уровней ИБ и соответствующих им требований к содержанию базового состава организационных и технических мер обеспечения безопасности информационных активов.

2. Достижение адекватности состава и содержания мер обеспечения ИБ.

3. Обеспечение эффективности и возможности стандартизированного контроля за СОИБ организаций.

Для достижения вышеизложенных целей и в рамках разработки модели диагностики на соответствие требованиям стандарта, автором разработан алгоритм диагностики СОИБ на соответствие адаптированным для ОГВ требованиям ГОСТ Р 57580.1-2017 (рисунок 3.12).

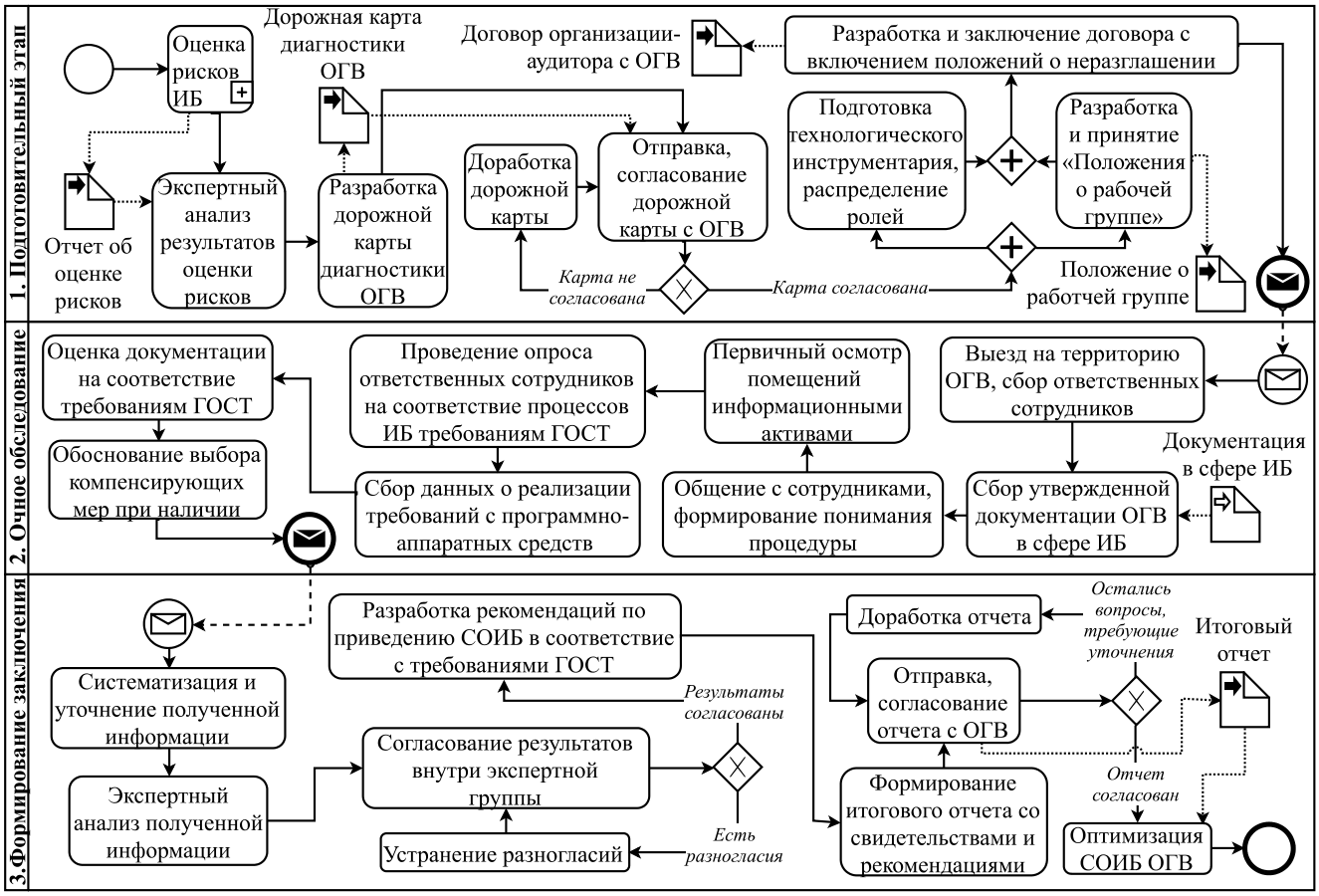

Рисунок 3.12 – Алгоритм диагностики СОИБ в ОГВ на соответствие требованиям стандарта [составлено автором]

Диагностика совершается в 3 этапа. В ходе первого (подготовительного) этапа на основании результата оценки рисков ИБ (п. 2.3 диссертации)

формируется дорожная карта с планом диагностики СОИБ в ОГВ, разрабатывается «Положение о рабочей группе» и заключается договор между аудитором и организацией-объектом диагностики. Стоит отметить, что оценка рисков ИБ может проводиться как силами сотрудников ОГВ, так и с помощью иной организации.

В ходе очного обследования проводятся все процедуры оценки СОИБ, выявляются аспекты внедренных мер и средств обеспечения ИБ. Завершающим этапом является «Формирование заключения», в ходе которого экспертная группа определяет и согласовывает оценки процессов ИБ согласно ГОСТ внутри рабочей группы, формирует отчет с рекомендациями и согласовывает его с объектом диагностики.

По результатам диагностики ОГВ получает:

– отчет о диагностике СОИБ с числовыми оценками соответствия процессов и их обоснованием;

– листы сбора свидетельств и перечень выявленных нарушений;

– рекомендации по совершенствованию СОИБ.

Подход, изложенный в исследуемых стандартах, предполагает наличие трех уровней защиты информации. Апробация настоящей методики проводилась для 2-го уровня защиты информации. С учетом указанной разницы в сферах, важно обозначить необходимость адаптации показателей указанных процессов под специфику функционирования ОГВ, которая была проведена автором.

Переходя к сути рассматриваемых стандартов, стоит отметить, что в нем выделяются 8 процессов и 10 подпроцессов СИБ, 4 направления системы организации и управления ИБ (СМИБ), а также в отдельное направление оценки выделено обеспечение ИБ на этапах жизненного цикла ИС.

Диагностика СОИБ ОГВ на соответствие требованиям стандарта основывается на свидетельствах, в качестве основных источников данных которых могут использоваться:

– отчет об оценке рисков ИБ;

– документы ОГВ и иные материалы в бумажном или электронном виде и, при необходимости, документы третьих лиц, обслуживающих ИС, или иным образом относящиеся к обеспечению ИБ в ОГВ и находящиеся в распоряжении проверяемой организации;

– устные высказывания сотрудников проверяемой организации в процессе проводимых опросов в области оценки соответствия требованиям стандарта;

– результаты наблюдений членов экспертной группы за процессами ИБ и деятельностью сотрудников проверяемого ОГВ в области оценки соответствия требованиям стандарта;

– параметры конфигураций и настроек объектов информатизации и средств обеспечения ИБ;

– технические и программные средства сбора свидетельств полноты реализации мер обеспечения ИБ (анализ электронных журналов, фактических настроек, уязвимостей и др.).

Выбор конкретных источников свидетельств при проведении диагностики осуществляет экспертная группа с учетом предложений проверяемого ОГВ и обеспечения максимальной достоверности оценки соответствия СОИБ. Полученные свидетельства и источники их получения должны быть задокументированы путем составления листов для сбора свидетельств оценки процессов СОИБ и направлений обеспечения ИБ.

При заполнении листов для сбора свидетельств указываются ссылки на: соответствующие документы и иные материалы проверяемого ОГВ или документы третьих лиц; результаты опроса сотрудников проверяемого ОГВ; результаты наблюдений членов проверяющей группы, а также результаты работы технических и программных средств. Результаты опроса должны быть подтверждены подписями члена (членов) проверяющей группы и опрашиваемого сотрудника (сотрудников) проверяемого ОГВ. Оценку соответствия СОИБ осуществляют по следующим направлениям:

– выбор органом государственной власти мер обеспечения ИБ, направленных на непосредственное обеспечение процессов, входящих в СОИБ;

– полнота реализации ОГВ мер обеспечения ИБ, направленных на непосредственное обеспечение процессов, входящих в СОИБ;

– обеспечение ИБ на этапах жизненного цикла ИС.

По завершению подготовительного этапа и этапа очного обследования экспертами заполняются сводные таблицы с результатами реализации оцениваемым ОГВ базового состава мер обеспечения ИБ. Для вычисления основных показателей процессов обеспечения ИБ использована шкала, представленная в таблице 3.8.

Таблица 3.8 – Шкала оценки мер обеспечения ИБ [составлено автором на основе [220]]

Показатель	Значения
$E_{\text{МИБ}}$ (оценка выбора ОГВ мер обеспечения ИБ, входящих в СИБ)	0 – отсутствие у ОГВ свидетельств выбора меры; 1 – предъявление ОГВ свидетельств выбора меры.
$E_{\text{МОУ}}$ (полнота реализации организационно-технических мер обеспечения ИБ, входящих в СМИБ)	0 – мера полностью не реализуется; 0,5 – мера реализуется не в полном объеме; 1,0 – мера реализуется в полном объеме.
$E_{\text{МАС}}$ (оценка, реализации каждой из мер обеспечения ИБ, применяемых на этапах жизненного цикла ИС)	

В начале диагностики на соответствие требованиям стандарта эксперты проводят оценку, характеризующую выбор ОГВ мер обеспечения ИБ, $\text{Е}_{\text{МИБ}}$, оценку характеризующая полноту реализации каждой из мер обеспечения ИБ, $\text{Е}_{\text{МОУ}}$, а также оценку, характеризующую реализацию каждой из мер обеспечения ИБ, применяемых на этапах жизненного цикла ИС, $E_{\text{МАС}}$.

В случае, если вместо мер обеспечения ИБ, предусмотренных ГОСТ Р 57580.1, применяются иные (компенсирующие) меры обеспечения ИБ, при определении оценок $E_{\text{МИБ}}$, $E_{\text{МОУ}}$ и $E_{\text{МАС}}$ эксперты осуществляют оценку компенсирующих мер в соответствии с вышеуказанными критериями. После выставления экспертных оценок табличные данные с заполненными значениями о мерах согласно шкале от каждого эксперта собираются и проводится вычисление итоговых показателей. В Приложении М представлена структура процессов, подпроцессов и направлений оценки соответствия стандарту. В таблице 3.9 представлены показатели, определяющие соответствие СОИБ ОГВ адаптированным требованиям ГОСТ 57580.1 и формулы их расчета.

Таблица 3.9 – Показатели, определяющие соответствие СОИБ ОГВ адаптированным требованиям стандарта и способы их расчета [составлено автором]

Показатель	Формула	Переменные	Описание
1	2	3	4
Числовые значения оценок, характеризующих выбор ОГВ мер обеспечения ИБ ($E_{\text{ПИБ}_i}$ ($E_{\text{ППИБ}_i}$))	$E_{\text{ПИБ}_i}$ ($E_{\text{ППИБ}_i}$) $= \frac{\sum_{j=1}^{N} E_{\text{МИБ}_j}}{N}$	$E_{\text{МИБ}_j}$ – оценка выбора j-й меры обеспечения ИБ, оцениваемой в рамках i-го процесса (подпроцесса) СОИБ; i – порядковый номер процесса (подпроцесса) СОИБ; j – порядковый номер меры обеспечения ИБ в процессе (подпроцессе) СОИБ, оцениваемой для соответствующего уровня; N – общее количество мер обеспечения ИБ, выбор которых оценивается в рамках процесса (подпроцесса) СОИБ.	Вычисляется отдельно по каждому из процессов СОИБ как среднеарифметическое значение оценок $\text{Е}_{\text{МИБ}_j}$ для каждой из мер обеспечения ИБ, входящих в состав оцениваемого процесса.
Числовые значения оценок, характеризующих выбор ОГВ мер обеспечения ИБ ($E_{\text{ПИБ}_i}$)	$E_{\text{ПИБ}_i} = \frac{\sum_{k=1}^{M} E_{\text{ППИБ}_k}}{M}$	$E_{\text{ППИБ}_k}$ – оценка выбора мер обеспечения ИБ k-го подпроцесса в i-м процессе СОИБ; i – порядковый номер процесса СОИБ; k – порядковый номер подпроцесса в процессе СОИБ; M – общее количество мер обеспечения ИБ, выбор которых оценивается в рамках процесса СОИБ.	Вычисляется как среднее арифметическое значение оценок $\text{Е}_{\text{ППЗИ}_k}$ для каждого из подпроцессов к процессам 1, 2 и 6 (Приложение М), входящих в состав оцениваемого процесса.
Числовые значения оценок, характеризующих планирование процессов СОИБ ($E_{\text{П}_i}$)	$E_{\text{П}_i} = \frac{\sum_{n=1}^{F} E_{\text{МОУ}_n}}{F}$	$E_{\text{МОУ}_n}$ – оценка полноты реализации n-й меры обеспечения ИБ, оцениваемой в рамках направления 1 «Планирование процесса СОИБ» для соответствующего уровня обеспечения ИБ; i – порядковый номер процесса СОИБ; n – порядковый номер меры обеспечения ИБ, оцениваемой в рамках направления 1 «Планирование процесса СОИБ» для соответствующего уровня обеспечения ИБ; F – общее количество мер обеспечения ИБ, реализация которых оценивается в рамках направления 1 «Планирование процесса СОИБ».	Вычисляется отдельно по каждому из процессов ИБ как среднеарифметическое значение оценок для мер обеспечения ИБ, входящих в СМИБ ОГВ.
Числовые значения оценок, характеризующих реализацию процессов СОИБ ($E_{\text{Р}_i}$)	$E_{\text{Р}_i} = \frac{\sum_{j=1}^{\text{P}} E_{\text{МОУ}_j}}{P}$	$E_{\text{МОУ}_j}$ – оценка полноты реализации j-й меры обеспечения ИБ, оцениваемой в рамках направления 2 «Реализация процесса СОИБ»; i – порядковый номер процесса СОИБ; j – порядковый номер меры обеспечения ИБ, оцениваемой в рамках направления 2 «Реализация процесса СОИБ» для соответствующего уровня обеспечения ИБ; P – общее количество мер обеспечения ИБ, реализация которых оценивается в рамках направления 2 «Реализация процесса СОИБ».	Вычисляется отдельно по каждому из процессов СОИБ как среднеарифметическое значение оценок для мер обеспечения ИБ, входящих в СМИБ ОГВ.

Продолжение таблицы 3.9

1	2	3	4
Числовые значения оценок, характеризующих контроль процессов СОИБ ($E_{\text{К}_i}$)	$E_{\text{К}_i} = \frac{\sum_{k=1}^{S} E_{\text{МОУ}_k}}{S}$	$E_{\text{МОУ}_\text{к}}$ – оценка полноты реализации k-й меры обеспечения ИБ, оцениваемой в рамках направления 3 «Контроль процесса СОИБ»; i – порядковый номер процесса СОИБ; k – порядковый номер меры обеспечения ИБ, оцениваемой в рамках направления 2 «Реализация процесса СОИБ» для соответствующего уровня обеспечения ИБ; S – общее количество мер обеспечения ИБ, реализация которых оценивается в рамках направления 3 «Контроль процесса СОИБ».	Вычисляется отдельно по каждому из процессов СОИБ как среднеарифметическое значение оценок для мер обеспечения ИБ, входящих в СМИБ ОГВ.
Числовые значения оценок, характеризующих совершенствование процессов СОИБ ($E_{\text{С}_\text{i}}$)	$E_{\text{С}_i} = \frac{\sum_{m=1}^{Q} E_{\text{МОУ}_m}}{Q}$	$E_{\text{МОУ}_\text{m}}$ – оценка полноты реализации m-й меры обеспечения ИБ, оцениваемой в рамках направления 4 «Совершенствование процесса СОИБ». i – порядковый номер процесса СОИБ; m – порядковый номер меры обеспечения ИБ, оцениваемой в рамках направления 2 «Совершенствование процесса СОИБ»; Q – общее количество мер обеспечения ИБ, реализация которых оценивается в рамках направления 4 «Совершенствование процесса СОИБ».	Вычисляется отдельно по каждому из процессов СОИБ как среднеарифметическое значение оценок для мер обеспечения ИБ, входящих в СМИБ ОГВ.
Числовое значение оценки, характеризующей применение мер обеспечения ИБ на этапах жизненного цикла ИС (E_{AC})	$E_{AC} = \frac{\sum_{j=1}^{L} E_{\text{МАС}_j}}{L}$	$E_{\text{МАС}_\text{j}}$ – оценка полноты реализации j-й меры обеспечения ИБ, оцениваемой на этапах жизненного цикла ИС. j – порядковый номер меры обеспечения ИБ, оцениваемой в рамках применения на этапах жизненного цикла ИС; L – общее количество мер обеспечения ИБ, оцениваемых в рамках применения на этапах жизненного цикла ИС.	Вычисляется как среднеарифметическое значение оценок $E_{\text{МАС}}$ для всех мер обеспечения ИБ, применяемых на этапах жизненного цикла ИС.
Числовые значения оценок соответствия каждого процесса СОИБ (E_i)	$E_i = \frac{E_{\text{ПИБ}_i} + (0{,}2 * E_{\text{П}_i} + 0{,}4 * E_{\text{Р}_i} + 0{,}25 * E_{\text{К}_i} + 0{,}15 * E_{\text{С}_i})}{2}$	$E_{\text{ПИБ}_i}$ – числовая оценка, характеризующая выбор мер процесса СОИБ; $E_{\text{П}_i}$ – числовая оценка, характеризующая планирование процесса СОИБ; $E_{\text{Р}_i}$ – числовая оценка, характеризующая реализацию процесса СОИБ; $E_{\text{К}_i}$ – числовая оценка, характеризующая контроль процесса СОИБ; $E_{\text{С}_i}$ – числовая оценка, характеризующая совершенствование процесса СОИБ.	Вычисляется отдельно по каждому -му процессу как среднеарифметическое значение числовой оценки $E_{\text{ПЗИ}_i}$ и суммы числовых значений оценок $E_{\text{П}_i}$, $E_{\text{Р}_i}$, $E_{\text{К}_i}$, $E_{\text{С}_i}$, с учетом их весовых коэффициентов.
Итоговая числовая оценка соответствия СОИБ ОГВ (R)	$R = \frac{\sum_{i=1}^{T} E_i + E_{\text{АС}}}{T+1} - 0{,}01 * Z$	E_i – оценка соответствия обеспечения ИБ i-го процесса СОИБ; i – номер процесса СОИБ; T – количество процессов СОИБ, вошедших в область диагностики; $E_{\text{АС}}$ – оценка полноты применения мер обеспечения ИБ на этапах жизненного цикла ИС ОГВ; Z – количество нарушений обеспечения ИБ, выявленных членами экспертной группы в процессе оценки соответствия.	Вычисляется как среднеарифметическое значение оценок для всех процессов СОИБ и оценки $E_{\text{АС}}$.

Качественная оценка уровня соответствия каждого процесса СОИБ для оценки полноты его реализации определяется согласно адаптированным для ОГВ значениям таблицы 3.10 в соответствии с числовыми оценками E_i.

Таблица 3.10 – Диапазоны значений уровней соответствия процессов СОИБ органа государственной власти (E_i) [составлено автором на основе [220]]

Уровень соответствия	E_i	Описание уровня
0	$E_i = 0$	Меры обеспечения ИБ не реализуются или реализуются в единичных случаях. Общие подходы (способы) реализации мер процесса СОИБ не установлены. Контроль и совершенствование реализации мер обеспечения ИБ не осуществляются.
1	$0 < E_i \leq 0{,}3$	Меры обеспечения ИБ реализуются в незначительном количестве, бессистемно и/или эпизодически. Общие подходы (способы) реализации мер процесса СОИБ не установлены. Контроль и совершенствование реализации мер обеспечения ИБ не осуществляются.
2	$0{,}3 < E_i \leq 0{,}6$	Меры обеспечения ИБ реализуются в значительном количестве на постоянной основе. Общие подходы (способы) реализации мер процесса СОИБ установлены в единичных случаях и (или) на усмотрение исполнителя. Контроль и совершенствование реализации процессов СОИБ нуждаются в оптимизации.
3	$0{,}6 < E_i \leq 0{,}75$	Меры обеспечения ИБ реализуются в значительном количестве на постоянной основе в соответствии с общими подходами (способами), установленными в ОГВ. Контроль и совершенствование реализации мер процесса СОИБ осуществляются эпизодически.
4	$0{,}75 < E_i \leq 0{,}9$	Меры обеспечения ИБ реализуются в полном объеме на постоянной основе в соответствии с общими подходами (способами), установленными в ОГВ. В ОГВ преимущественно реализованы контроль и совершенствование реализации мер процесса СОИБ.
5	$0{,}9 < E_i \leq 1$	Меры обеспечения ИБ реализуются в полном объеме на постоянной основе в соответствии с общими подходами (способами), установленными в ОГВ. Реализованы постоянный контроль и необходимое своевременное совершенствование реализации мер процесса СОИБ.

Согласно разработанному методическому подходу экспертами было определено, что оценки соответствия процессов СОИБ (E_i) превышающие числовое значение 0,6 соответствуют рекомендуемому (3-му уровню соответствия) для ОГВ ДНР.

При выявлении членами экспертной группы в процессе оценки соответствия фактов нарушений ИБ, в результате которых имелась или имеется возможность наступления инцидентов ИБ, наносящих ущерб информационным

активам ОГВ, итоговая оценка соответствия СОИБ (R) снижается на значение, равное 0,01, за каждый выявленный факт нарушения. Факты нарушений ИБ, выявленные проверяемым ОГВ самостоятельно до начала или в процессе диагностики, по которым проведено расследование до окончания диагностики и приняты или запланированы соответствующие меры реагирования с документальным оформлением, при снижении итоговой числовой оценки соответствия СОИБ не учитываются. Перечень нарушений приведен в приложении Б ГОСТ Р 57580.2-2018.

В качестве апробации предлагаемого методического подхода к комплексной диагностике СОИБ при реализации диагностики на соответствие требованиям стандарта выбрано Министерство связи ДНР. Для проведения диагностики ОГВ автором было привлечено 10 экспертов из числа профильных специалистов: 5 специалистов Министерства связи ДНР, 5 специалистов ГУП ДНР «Углетелеком». В несколько этапов в период с 17.02.2020 г. по 17.04.2020 г. проведены работы, согласно разработанного алгоритма (рисунок 3.12).

Результаты оценок уровня соответствия процессов и реализации мер обеспечения ИБ были рассчитаны на основании разработанного методического подхода с учетом полученных от экспертов данных, в результате чего подготовлена сводная таблица (таблица 3.11).

Оценки процессов 1, 2, 3, 4, 7, 8 СОИБ Министерства связи ДНР определены как соответствующие рекомендуемому (3-му уровню соответствия). В свою очередь, процессы 5 и 6 определены экспертами как рекомендуемые к анализу на целесообразность оптимизации (2 уровень соответствия). Направления «планирование», «контроль» и «совершенствование» процессов обеспечения ИБ определены как рекомендуемые к развитию.

В результате расчета значение оценки применения мер обеспечения ИБ на этапах жизненного цикла ИС (E_{AC}) определено как 0,54. Также в результате диагностики экспертами выявлено 2 нарушения ИБ (Z), в результате чего итоговая числовая оценка соответствия СОИБ Министерства связи ДНР (R) определена как 0,55.

Таблица 3.11 – Оценки соответствия процессов СОИБ Министерства связи ДНР адаптированным значениям требований стандарта ГОСТ 57580.1-2017 [составлено автором]

Наименование процесса СОИБ	Оценка организационных и технических мер обеспечения ИБ ($E_{\text{ПИБ}_i}$)	Система менеджмента информационной безопасности								Числовое значение оценки соответствия процесса (E_i)	Уровень соответствия процесса
		Планирование процесса		Реализация процесса		Контроль процесса		Совершенствование процесса			
		Вес	$E_{\text{П}_i}$	Вес	$E_{\text{Р}_i}$	Вес	$E_{\text{К}_i}$	Вес	$E_{\text{С}_i}$		
Процесс 1 «Обеспечение защиты информации при управлении доступом»	0,85	0,2	0,4	0,4	0,6	0,25	0,41	0,15	0,35	0,66	3
Процесс 2 «Обеспечение защиты вычислительных сетей»	0,87		0,2		0,6		0,32		0,25	0,63	3
Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»	0,84		0,4		0,6		0,35		0,1	0,63	3
Процесс 4 «Защита от вредоносного кода»	0,85		0,2		0,45		0,35		0,35	0,61	3
Процесс 5 «Предотвращение утечек информации»	0,56		0,2		0,4		0,1		0,35	0,42	2
Процесс 6 «Управление инцидентами информационной безопасности»	0,54		0,4		0,41		0,35		0,1	0,44	2
Процесс 7 «Защита среды виртуализации»	0,81		0,3		0,73		0,35		0,1	0,63	3
Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»	0,78		0,2		0,63		0,35		0,35	0,61	3

Фактические оценки соответствия процессов СОИБ Министерства связи ДНР адаптированным значениям требований стандарта ГОСТ 57580.1-2017, представлены на рисунке 3.13.

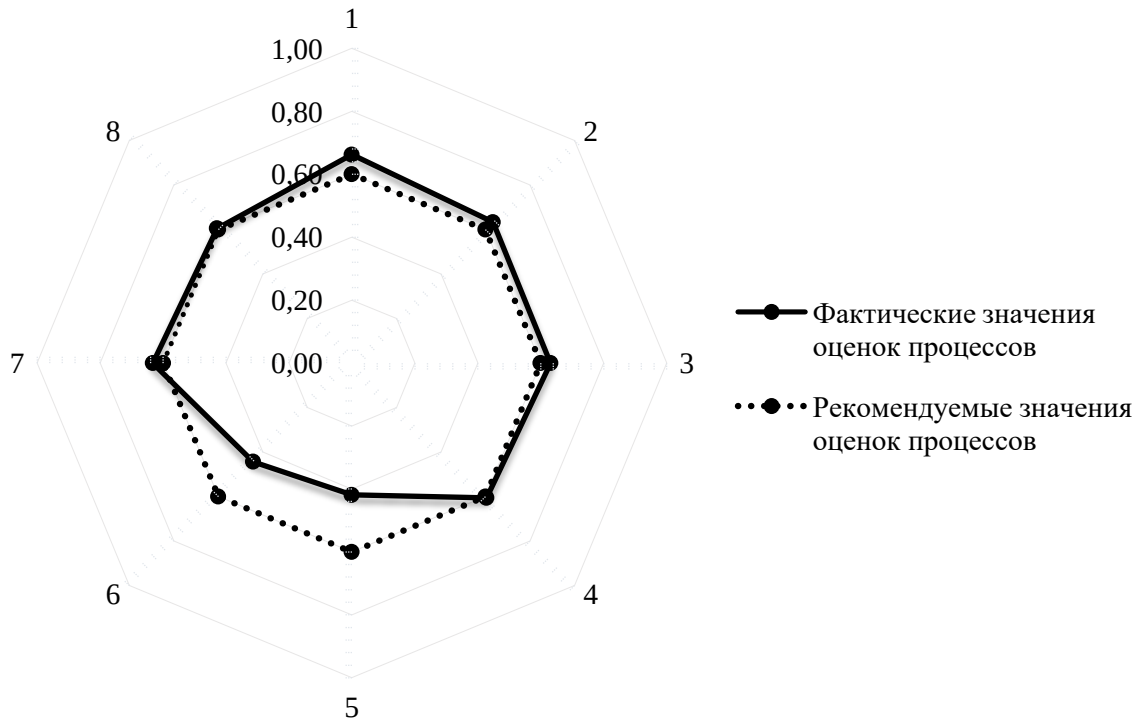

Рисунок 3.13 – Фактические и рекомендуемые значения оценок процессов СОИБ Министерства связи ДНР, согласно диагностике на соответствие требованиям стандарта [составлено автором]

Определенные оценки свидетельствуют о том, что техническим мерам в организации-объекте диагностики уделяется серьезное внимание, однако некоторые организационные аспекты, связанные с требованиями стандарта, в частности – «планирование», «контроль» и «совершенствование» процессов, нуждаются в оптимизации. Следствием данному факту можно назвать низкую эффективность контрольно-надзорной деятельности за сферой обеспечения ИБ со стороны государства и отсутствие соответствующих требований к ИБ в подзаконных НПА.

После получения экспертных оценок всех процессов и подпроцессов для Министерства связи ДНР, а также завершения остальных этапов диагностики

разработанного алгоритма, производится формирование экспертного заключения, содержащего рекомендации по оптимизации СОИБ. По факту получения отчета с оценками и рекомендациями в результате проведенной диагностики, ОГВ приступает к формированию корректирующих и оптимизационных процессов по устранению проблемных вопросов и оптимизации СОИБ.

С учетом отсутствия методических рекомендаций и однозначного трактования экспертным сообществом способов реализации мер, указанных в ГОСТ Р 57580.1-2017, автором было принято решение о сборе инициативной экспертной группы и формировании базы знаний, способствующей обеспечению единого трактования требований, изложенных в стандарте. Целями разработки данной базы знаний является не только детализация способов реализации мер обеспечения ИБ, но и корреляция мер стандарта ГОСТ с требованиями по обеспечению безопасности критической информационной инфраструктуры и мерами по защите ПД (Приказам ФСТЭК №239 и №21), что особенно актуально для ОГВ как субъектов критической информационной инфраструктуры и операторов информационных систем, содержащих ПД [248].

Разработка таких универсальных методических рекомендаций будет способствовать повышению уровня осведомленности, сокращению времени на осуществление работ, направленных на обеспечение соответствию требованиям ГОСТ Р 57580.1-2017 НПА и повышению уровня цельности проводимых мер по совершенствованию СОИБ в ОГВ. Фрагмент структуры базы знаний с результатами вышеуказанной работы представлен в Приложении Н.

Проведенное исследование позволило структурировать информацию, необходимую для осуществления комплексной диагностики СОИБ в ОГВ, выделить основные этапы ее проведения, проследить корреляционные взаимоотношения между процессами и подпроцессами, взаимосвязи объектов и процессов процедуры, а также сформировать комплексную модель диагностики, ключевой этап которой декомпозирован, систематизирован и усовершенствован, что позволило сформировать оптимальный механизм оценки состояния СОИБ в ОГВ.

Проведение оценки СОИБ в ОГВ на соответствие требованиям стандарта в рамках разработанного методического подхода к комплексной диагностике позволяет решить следующие задачи:

1. Повысить уровень защищенности информационных активов ОГВ.

2. Привести СОИБ в ОГВ в соответствие с современными государственными и отраслевыми требованиями РФ и мировыми «лучшими практиками».

3. Повысить уровень управляемости процессов ИБ, скорости и качества принимаемых в информационной среде ОГВ решений.

Таким образом, автором разработан методический подход к комплексной диагностике СОИБ в ОГВ, основанный на использовании международных и российских стандартов и «лучших практик», посредством формирования обобщенной схемы реализации подхода и декомпозиции ключевого этапа оценки соответствия требованиям стандарта, что дает возможность выбрать и обосновать эталонные значения критериев состояния СОИБ и осуществить объективную оценку ее уровня, а также определить и классифицировать основные процессные составляющие системы, отличающиеся от существующих тем, что имеют более полную структуру и являются адаптированными под специфику ОГВ.

Выводы к главе 3

1. Предложен теоретико-методический подход к совершенствованию системы обеспечения информационной безопасности в органах государственной власти ДНР за счет разработки концепции совершенствования системы, которая, в отличие от существующих, базируется на системных процессно-ориентированных принципах управления, повышении эффективности применения комплексного

подхода к обеспечению информационной безопасности в органах государственной власти, инструментарии оценки рисков и диагностики, объектной модели регулирования и оптимизации механизмов государственного управления в исследуемой сфере. Концепция содержит комплекс мероприятий по совершенствованию СОИБ ДНР на общегосударственном уровне и уровне ОГВ, позволяет определить алгоритм необходимых действий по совершенствованию системы и спрогнозировать результаты соответствующих преобразований. Разработан комплекс базовых нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры ДНР; предложены первоочередные меры, направленные на ее защиту; определен комплекс мероприятий, направленных на создание и развитие систем обеспечения безопасности критической информационной инфраструктуры в ОГВ.

2. Обоснована необходимость создания Единого государственного центра координации органов государственной власти в сфере обеспечения информационной безопасности, что позволит оптимизировать процессы взаимодействия органов-регуляторов в сфере обеспечения информационной безопасности, Правительства ДНР и других органов государственной власти, повысить эффективность, зрелость и оперативность принятия управленческих решений. Определены основные задачи ЕГЦК; сформирована организационная структура ЕГЦК; разработана схема его функционального взаимодействия с ключевыми субъектами в сфере обеспечения информационной безопасности ДНР; определены группы сервисов, предоставляемых ЕГКЦ для органов государственной власти; определены этапы создания ЕГЦК.

3. Предложены организационные подходы к формированию архитектуры единого информационного пространства органов государственной власти за счет создания системы управления информационной безопасностью в органах государственной власти, что, в отличие от существующей структуры управления, позволит стандартизировать, унифицировать и обеспечить единство механизмов развития системы обеспечения информационной безопасности в публичном управлении, а также оптимизировать процессы взаимодействия органов

государственной власти в сфере обеспечения информационной безопасности. Сформирована архитектура государственной системы управления информационной безопасностью и обобщенный алгоритм взаимодействия ОГВ с ЕГЦК в рамках государственной системы управления ИБ, а также обобщенный план создания ЕИП и выделены основные положения ожидаемого социально-экономического эффекта от его функционирования.

4. Определено, что внедрение предложенных подходов позволит усовершенствовать процессы взаимодействия всех субъектов информационного пространства ДНР, реализуя подход, базирующийся на формировании ключевых систем электронного правительства, повышении функциональной совместимости государственных информационных систем и формировании комплексной системы управления информационной безопасностью в органах государственной власти, что позволяет усовершенствовать и стандартизировать подходы к информатизации и обеспечению информационной безопасности в органах государственной власти, а также повысить эффективность системы публичного управления и создать условия, способствующие обеспечению устойчивого развития ДНР в цифровую эпоху.

5. Определены и декомпозированы ключевые этапы, необходимые для комплексной, всесторонней, адаптированной для органов государственной власти методики диагностики системы обеспечения информационной безопасности, порядок проведения которой представлен в виде функциональной поэтапной модели. Проведенный анализ позволил структурировать информацию, необходимую для поддержки функций диагностики системы обеспечения информационной безопасности в органах государственной власти, выделить основные этапы проведения диагностики, проследить корреляционные взаимоотношения между процессами и подпроцессами, а также взаимосвязи активов и производственных процессов и сформировать комплексную модель диагностики.

6. В целях оптимизации процесса оценки эффективности системы обеспечения информационной безопасности в органах государственной власти

разработан методический подход к комплексной диагностике СОИБ в ОГВ, основанный на использовании международных и российских стандартов и «лучших практик», посредством формирования обобщенной схемы реализации подхода и декомпозиции ключевого этапа оценки соответствия требованиям стандарта, что дает возможность выбрать и обосновать эталонные значения критериев состояния СОИБ и осуществить объективную оценку ее уровня, а также определить и классифицировать основные процессные составляющие системы, отличающиеся от существующих тем, что имеют более полную структуру и являются адаптированными под специфику ОГВ.

Основные результаты главы опубликованы в научных трудах автора [221; 222].

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования решена актуальная научно-практическая задача, заключающаяся в развитии теоретических положений, а также разработке методических и практических рекомендаций по совершенствованию системы обеспечения информационной безопасности в органах государственной власти в условиях неопределенности внешней среды.

Полученные результаты исследования позволили обосновать и сформулировать следующие выводы и рекомендации:

1. В результате исследования понятийно-категориального аппарата уточнено содержание понятия «информационная безопасность» в органах государственной власти», под которым предложено понимать защищенность информационных активов органа от любых случайных или преднамеренных воздействий, результатом которых может явиться нанесение ущерба любым свойствам информации и (или) средствам ее обработки, обеспечивающим удовлетворение информационных потребностей граждан, органов государственной власти и других субъектов информационных отношений за счет внедрения мер, средств и процессов защиты информации, достаточных для нейтрализации существующих угроз безопасности информации в условиях непрерывного совершенствования методов и способов их реализации; предложена авторская трактовка понятия «информационный актив» в органах государственной власти», под которым принято понимать информацию и (или) средство ее обработки, определенные и управляемые как единое целое; с реквизитами, позволяющими их идентифицировать; имеющие ценность для органов государственной власти и находящиеся в их распоряжении; представленные на любом материальном носителе или в его виде в пригодной форме для выполнения присущих им задач; необходимые для реализации

социальных, политических, экономических и других функций и полномочий.

2. В результате обобщения теоретико-методологических подходов и исследования зарубежного опыта формирования, функционирования и развития систем обеспечения информационной безопасности в органах государственной власти определена целесообразность применения комплексного подхода к обеспечению информационной безопасности и объектной модели регулирования, способствующих совершенствованию системы обеспечения информационной безопасности в органах государственной власти ДНР.

3. В результате анализа тенденций развития системы обеспечения информационной безопасности в органах государственной власти ДНР, а также системы обеспечения информационной безопасности в отдельном органе государственной власти с использованием разработанного методического подхода к оценке рисков информационной безопасности выявлены актуальные угрозы безопасности информации, уровень рисков, связанный с каждой угрозой, и приоритизирована последовательность их обработки.

4. Разработана концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти ДНР, в которой предложен: комплекс мероприятий по совершенствованию системы обеспечения информационной безопасности на общегосударственном уровне и уровне органов государственной власти; комплекс базовых нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры ДНР; комплекс мероприятий, направленных на создание и развитие систем обеспечения безопасности критической информационной инфраструктуры в органах государственной власти.

5. Усовершенствованы организационные подходы к формированию архитектуры единого информационного пространства органов государственной власти за счет создания системы управления информационной безопасностью в органах государственной власти, что, в отличие от существующей структуры управления, позволит стандартизировать, унифицировать и обеспечить единство механизмов развития системы обеспечения информационной безопасности в

публичном управлении, а также оптимизировать процессы взаимодействия органов государственной власти в сфере обеспечения информационной безопасности.

6. Усовершенствован методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти, основанный на использовании международных и российских стандартов и «лучших практик», посредством формирования обобщенной схемы реализации подхода и декомпозиции ключевого этапа оценки соответствия требованиям стандарта, что дает возможность выбрать и обосновать эталонные значения критериев состояния системы обеспечения информационной безопасности и осуществить объективную оценку ее уровня, а также определить и классифицировать основные процессные составляющие системы, отличающиеся от существующих тем, что имеют более полную структуру и являются адаптированными под специфику органов государственной власти.

Дальнейшие исследования связываются с совершенствованием механизма контрольно-надзорной деятельности государства в сфере обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Джура, Г. С. Особенности формирования и развития единого государственного информационного пространства / Е. А. Шумаева, Г. С. Джура // Завалишинские чтения’17: сб. докл., г. Санкт-Петербург, 10-14 апреля 2017 г. / СПб.: ГУАП, 2017. – С. 333-336.

2. Джура, Г. С. К вопросу об утечках информации в государственных информационных системах / Г. С. Джура, Е. А. Шумаева // Современное государственное и муниципальное управление: проблемы, технологии, перспективы: сб. материалов III международ. науч.-практ. конф., г. Донецк, 26 апреля 2017 г. – Донецк: ДонНТУ, 2017. – С. 127-130.

3. Гарин, Е. В. Иерархия потребностей человека / Е. В. Гарин // Вестник науки Сибири. – 2014. – № 2 (12). – С. 168-181.

4. Дроботенко, О. Н. Информационная безопасность России в условиях глобализации: внешнеполитический аспект: дис. … канд. полит. наук: 23.00.04: защищена 31.10.2014 / Дроботенко Олег Николаевич. – Пятигорск, 2014. – 207 с.

5. Тершуков, Д. А. Анализ современных угроз информационной безопасности / Д. А. Терщуков // НБИ Технологии. – 2018. – Вып. 12. № 3. – С. 6-12.

6. Балановская, А. В. Анализ современного состояния угроз информационной безопасности предприятий / А. В. Балановская // Информационная безопасность регионов. – 2015. – № 3 (20). – С. 9-16.

7. Энес, А. З. Технологические тенденции, влияющие на развитие информационных систем / А. З. Энес // Проблемы современной науки и образования. – 2017. – № 28 (110). – С. 20-22.

8. Богачев, В. Я. Информационная безопасность как составная часть национальной безопасности российской федерации [Электронный ресурс] /

В. Я. Богачев, В. В. Редин // Стратегия гражданской защиты: проблемы и исследования. – 2012. – № 2. – Режим доступа: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavnaya-chast-natsionalnoy-bezopasnosti-rossiyskoy-federatsii. – Дата обращения: 18.07.2020. – Загл. с экрана.

9. О стратегии национальной безопасности Российской Федерации [Электронный ресурс]: Указ Президента Российской Федерации от 31 декабря 2015 г. № 683: по состоянию на 03 июля 2020 г. // Официальный интернет-портал правовой информации. – Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202107030001. – Дата обращения: 03.07.2020. – Загл. с экрана.

10. Кучерявый, М. М. Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации / М. М. Кучерявый // Известия Российского государственного педагогического университета им. А. И. Герцена. – 2014. – № 164. – С. 155-163.

11. Черкашина, А. С. Использование автоматизированных информационных систем на предприятиях ОПК России / А. С. Черкашина, Н. Е. Гильц // Решетневские чтения. – 2018. – Т. 2. – С. 424-426.

12. Голубев, С. С. Влияние информационных технологий на деятельность оборонных промышленных предприятий России / С. С. Голубев, А. Г. Щербаков // Вестник Московского государственного областного университета. – 2018. – № 3. – С. 55-68.

13. Ваганова, Е. В. Медицинские информационные системы как объект оценки: факторы и тенденции развития / Е. В. Ваганова // Вестник Томского государственного университета. – 2017. – № 37. – С. 113-130.

14. Джура, Г. С. Сущность процесса обеспечения информационной безопасности в органах государственной власти / Е. А. Шумаева, Г. С. Джура // Сборник научных работ серии «Государственное управление». Вып. 20: Экономика и управление народным хозяйством / ГОУ ВПО «ДонАУиГС». – Донецк: ДонАУиГС, 2020. – С. 55-62.

15. Хаббард, Д. Как измерить всё, что угодно. Оценка стоимости нематериального в бизнесе [Электронный ресурс] / Д. Хаббард. – Режим доступа: https://medium.com/@magnolia.frau1990/дуглас-хаббард-как-измерить-все-что-угодно-оценка-стоимости-нематериального-в-бизнесе-baf3c9f7b395. – Дата обращения: 18.07.2020. – Загл. с экрана.

16. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента Российской Федерации от 5 декабря 2016 г. № 646: по состоянию на 18 июля 2020 г. // Документы системы ГАРАНТ. – Режим доступа: https://base.garant.ru/71556224/. – Дата обращения: 18.07.2020. – Загл. с экрана.

17. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. [Электронный ресурс]: ГОСТ Р ИСО/МЭК 27002-2012: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 423-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/ 1200103619. – Дата обращения: 18.07.2020. – Загл. с экрана.

18. Лопатин, В. Н. Информационная безопасность России: Человек. Общество. Государство / В. Н. Лопатин. – СПб.: Фонд «Университет», 2000. – 424 с.

19. Асаул, А. Н. Организация предпринимательской деятельности / А. Н. Асаул. – СПб.: АНО ИПЭВ, 2009. – 336 с.

20. Арсентьев, М. В. К вопросу о понятии об информационной безопасности / М. В. Арсентьев // Информационное общество. – 1997. – № 4-6. – С. 48-50.

21. Владимирова, Т. В. Социальная природа информационной безопасности: монография / Т. В. Владимирова. – М.: АНО Изд. Дом «Науч. обозрение», 2014. – 239 с.

22. Юсупов, Р. М. Информационное обеспечение национальной безопасности / Р. М. Юсупов // Национальная безопасность. Notabene. – 2010. – № 7/8. – С. 87.

23. Урсул, А. Д. Природа безопасности / А. Д. Урсул // Безопасность Евразии. – 2008. – № 1. – С. 7-36.

24. Пилипенко, В. Ф. Безопасность: теория, парадигма, концепция, культура: словарь-справочник / В. Ф. Пилипенко. – М.: ПЕР СЭ-Пресс, 2005. – 192 с.

25. Шободоева, А. В. Развитие понятия «информационная безопасность» в научно-правовом поле России / А. В. Шободоева // Известия Байкальского государственного университета. – 2017. – № 1. – С. 73-78.

26. Сергиенко, Л. А. История формирования информационного права в СССР и Российской Федерации 1960-2000 гг.: монография / Л. А. Сергиенко. – М.: ЮРКОМПАНИ, 2013. – 271 с.

27. Данилов, А. П. К вопросу об информационной безопасности в регионах российской Федерации: историко-правовые аспекты / А. П. Данилов, А. А. Данилов // Вестник Чувашского государственного университета. – 2015. – № 2. – С. 26-30.

28. Ганибаев, Г. Р. Эволюция представлений о содержании информационной безопасности / Г. Р. Ганибаев // СЕГОДНЯ И ЗАВТРА РОССИЙСКОЙ ЭКОНОМИКИ. – 2017. – № 85. – С. 26-34.

29. Шевко, Н. Р. Актуальные проблемы обеспечения информационной безопасности современного общества / Н. Р. Шевко // Вестник Казанского юридического института МВД России. – 2012. – № 8. – С. 57-59.

30. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология [Электронный ресурс]: ГОСТ Р ИСО/МЭК 27000-2012: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 15 ноября 2012 г. № 813-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим

доступа: http://docs.cntd.ru/document/ 1200102762. – Дата обращения: 18.07.2020. – Загл. с экрана.

31. Защита информации. Основные термины и определения. Национальный стандарт Российской Федерации. Защита информации Основные термины и определения Protection of information. Basic terms and definitions [Электронный ресурс]: ГОСТ Р 50922-2006 [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 27 декабря 2006 г. № 373-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/gost-r-50922-2006. – Дата обращения: 18.07.2020. – Загл. с экрана.

32. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели [Электронный ресурс]: ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 10 ноября 2014 г. № 1493-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/ 1200114169. – Дата обращения: 18.07.2020. – Загл. с экрана.

33. Стэнджер, Д. В чем разница между терминами «безопасность информационных технологий» и «кибербезопасность»? [Электронный ресурс] / Д. Стэнджер. – Режим доступа: https://www.securitylab.ru /blog/personal/ rusrim/346772.php. – Дата обращения: 18.07.2020. – Загл. с экрана.

34. Алпеев, А. С. Терминология безопасности: кибербезопасность, информационная безопасность / А. С. Алпеев // Вопросы кибербезопасности. – 2014. – № 5 (8). – С. 39-42.

35. Безкоровайный, М. М. Кибербезопасность подходы к определению понятия / М. М. Безкоровайный, А. Л. Татузов // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 22-27.

36. Грошева, Е. К. Информационная безопасность: современные реалии / Е. К. Грошева, П. И. Невмержицкий // Бизнес-образование в экономике знаний. – 2017. – № 3. – С.35-38.

37. Курейчук, К. П. Основы классификации угроз информационной безопасности информационно-измерительных систем удаленной обработки данных / К. П. Курейчик, А. А. Трушкевич // Доклады Белорусского государственного университета информатики и радиоэлектроники. – 2011. – № 5 (59). – С. 35-41.

38. Информатизация здоровья. Требования защиты и конфиденциальности систем EHR, используемые при оценке соответствия. Защита информации. Основные термины и определения. Национальный стандарт российской федерации [Электронный ресурс]: ГОСТ Р 57301-2016/ISO/TS 14441:2013: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 30 ноября 2016 г. № 1869-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/1200142738. – Дата обращения: 18.07.2020. – Загл. с экрана.

39. Национальный стандарт Российской Федерации стратегический и инновационный менеджмент. Термины и определения Strategic and innovation management. Terms and definitions [Электронный ресурс]: ГОСТР 54147-2010: [принят Приказом Федерального агентства по техническому регулированию и метрологии 21 декабря 2010 г. № 901-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/gost-r-54147-2010. – Дата обращения: 18.07.2020. – Загл. с экрана.

40. Домбровская, Л. А. Организационные средства защиты информации как элемент общей системы защиты информации. [Электронный ресурс] / Л. А. Домбровская, Т. Л. Васютина // European science. – 2016. – № 11 (21). – С. 21-25.

41. Гончарова Т. В. Социо-технико-технологическая концепция информационно-коммуникационной системы обеспечения муниципальных услуг / В.Д. Малыгина, Т.В. Гончарова // Торговля и рынок. – 2019. – Вып. 4. – Т.1. – С. 62-75.

42. Головкина, Д. В. Правовые меры обеспечения информационной безопасности и защиты интеллектуальной собственности предприятия / Д. В. Головкина // Вестник Прикамского социального института. – 2018. – № 2 (80). – С. 14-17.

43. Джура, Г. С. Кадры для цифровой экономики / А. В. Бутко, Г. С. Джура // Бизнес-инжиниринг сложных систем: модели, технологии, инновации : сб. материалов IV международ. науч.-практ. конф., г. Донецк-Екатеринбург, 14-16 ноября 2019 г. – Донецк: ДОННТУ, 2019. – С. 34-38.

44. Белозеров, О. И. Программно-технические аспекты функционирования систем обеспечения информационной безопасности / О. И. Белозеров, И. И. Топоркова // Вопросы науки и образования – 2018. – № 10 (22). – С. 45-47.

45. Ткачева, А. В. Информационная безопасность: понятие, виды угроз, примеры нарушений защиты / А.В. Лукьянчук, А.В. Ткачева // Донецкие чтения 2020: образование, наука, инновации, культура и вызовы современности: материалы V международ. науч. конф. (Донецк, 17-18 ноября 2020 г.). – Том 3: Экономические науки. Часть 2 / под общ. ред. проф. С.В. Беспаловой. – Донецк: Изд-во ДонНУ, 2020. – С. 394-396.

46. Захаров, С. В. Обеспечение информационной безопасности предприятий в трансформационной экономике / С.В. Захаров // Менеджер. – 2017. – № 1 (79). – С. 15-20.

47. Обеспечение информационной безопасности организаций банковской системы Российской Федерации/Общие положения [Электронный ресурс]: СТО БР ИББС-1.0-2014 [принят распоряжением Банка России 17 мая 2014 г. № Р-399: по состоянию на 18 июля 2020 г.] // Информационно-правовой портал ГАРАНТУ.РУ. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70567254/. – Дата обращения: 18.07.2020. – Загл. с экрана.

48. Кверевкина, Д. Г. Системный подход к менеджменту / Д. Г. Кверевкина // Символ науки. – 2016. – № 10 (1). – С. 113-121.

49. Белоножкин, В. И. Средства защиты информации в компьютерных системах: учебное пособие / В. И. Белоножкин, Г. А. Остапенко. – Воронеж: ВГТУ, 2005. – 337 с.

50. Пискунов, И. Классификация информационных активов: взгляд со стороны ИБ [Электронный ресурс] / И. Пискунов. – Режим доступа: https://ipiskunov.blogspot.com/2016/07/blog-post_0.html. – Дата обращения: 18.07.2020. – Загл. с экрана.

51. Framework for Improving Critical Infrastructure Cybersecurity [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf – Дата обращения: 18.07.2020. – Загл. с экрана.

52. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: приказ № 239: [утвержден Приказом Федеральной службы по техническому и экспортному контролю 25 декабря 2017 г.: по состоянию на 18 июля 2020 г.] // Федеральная служба по техническому и экспортному контролю. – Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239. – Дата обращения: 18.07.2020. – Загл. с экрана.

53. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования [Электронный ресурс]: ГОСТ Р ИСО/МЭК 27001-2006: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 27 декабря 2006 г. № 375-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006. – Дата обращения: 18.07.2020. – Загл. с экрана.

54. ISO 55000:2014 Asset management – Overview, principlesandterminology [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/55088.html. – Дата обращения: 18.07.2020. – Загл. с экрана.

55. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности [Электронный ресурс]: РС БР ИББС-2.2-2009: [принят распоряжением Банка России 11 ноября 2009 г. № Р-1190: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/902189338. – Дата обращения: 18.07.2020. – Загл. с экрана.

56. Буренин, А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А. Н. Буренин, К. Е. Легков // Наукоемкие технологии в космических исследованиях Земли. – 2015. – № 3. – С. 46-61.

57. Антопольский, А. Б. Информационные ресурсы России / А. Б. Антопольский – М.: НТЦ «Информрегистр» ИПКИР, 2004. – 330 с.

58. Собакин, И. Б. Идентификация активов как ключевых факторов риска информационной безопасности / И. Б. Собакин // Вопросы защиты информации. – 2011. – № 2 (93). – С. 45-49.

59. Мирошниченко, М. А. Информационная безопасность учета активов при сертификации систем менеджмента / М. А. Мирошниченко // Научный журнал КубГАУ. – 2015. – № 111 (07). – С. 1383-1393.

60. Жук, Е. И. Концептуальные основы информационной безопасности [Электронный ресурс] / Е. И. Жук // Машиностроение и компьютерные технологии. – 2010. – № 4. – Режим доступа: https://cyberleninka.ru/article/n/kontseptualnye-osnovy-informatsionnoy-bezopasnosti. – Дата обращения: 18.07.2020. – Загл. с экрана.

61. Челухин, В. А. Комплексное обеспечение информационной безопасности автоматизированных систем: учебное пособие / В. А. Челухин. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2014. – 207 с.

62. Процессы информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.uipdp.com/articles/2012-09/10.html. – Дата обращения: 18.07.2020. – Загл. с экрана.

63. Махалина, О. М. Цифровизация бизнеса увеличивает затраты на информационную безопасность / О. М. Махалина, В. Н. Махалин // Управление. – 2020. – № 1. – С. 134-140.

64. Белов, С. В. Методика системного анализа задач обеспечения информационной безопасности объектов критической информационной инфраструктуры / С. В. Белов, Т. М. Исламов // Методы и технические средства обеспечения безопасности информации – 2020. – № 29. – С. 120-121.

65. Кураленко, А. И. Методика аудита информационной безопасности информационно-телекоммуникационной системы: дис. … канд. техн. наук: 05.13.19: защищена 28.12.2015 / Кураленко Алексей Игоревич. – Томск, 2015. – 147 с.

66. Загорная, Т. О. Структурный анализ элементов цифровой экономики: инструменты, алгоритмы, тенденции / Т. О. Загорная, А. В. Ткачева // Новое в экономической кибернетике: сборник научных трудов. – Донецк: ГОУВПО «ДонНУ», 2018. – № 1. – С. 43-57.

67. Ободец, Р. В. Тенденции развития информационно-коммуникационной инфраструктуры в Донецкой Народной Республике / Р. В. Ободец, М. В. Иовенко // Сборник научных работ серии «Государственное управление». Вып. 14: Экономика и управление народным хозяйством / ГОУ ВПО «ДонАУиГС». – Донецк: ДонАУиГС, 2019. – С. 73-81.

68. Нежельский, А. А. Информационная безопасность государства и граждан в нем: ключевые компоненты и группы интересов / А. А. Нежельский // Азимут научных исследований: экономика и управление. – 2017. – № 3 (20). – С. 404-408.

69. Шамсутдинов, Р. Р. Обеспечение безопасности информационных технологий в банковских организациях Российской Федерации / Р. Р. Шамсутдинов // Colloquium-journal. – 2019. – № 3 (27). – С. 50-52.

70. Джура, Г. С. Анализ зарубежного и отечественного опыта формирования государственной системы обеспечения информационной безопасности / Г. С. Джура, Е.А. Шумаева // Стратегия интеграционного антикризисного развития социально-экономических систем: научно-прикладной аспект: монография / [О. Н. Шарнопольская, Е. Г. Курган, Е. А. Шумаева и др.]; под науч. ред. О. Н. Шарнопольской ; ГОУВПО «ДОННТУ». – Донецк: ДОННТУ, 2021. – Р. 4. – С. 52-77.

71. Машкина, И. В. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем / И. В. Машкина, А. Ю. Сенцова, Р. М. Гузаиров, В. Е. Кладов // Известия Южного федерального университета. Технические науки. – 2011. – С. 25-35.

72. Шилкина, А. Т. Тенденции развития риск ориентированного подхода в контексте индустрии 4.0 / А. Т. Шилкина, О. Е. Варакина // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. – 2019. – № 1. – С. 9-20.

73. Лонцих, П. А. Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии / П. А. Лонцих, О. М. Сафонова // Системы. Методы. Технологии. – 2020. – № 4 (48). – С. 80-87.

74. Соколов, Д. В. Обеспечение информационной безопасности органами государственной власти на территории субъектов Российской Федерации [Электронный ресурс] / Д. В. Соколов // Теория и практика общественного развития. – Режим доступа: http://teoria-practica.ru/rus/files/arhiv_zhurnala/2015/10/law/sokolov.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

75. Назыров, М. В. Особенности применения процессного подхода в обеспечении информационной безопасности инновационной организации / М. В. Назыров // Альманах научных работ молодых ученых университета ИТМО:

XLVIII науч. и учеб.-метод. конф. Университета ИТМО (г. Санкт-Петербург, 29 янв. 2019 г.). – Санкт-Петербург: ИТМО, 2019. – С. 158-162.

76. NIST Special Publication 800-61 Revision 2 Computer Security Incident Response Team (CSIRT) [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

77. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: Приказ Федеральной службы по техническому и экспортному контролю России № 17 от 11 февраля 2013 г.: по состоянию на 18 июля 2020 г. // Федеральная служба по техническому и экспортному контролю. – Режим доступа: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/53-normotvorcheskaya/akty/prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17. – Дата обращения: 18.07.2020. – Загл. с экрана.

78. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования [Электронный ресурс]: Приказ Федеральной службы по техническому и экспортному контролю России № 235 от 21 декабря 2017 г.: по состоянию на 18 июля 2020 г. // Федеральная служба по техническому и экспортному контролю. – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1589-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-236. – Дата обращения: 18.07.2020. – Загл. с экрана.

79. Агафонова, М. Е. К вопросу о проведении внутреннего аудита системы менеджмента информационной безопасности / М. Е. Агафонова, И. Ю. Шахалов // Вопросы кибербезопасности. – 2013. – № 3. – С. 2-7.

80. Information Systems Security Assessment Framework (ISSAF) draft 0.2 [Электронный ресурс]. – Режим доступа: https://untrustednetwork.net/files/issaf0.2.1.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

81. ITIL 4 edition [Электронный ресурс]. – Режим доступа: https://www.axelos.com/store/book/itil-foundation-itil-4-edition. – Дата обращения: 18.07.2020. – Загл. с экрана.

82. COBIT 5 FRAMEWORK [Электронный ресурс]. – Режим доступа:https://www.isaca.org/resources/cobit/cobit-5#sort=relevancy. – Дата обращения: 18.07.2020. – Загл. с экрана.

83. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. – Дата обращения: 18.07.2020. – Загл. с экрана.

84. Сказ о том, почему цикл PDCA плохо работает в ИБ [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/Business_without_danger/294633.php. – Дата обращения: 18.07.2020. – Загл. с экрана.

85. Размышления о PDCA (Цикл Деминга) [Электронный ресурс]. – Режим доступа: https://ipiskunov.blogspot.com/2016/05/pdca_5.html. – Дата обращения: 18.07.2020. – Загл. с экрана.

86. ISO 27001:2013 INFORMATION SECURITY IMPLEMENTATION GUIDE [Электронный ресурс]. – Режим доступа: https://www.isaca.de/sites/default/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

87. Иншакова, Е. Г. "Электронное правительство" в публичном управлении: административно-правовые проблемы организации и функционирования: дис. ... канд. юрид. наук: 12.00.14 / Иншакова Екатерина Геннадьевна. – Москва, 2015. – 213 с.

88. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management [Электронный ресурс]. – Режим доступа: https://www.iso.org/ru/standard/75281.html. – Дата обращения: 18.07.2020. – Загл. с экрана.

89. Исаев, А. С. Метод и модель управления информационной безопасностью на основе динамических экспертных систем поддержки принятия решений: дис. ... канд. техн. наук: 05.13.19: защищена 20.05.2015 / Исаев Александр Сергеевич. – Санкт-Петербург, 2015. – 187 с.

90. Дорофеев, А. В. Менеджмент информационной безопасности: основные концепции / А. В. Дорофеев, А. С. Марков // Вопросы кибербезопасности. – 2014. – № 1 (2). – С. 67-73.

91. Арутюнов, В. В. Современные проблемы и задачи обеспечения информационной безопасности / В. В. Арутюнов // Вестник Московского финансово-юридического университета. – 2014. – № 3. – С. 140-146.

92. Попов, С. В. О влиянии состояний функционирования средств защиты информации на эффективность мониторинга инцидентов информационной безопасности банка / С. В. Попов, В. Н. Шамкин // Вестник Тамбовского государственного технического университета. – 2011. – № 2. – С. 297-303.

93. Дорофеев, А. В. Планирование обеспечения непрерывности бизнеса и восстановления / А. В. Дорофеев, А. С. Марков // Вопросы кибербезопасности. – 2015. – № 3 (11). – С. 68-73.

94. Мамушкина, Н. В. Внутренний аудит как эффективный метод управления организацией / Н. В. Мамушкина // Вестник НГИЭИ. – 2013. – № 1 (20). – С. 48-63.

95. Козьминых, С. И. Аудит информационной безопасности / С. И. Козьминых, П. С. Козьминых // Вестник Московского университета МВД России – 2016. – № 1. – С. 181-186.

96. Хлестова, Д. Р. Аудит информационной безопасности в организации / Д. Р. Хлестова, Ф. Т. Байрушин // Символ науки. – 2016. – № 11-3. – С. 175-176.

97. Алексеева, Л. Н. Система информационной безопасности органов государственной власти как основа современного государственного управления / Л. Н. Алексеева // Вестник университета. – 2015. – № 13. – С. 5-9.

98. Мурашкина, А. А. Совершенствование системы информационной безопасности в органах государственной власти / А. А. Мурашкина // Символ науки. – 2018. – № 11. – С. 34-36.

99. Терещенко, Л. К. Информационная безопасность органов исполнительной власти на современном этапе / Л. К. Терещенко, О. Г Тиунов // Журнал российского права. – 2015. – № 8. – С. 100-109.

100. Лившиц, И. И. Методы оценки защищенности систем менеджмента информационной безопасности, разработанных в соответствии с требованиями международного стандарта ИСО/МЭК 27001:2005: дис. ... канд. техн. наук: 05.13.19: защищена 28.06.2012 / Лившиц Илья Иосифович. – Санкт-Петербург, 2012. – 187 с.

101. Сагитова, В. В. Модели и алгоритмы анализа информационных рисков при проведении аудита безопасности информационной системы персональных данных: дис. ... канд. техн. наук: 05.13.19: защищена 14.06.2019 / Сагитова Валентина Владимировна. – Уфа, 2019. – 229 с.

102. Макаренко, С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С. И. Макаренко // Системы управления, связи и безопасности. – 2018. – № 1. – С. 1-29.

103. Джура, Г. С. Инновационные подходы к созданию единого государственного информационного пространства / Г. С. Джура, Е. А. Шумаева // Государственное управление инновациями: проблемы, технологии, перспективы: сб. материалов II международ. науч.-практ. конф., г. Донецк, 14 апреля 2016 г. – Донецк: ДонНТУ, 2016. – С. 86-88.

104. Jura, G. S. Características de la formación y el desarrollo del espacio de información uniforme del estado (Особенности формирования и развития единого государственного информационного пространства) / E. A. Shumaeva, G. S. Jura // Área Académica de Administración de Empresas, IESTP Simón Bolívar Revista Gerencia. – 2017. – VOL. 2, NÚM. 1. – P. 36-41.

105. Джура, Г. С. Проблемы безопасности информационных систем органов государственного управления / Е. А. Шумаева, Г. С. Джура // Сборник

научных работ серии «Экономика». Вып. 10: Проблемы и перспективы развития социально-экономических систем / ГОУ ВПО «ДонАУиГС». – Донецк: ДонАУиГС, 2018. – С. 178-187.

106. Джура, Г. С. Оценка уровня кибербезопасности организации при формировании бюджета на систему обеспечения информационной безопасности / Е. А. Шумаева, Г. С. Джура // Стратегия устойчивого развития в антикризисном управлении экономическими системами: материалы VI международ. науч.-практ. конф., г. Донецк, 8 апреля 2020 г. / отв. ред. О.Н. Шарнопольская, И.А. Кондаурова, Е.Г. Курган ; ГОУВПО «ДОННТУ». – Донецк: ДОННТУ, 2020. – С. 489-496.

107. Господарик, Ю. П. Международная экономическая безопасность / Ю. П. Господарик, М. В. Пашковская. – М.: Университет «Синергия», 2016. – 416 с.

108. Schreier, F. Cybersecurity: The Road Ahead. Geneva Centre for the Democratic Control of Armed Forces (DCAF) [Электронный ресурс] / F. Schreier, B. Weekes, T.H. Winkler // DCAF Horizon 2015. – Working Paper №. 4 – Режим доступа: ttps://dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf. – Дата обращения: 14.06.2018. – Загл. сэкрана.

109. Кандрава, Н. В. Политика обеспечения кибербезопасности в Европейском Союзе: национальный и наднациональный уровни / Н. В. Кандрава // Каспийский регион: политика, экономика, культура. – 2019. – № 3 (60). – С. 73-78.

110. Джура, Г. С. Опыт государственного регулирования защиты персональных данных в странах Европейского Союза / Е. А. Шумаева, Г. С. Джура // Сборник научных работ серии «Государственное управление». Вып. 17: Экономика и управление народным хозяйством / ГОУ ВПО «ДонАУиГС». – Донецк: ДонАУиГС, 2020. – С. 87-99.

111. Джура, Г. С. Информационное право как инструмент обеспечения информационной безопасности государства / К. А. Пьянков, Г. С. Джура, Е. С. Декунова // Современное государственное и муниципальное управление:

проблемы, технологии, перспективы: сб. материалов V международ. науч.-практ. конф., г. Донецк, 25 апреля 2019 г. – Донецк, ДонНТУ, 2019. – С. 298-303.

112. Джура, Г. С. Информационное право как инструмент обеспечения кибербезопасности государства / Е. А. Шумаева, Г. С. Джура // Информационные технологии и информационная безопасность в науке, технике и образовании "ИНФОТЕХ – 2019": сборник статей всероссийской науч.-техн. конф., г. Севастополь, 18-20 сентября 2019 г. / М-во науки и высшего образования РФ, Севастопольский государственный университет; науч. ред. Е. Н. Мащенко. – г. Севастополь: СевГУ, 2019. – С. 98-103.

113. Киселева, Н. В. Организационно-правовая основа обеспечения информационной безопасности США / Н. В. Киселева // Академический вестник Ростовского филиала Российской таможенной академии. – 2019. – № 2 (35). – С. 101-109.

114. США потратят $10 миллиардов на «защиту нации» в Интернете [Электронный ресурс]. – Режим доступа: https://www.cnews.ru/news/top/2019-03-13_tramp_prosit_u_kongressa_milliardy_na_zashchitu. – Дата обращения: 18.07.2020. – Загл. с экрана.

115. В США принят план защиты информационных систем [Электронный ресурс]. – Режим доступа: http://ww-4.narod.ru/warfare/levakov/page003.htm. – Дата обращения: 18.07.2020. – Загл. с экрана.

116. Большой свод законов США // 115 Stat. 272 (2001) / Public Law 107-56-Oct. 26, 2001 [Электронный ресурс]. – Режим доступа: https://www.govinfo.gov/app/details/PLAW-107publ56. – Дата обращения: 18.07.2020. – Загл. с экрана.

117. Ковалева, Т. К. Критическая инфраструктура в системе обеспечения национальной безопасности США / Т. К. Ковалева // Инновации и инвестиции. – 2019. – № 9. – С. 81-89.

118. Конгресс США [Электронный ресурс]. – Режим доступа: https://www.govtrack.us/congress/bills/107/ hr5005. – Дата обращения: 10.10.2018. – Загл. с экрана.

119. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. February, 2003. P. 71. Официальный сайт архивных документов Белого дома США [Электронный ресурс]. – Режим доступа: https://georgewbushwhitehouse.archives.gov/pcipb/physical.html. – Дата обращения: 18.09.2019. – Загл. с экрана.

120. National Strategy to Secure Cyberspace [Электронный ресурс]. – Режим доступа: https://gssd.mit.edu/search-gssd/site/national-strategy-secure-cyberspace-60366-sun-06-16-2013-1544. – Дата обращения: 18.07.2020. – Загл. с экрана.

121. Сравнительный анализ подходов к регулированию критической информационной инфраструктуры [Электронный ресурс]. – Режим доступа: https://internetpolicy.kg/wp-content/uploads/2020/03/Сравнительный-анализ-подходов-к-регулированию-критической-информационной-инфраструктуры.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

122. Официальный сайт Министерства юстиции США (Department of Justice, DOJ) [Электронный ресурс]. – Режим доступа: https://www.justice.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

123. Официальный сайт Федерального бюро Расследований США (Federal Bureau of Investigation, FBI) [Электронный ресурс]. – Режим доступа: https://www.fbi.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

124. Официальный сайт Национальной объединенной рабочей группы по кибер-расследованиям США (National Cyber Investigative Joint Task Force, NCIJTF) [Электронный ресурс]. – Режим доступа: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. – Дата обращения: 18.07.2020. – Загл. с экрана.

125. Официальный сайт Министерства внутренней безопасности США (Department of Homeland Security, DHS) [Электронный ресурс]. – Режим доступа: https://www.dhs.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

126. Официальный сайт Министерства обороны США (Department of Defense, DoD) [Электронный ресурс]. – Режим доступа: https://www.defense.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

127. Официальный сайт Агентства кибербезопасности и защиты инфраструктуры США (Cyber security and Infrastructure Security Agency, CISA) [Электронный ресурс]. – Режим доступа: https://www.cisa.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

128. Официальный сайт Федеральной комиссии по связи США (Federal Communications Commission) [Электронный ресурс]. – Режим доступа: https://www.fcc.gov/. – Дата обращения: 18.07.2020. – Загл. с экрана.

129. Официальный сайт Национальной совместной рабочей группы по кибер-расследованиям США (National Cyber Investigative Joint Task Force, NCIJTF) [Электронный ресурс]. – Режим доступа: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. – Дата обращения: 18.07.2020. – Загл. с экрана.

130. Официальный сайт Национального института стандартов и технологий (NIST) [Электронный ресурс]. – Режим доступа: https://www.nist.gov/.– Дата обращения: 18.07.2020. – Загл. с экрана.

131. Володин, В.М. обеспечение безопасности России и США в информационном и кибер-пространстве: правовые, политические и экономические аспекты / В. М. Володин, Л. В. Рожкова, О. В. Сальникова // Право и управление. XXI век. – 2017. – № 4. – С. 59-68.

132. Рудевич, И. Персональные данные. Валюта XXI века [Электронный ресурс] / И. Рудевич, А. Рудевич. – Режим доступа: https://iz.ru/805131/irina-rudevich-aleksei-rudevich/personalnye-dannye-valiuta-xxi-veka. – Дата обращения: 29.10.2018. – Загл. с экрана.

133. Overview GDPR [Электронный ресурс]. – Режим доступа: https://gdpr.eu/. – Дата обращения: 29.10.2018. – Загл. с экрана.

134. О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза [Электронный ресурс]: Директива ЕС № 2016/1148: [утверждена Европейским Парламентом и Советом Европейского Союза 6 июля 2016 г.: по состоянию на 29 октября 2018 г.] // Информационно-

правовое обеспечение Гарант. – Режим доступа: http://base.garant.ru/71737658/. – Дата обращения: 29.10.2018. – Загл. с экрана.

135. Официальный сайт European Union Agency for Cyber security (ENISA) [Электронный ресурс]. – Режим доступа: https://www.enisa.europa.eu/. – Дата обращения: 29.10.2018. – Загл. с экрана.

136. Официальный сайт European Cybercrime Centre [Электронный ресурс]. – Режим доступа: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3. – Дата обращения: 29.10.2018. – Загл. с экрана.

137. Официальный сайт European Data Protection Supervisor [Электронный ресурс]. – Режим доступа: https://edps.europa.eu/. – Дата обращения: 29.10.2018. – Загл. с экрана.

138. Официальный сайт NIS Cooperation Group [Электронный ресурс]. – Режим доступа: https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. – Дата обращения: 29.10.2018. – Загл. с экрана.

139. Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions [Электронный ресурс]. – Режим доступа: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf. – Дата обращения: 29.10.2018. – Загл. сэкрана.

140. Outcome of proceedings [Электронный ресурс]. – Режим доступа: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf#:~:text=The%20EU%20Cyber%20Defence%20Policy%20Framework%20(CDPF)%20supports%20the%20development,legislation%2C%20including%2C%20when%20it%20is. – Дата обращения: 29.10.2018. – Загл. с экрана.

141. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions [Электронный ресурс]. – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192& from=EN. – Дата обращения: 29.10.2018. – Загл. с экрана.

142. ЕС провел очередные киберучения – самые масштабные за всю историю [Электронный ресурс]. – Режим доступа: http://d-russia.ru/es-provel-

ocherednye-kiberucheniya-samye-masshtabnye-za-vsyu-istoriyu.html. – Дата обращения: 29.10.2018. – Загл. с экрана.

143. Директива по сетевой и информационной безопасности от 18 декабря 2015 г. [Электронный ресурс]. – Режим доступа: https://www.enisa. europa.eu/topics/nis-directive. – Дата обращения: 29.10.2018. – Загл. с экрана.

144. OSSTMM 3 – The Open Source Security Testing Methodology Manual. – Режим доступа: https://www.isecom.org/OSSTMM.3.pdf. – Дата обращения: 29.10.2020. – Загл. с экрана.

145. Пантин, В. И. Кибербезопасность: проблемы формирования единой политики в Европейском союзе / В. И. Пантин, Н. В. Кардава // Вестник Пермского университета. Политология. – 2018. – № 3. – С. 5-18.

146. National Plan for Information Infrastructure Protection [Электронный ресурс]. – Режим доступа: https://www.qcert.org/sites/default/files/ public/documents/GER-PL-National%20Plan%20For%20Information%20 Infrastructure%20Protection-Eng-2005.pdf. – Дата обращения: 29.10.2018. – Загл. с экрана.

147. CIP Implementation Plan of the National Plan for Information Infrastructure Protection [Электронный ресурс]. – Режим доступа: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation %20Plan.pdf?__blob=publicationFile. – Дата обращения: 29.10.2018. – Загл. с экрана.

148. Cyber-Sicherheits strategiefür Deutschland [Электронный ресурс]. – Режим доступа: http://www.bmi.bund.de/cybersicherheitsstrategie/BMICyber SicherheitsStrategie.pdf. – Дата обращения: 29.10.2018. – Загл. с экрана.

149. The Evolution of German Cybersecurity Strategy [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/326511119_The_ Evolution_of_German_Cybersecurity_Strategy. – Дата обращения: 29.10.2018. – Загл. с экрана.

150. Gesetzzur Erhöhung der Sicherheit in formation stechnischer Systeme (IT-Sicherheitsgesetz – ITSG k.a.Abk.) [Электронный ресурс]. – Режим доступа:

http://www.buzer.de/gesetz/11682/a193756.htm. – Дата обращения: 29.10.2018. – Загл. с экрана.

151. Act on the Federal Office for Information Security (BSI Act – BSIG). [Электронный ресурс]. – Режим доступа: https://www.gesetze-iminternet.de/englisch_bsig/englisch_bsig.html. – Дата обращения: 29.10.2018. – Загл. с экрана.

152. О защите физических лиц применительно к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, и о свободном движении таких данных [Электронный ресурс]: Директива ЕС 2016/680: [утверждена Европейским Парламентом и Советом Европейского Союза 27 апреля 2016 г.: по состоянию на 29 октября 2018 г.] // Информационно-правовое обеспечение Гарант. – Режим доступа: https://base.garant.ru/71936226/. – Дата обращения: 29.10.2018. – Загл. с экрана.

153. Strafgesetzbuch (StGB) [Электронный ресурс]. – Режим доступа: https://www.gesetze-im-internet.de/stgb/index.html#BJNR001270871BJNE0684 03123. – Дата обращения: 29.10.2018. – Загл. с экрана.

154. Act to Strengthen the Security of Federal Information Technology [Электронный ресурс]. – Режим доступа: https://www.bsi.bund.de/EN/TheBSI/ BSIAct/bsiact_node.html. – Дата обращения: 29.10.2018. – Загл. с экрана.

155. Хатауэй, М. Киберготовность Германии: краткий обзор [Электронный ресурс] / М. Хатауэй, К. Демчак, Д. Кербен, Д. МакАрдл, Ф. Спидальери. – Режим доступа: https://analytica.digital.report/wp-content/uploads/2017/05/CRI-Germany-RU.pdf. – Дата обращения: 29.10.2018. – Загл. с экрана.

156. National cybersecurity and cyberdefense policy snapshots Zürich, September 2018 Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH Zürich [Электронный ресурс]. – Режим доступа:https://css.ethz.ch/ content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf. – Дата обращения: 29.10.2018. – Загл. с экрана.

157. Джура, Г. С. Оценка эффективности национальных стратегий кибербезопасности / Е. А. Шумаева, Г. С. Джура // Инновационные перспективы Донбасса: материалы VI международ. науч.-практ. конф., г. Донецк, 26-28 мая 2020 г. – Донецк: ДонНТУ, 2020. Т. 5: 5. Актуальные проблемы инновационного развития экономики Донбасса. – 2020. – С. 164-170.

158. CERT-Bund [Электронный ресурс]. – Режим доступа: https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html. – Дата обращения: 29.10.2018. – Загл. с экрана.

159. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы [Электронный ресурс]: Указ Президента Российской Федерации от 09 мая 2017 г. № 203: по состоянию на 29 октября 2018 г. // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_216363/. – Дата обращения: 29.10.2018. – Загл. с экрана.

160. Военная доктрина Российской Федерации [Электронный ресурс]: [утверждена указом Президента Российской Федерации 25 декабря 2014 г. № Пр-2976: по состоянию на 18 июля 2020 г.] // Информационно-правовое обеспечение Гарант. – Режим доступа: https://base.garant.ru/70830556/. – Дата обращения: 18.07.2020. – Загл. с экрана.

161. Конституция Российской Федерации [Электронный ресурс]: [принята всенародным голосованием 12.12.1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/. – Дата обращения: 18.07.2020. – Загл. с экрана.

162. Гражданский кодекс Российской Федерации [Электронный ресурс]: [принят Государственной Думой 21 октября 1994 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/. – Дата обращения: 18.07.2020. – Загл. с экрана.

163. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс]: [принят Государственной Думой 20 декабря 2001 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34661/. – Дата обращения: 18.07.2020. – Загл. с экрана.

164. Уголовный кодекс Российской Федерации [Электронный ресурс]: [принят Государственной Думой 24 мая 1996 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/. – Дата обращения: 18.07.2020. – Загл. с экрана.

165. О безопасности [Электронный ресурс]: Федер. закон № 390-ФЗ: [принят Государственной Думой 7 декабря 2010 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_108546/. – Дата обращения: 18.07.2020. – Загл. с экрана.

166. О государственной тайне [Электронный ресурс]: закон Российской Федерации № 5485-1: [принят Домом Советов России 21 июля 1993 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/. – Дата обращения: 18.07.2020. – Загл. с экрана.

167. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: Федер. закон № 149-ФЗ: [принят Государственной Думой 8 июля 2006 г.: одобр. Советом Федерации 14 июля 2016 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. – Дата обращения: 18.07.2020. – Загл. с экрана.

168. Об электронной подписи [Электронный ресурс]: Федер. закон № 63-ФЗ: [принят Государственной Думой 25 марта 2011 г.: одобр. Советом Федерации 30 марта 2011 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая

система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/. – Дата обращения: 18.07.2020. – Загл. с экрана.

169. О техническом регулировании [Электронный ресурс]: Федер. закон № 184-ФЗ: [принят Государственной Думой 15 декабря 2002 г.: одобр. Советом Федерации 18 декабря 2002 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/. – Дата обращения: 18.07.2020. – Загл. с экрана.

170. О связи [Электронный ресурс]: Федер. закон № 126-ФЗ: [принят Государственной Думой 18 июня 2003 г.: одобр. Советом Федерации 25 июня 2003 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/. – Дата обращения: 18.07.2020. – Загл. с экрана.

171. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федер. закон № 187-ФЗ: [принят Государственной Думой 12 июля 2017 г.: одобр. Советом Федерации 19 июля 2017 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_ 220885/. – Дата обращения: 18.07.2020. – Загл. с экрана.

172. Джура, Г. С. Анализ правовых и институциональных аспектов функционирования государственной системы информационной безопасности Российской Федерации / Г. С. Джура // Актуальные проблемы обеспечения национальной безопасности: материалы международ. науч.-практ. конф., г. Донецк, 17 декабря 2020 г. / под общей редакцией С.В. Беспаловой. – Донецк: Изд-во ДонНУ, 2021. – С. 164-174.

173. О Федеральной службе безопасности [Электронный ресурс]: Федер. закон № 40-ФЗ: [принят Государственной Думой 22 февраля 1995 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6300/. – Дата обращения: 18.07.2020. – Загл. с экрана.

174. О Министерстве связи и массовых коммуникаций Российской Федерации [Электронный ресурс]: Постановление Правительства Российской Федерации № 418 [принят Правительством Российской Федерации 02 июня 2008 г.: по состоянию на 18 июля 2020 г.] // Министерство связи и массовых коммуникаций Российской Федерации. – Режим доступа: https://digital.gov.ru/ru/documents/3227/. – Дата обращения: 18.07.2020. – Загл. с экрана.

175. О Центральном банке Российской Федерации (Банке России) [Электронный ресурс]: Федер. закон № 86-ФЗ: [принят Государственной Думой 27 июня 2002 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_37570/. – Дата обращения: 18.07.2020. – Загл. с экрана.

176. О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]: Постановление Правительства Российской Федерации № 228 [принят Правительством Российской Федерации 16 марта 2009 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_85889/. – Дата обращения: 18.07.2020. – Загл. с экрана.

177. О Федеральной службе по техническому и экспортному контролю [Электронный ресурс]: Указ Президента № 1085 [утверждено Президентом Российской Федерации от 16 августа 2004 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_14031/b4771b0410795ff8f613586883b317d567990cc7/. – Дата обращения: 18.07.2020. – Загл. с экрана.

178. О Национальном координационном центре по компьютерным инцидентам [Электронный ресурс]: приказ ФСБ Российской Федерации № 366 [утверждено Федеральной службой безопасности Российской Федерации 24 июля 2018 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_

doc_LAW_306334/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/. – Дата обращения: 18.07.2020. – Загл. с экрана.

179. Джура, Г. С. Проблемы лицензирования в сфере информационной безопасности в Российской Федерации / Е. А. Шумаева, Г. С. Джура // Стратегия устойчивого развития в антикризисном управлении экономическими системами: материалы V международ. науч.-практ. конф., г. Донецк, 17 апреля 2019 г. / отв. ред. О.Н. Шарнопольская, И.А. Кондаурова, Е.Г. Курган / ГОУВПО ДОННТУ. – Донецк: ДОННТУ, 2019. – С. 305-312.

180. Global Cybersecurity Index (GCI) 2018 [Электронный ресурс]. – Режим доступа: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

181. Global Cybersecurity Index (GCI) 2017 [Электронный ресурс]. – Режим доступа: https://nonews.co/wp-content/uploads/2018/09/ITU2017.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

182. Глобальный индекс кибербезопасности и профили по киберблагополучию за 2015 г. [Электронный ресурс]. – Режим доступа: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

183. Джура, Г. С. Информационная безопасность. Перспективы и вызовы / Г. С. Джура // Программная инженерия: методы и технологии разработки информационно-вычислительных систем (ПИИВС-2018): сб. науч. трудов II международ. науч.-практ. конф., г. Донецк, 14-18 ноября 2018 г. Том. 1. – Донецк, ГОУВПО «Донецкий национальный технический университет», 2018. – С. 82-88.

184. План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

185. Об информации и информационных технологиях [Электронный ресурс]: Закон Донецкой Народной Республики № 71-IНС: [принят Постановлением Народного Совета 07 августа 2015 г.: по состоянию на 18 июля

2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakonodatelnaya-deyatelnost/prinyatye/zakony/zakon-donetskoj-narodnoj-respubliki-ob-informatsii-i-informatsionnyh-tehnologiyah/. – Дата обращения: 18.07.2020. – Загл. с экрана.

186. О персональных данных [Электронный ресурс]: Закон Донецкой Народной Республики № 61-IНС: [принят Постановлением Народного Совета 19 июня 2015 г.: по состоянию на 18 июля 2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakon-donetskoj-narodnoj-respubliki-o-personalnyh-dannyh/. – Дата обращения: 18.07.2020. – Загл. с экрана.

187. О безопасности [Электронный ресурс]: Закон Донецкой Народной Республики № 04-IНС: [принят Постановлением Народного Совета 12 декабря 2014 г.: по состоянию на 18 июля 2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakon-dnr-o-bezopasnoste/. – Дата обращения: 18.07.2020. – Загл. с экрана.

188. О Министерстве государственной безопасности [Электронный ресурс]: Закон Донецкой Народной Республики № 238-IНС: [принят Постановлением Народного Совета 03 августа 2018 г.: по состоянию на 18 июля 2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su//zakonodatelnaya-deyatelnost/prinyatye/zakony/zakon-donetskoj-narodnoj-respubliki-o-ministerstve-gosudarstvennoj-bezopasnosti/. – Дата обращения: 18.07.2020. – Загл. с экрана.

189. Об утверждении Положения о Министерстве связи Донецкой Народной Республики [Электронный ресурс]: Постановление № 22-6: [принят Постановлением Правительства Донецкой Народной Республики 30 апреля 2020 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0030-22-6-20200430/. – Дата обращения: 18.07.2020. – Загл. с экрана.

190. Об утверждении Положения о Министерстве информации Донецкой Народной Республики [Электронный ресурс]: Постановление № 1-18: [принят Постановлением Правительства Донецкой Народной Республики 10 января 2015 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0003-1-18-20150110/. – Дата обращения: 18.07.2020. – Загл. с экрана.

191. Об утверждении Положения о Центральном Республиканском Банке и других вопросах его деятельности [Электронный ресурс]: Постановление № 8-2: [принят Постановлением Правительства Донецкой Народной Республики 06 мая 2015 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0009-8-2-20150506/. – Дата обращения: 18.07.2020. – Загл. с экрана.

192. Правительство Донецкой Народной Республики утвердило Распоряжение «О создании межведомственной комиссии по информационной безопасности Донецкой Народной Республики» [Электронный ресурс]. – Режим доступа: http://dnr-live.ru/pravitelstvom-sozdana-komissiya-po-informatsionnoy-bezopasnosti-dnr/. – Дата обращения: 18.07.2020. – Загл. с экрана.

193. Об утверждении Положения о Министерстве юстиции Донецкой Народной Республики [Электронный ресурс]: Указ № 158: [принят Главой Донецкой Народной Республики 27 мая 2019 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0001-158-20190527/. – Дата обращения: 18.07.2020. – Загл. с экрана.

194. Тютин, А. В. Организационно-методический аспект совершенствования подсистемы информационной безопасности объектов промышленного комплекса региона: дис. ... канд. экон. наук: 08.00.05: защищена 30.04.2004 / Тютин Антон Витальевич. – Иваново, 2004. – 102 с.

195. Трунова, А. В. Обеспечение информационной безопасности предприятия / А. В. Трунова, // Современные инновации. – 2018. – № 4 (26). – С. 33-35.

196. О центральном республиканском банке Донецкой Народной Республики [Электронный ресурс]: Закон Донецкой Народной Республики № 32-IHC: [принят Постановлением Народного Совета 26 апреля 2019 г.: по состоянию на 18 июля 2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakonodatelnaya-deyatelnost/prinyatye/zakony/zakon-donetskoj-narodnoj-respubliki-o-tsentralnom-respublikanskom-banke-donetskoj-narodnoj-respubliki/. – Дата обращения: 18.07.2020. – Загл. с экрана.

197. О лицензировании отдельных видов хозяйственной деятельности [Электронный ресурс]: Закон Донецкой Народной Республики № 18-IHC: [принят Постановлением Народного Совета 27 февраля 2015 года: по состоянию на 12 января 2021 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakon-dnr-o-litsenzirovanii/. – Дата обращения: 12.01.2021. – Загл. с экрана.

198. Конституция Донецкой Народной Республики [Электронный ресурс]: Постановление № 1-1: [принята Постановлением Верховного Совета Донецкой Народной Республики 14 мая 2014 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики – Режим доступа: https://gisnpa-dnr.ru/npa/0002-106-iihc-20200306/. – Дата обращения: 18.07.2020. – Загл. с экрана.

199. Global cybersecurityindex v4 [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. – Дата обращения: 18.07.2020. – Загл. с экрана.

200. Программа МСЭ/БРЭ в области кибербезопасности Группа экспертов по определению весовых коэффициентов для GCI Круг ведения Август 2020 года [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/Expert-Meeting/weightage%20Expert%20Group%

20Terms%20of%20Reference%20Russian.pdf. – Дата обращения: 18.07.2020. – Загл. с экрана.

201. Преимущества риск-ориентированного подхода к управлению информационной безопасностью [Электронный ресурс]. – Режим доступа: http://анализ-риска.рф/content/preimushchestva-risk-orientirovannogo-podhoda-k-upravleniyu-informacionnoy-bezopasnostyu. – Дата обращения: 18.07.2020. – Загл. с экрана.

202. Созинова, Е. Н. Риск-ориентированный подход к проведению аудита информационной безопасности / Е. Н. Созинова, А. А. Медведев // Научно-технический вестник Поволжья. – 2015. – № 3. – С. 215-217.

203. Джура, Г. С. Особенности оценки рисков информационной безопасности в современных организациях / Г. С. Джура // Сборник научных работ серии «Государственное управление». Вып. 19: Экономика и управление народным хозяйством / ГОУ ВПО «ДонАУиГС». – Донецк: ДонАУиГС, 2020. – С. 211-218.

204. Пугин, В. В. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В. В. Пугин, О. Ю. Губарева // T-Comm. Телекоммуникации и Транспорт. – 2012. – № 6. – С. 54-57.

205. Плетнев, П. В. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса / П. В. Плетнев, В. М. Белов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1-2 (25). – С. 83-86.

206. Одинцова, М. А. Методика управления рисками для малого и среднего бизнеса / М. А. Одинцова // Экономический журнал. – 2014. – № 3 (35). – С. 38-47.

207. Глушенко, С. А. Применение системы Matlab для оценки рисков информационной безопасности организации / С. А. Глущенко // Бизнес-информатика. – 2013. – № 4 (26). – С. 35-42.

208. Губарева, О. Ю. Оценка рисков информационной безопасности в телекоммуникационных сетях / О. Ю. Губарева // Вестник Волжского университета им. В.Н. Татищева. – 2013. – № 2 (21). – С. 76-81.

209. Ильченко, Л. М. Расчет рисков информационной безопасности телекоммуникационного предприятия / Л. М. Ильченко, Е. К. Брагина, И. Э. Егоров // Открытое образование. – 2018. – № 2. – С. 61-70.

210. Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс]. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g. – Дата обращения: 05.02.2021. – Загл. с экрана.

211. База данных угроз Федеральной службы по техническому и экспортному контролю Российской Федерации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat. – Дата обращения: 18.07.2020. – Загл. с экрана.

212. Калькулятор CVSS V3.1 [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/calc31. – Дата обращения: 18.07.2020. – Загл. с экрана.

213. NVD VulnerabilitySeverity Ratings (CVSS v 3.0) [Электронный ресурс]. – Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss. – Дата обращения: 18.07.2020. – Загл. с экрана.

214. Аникин, И. В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики: дис. …д-ра техн. наук: 05.13.19: защищена 30.03.2018 / Аникин Игорь Вячеславович. – Казань, 2017. – 278 с.

215. The Security Risk Management Guide [Электронный ресурс]. – Режим доступа: http://www.microsoft.com/en-us/download/details.aspx?id=6232. – Дата обращения: 18.07.2020. – Загл. с экрана.

216. Куканова, Н. Современные методы и средства анализа и управление рисками информационных систем компаний [Электронный ресурс] / Н. Куканова // CIT FORUM. – Режим доступа: http://citfomm.rn/products/dsec/ cramm. – Дата обращения: 18.04.2017. – Загл. с экрана.

217. Управление рисками. Метод CRAMM [Электронный ресурс]. – Режим доступа: http://www.itexpert.ru/ms/ITEMS/77-33. – Дата обращения: 18.04.2017. – Загл. с экрана.

218. Легчекова, Е. В. Метод расчета риска информационной безопасности [Электронный ресурс] / Е. В. Легчекова, О. В. Титов. – Режим доступа: https://core.ac.uk/download/pdf/145189961.pdf. – Дата обращения: 18.04.2017. – Загл. с экрана.

219. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер [Электронный ресурс]: ГОСТ Р 57580.1-2017: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 8 августа 2017 г. № 822-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/1200146534. – Дата обращения: 18.07.2020. – Загл. с экрана.

220. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия [Электронный ресурс]: ГОСТ Р 57580.2-2018: [утвержден Приказом Федерального агентства по техническому регулированию и метрологии 28 марта 2018 г. № 156-ст: по состоянию на 18 июля 2020 г.] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: http://docs.cntd.ru/document/ 1200158801. – Дата обращения: 18.07.2020. – Загл. с экрана.

221. Джура, Г. С. Организационные подходы к модернизации системы обеспечения информационной безопасности в органах государственной власти Донецкой Народной Республики / Г. С. Джура // Торговля и рынок. – 2020. – Вып. 4. Т.2. Ч. 1. – С. 140-148.

222. Джура, Г. С. Совершенствование методического подхода к комплексной диагностике системы обеспечения информационной безопасности органа государственной власти / Г. С. Джура // Новое в экономической

кибернетике: сборник научных трудов. – Донецк: ГОУ ВПО «ДонНУ», 2020. – № 3-4. – С. 115-124.

223. The 20 CIS Controls & Resources [Электронный ресурс]. – Режим доступа: https://www.cisecurity.org/controls/cis-controls-list/. – Дата обращения: 18.04.2017. – Загл. с экрана.

224. OWASP SAMM [Электронный ресурс]. – Режим доступа: https://owaspsamm.org/assessment/.– Дата обращения: 18.04.2017. – Загл. с экрана.

225. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [Электронный ресурс]: ГОСТ Р ИСО/МЭК 15408-1-2012; введ. 2013-12-01. – Режим доступа: http://docs.cntd.ru/document/1200101777. – Дата обращения: 18.07.2020. – Загл. с экрана.

226. Люльченко, А. Н. Модели технологии и методика оценки состояния системы обеспечения информационной безопасности в органе власти, организации: дис. … канд. техн. наук: 05.13.19: защищена 24.12.2014 / Люльченко Андрей Николаевич. – Санкт-Петербург, 2014. – 214 с.

227. Борискин, Д. Л. Проблемы информационной безопасности современных компьютерных сетей организации / Д. Л. Борискин, Е. В. Юфтайкина // Материалы X Международной студенческой научной конференции «Студенческий научный форум». – Режим доступа: https://scienceforum.ru/2018/article/2018003735 – Дата обращения: 18.07.2020. – Загл. с экрана.

228. Грибанов, Ю. И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции: дис. … д-ра экон. наук: 08.00.05: защищена 12.10.2019 / Грибанов Юрий Иванович. – Санкт-Петербург, 2019. – 355 с.

229. Петровский, М. В. Организационная защита информации на предприятии и ее режим защиты / М. В. Петровский, М. И. Данилов // Сборник материалов XXVIII Международной научно-практической конференции «Достижения вузовской науки». – Новосибирск, 2017. – С. 120-124.

230. Global Cybersecurity Index 2020 [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. – Дата обращения: 18.02.2021. – Загл. с экрана.

231. Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме [Электронный ресурс]: Постановление Правительства Российской Федерации № 451: [утверждено Постановлением Правительством Российской Федерации 8 июня 2011 г.: по состоянию на 18 июля 2020 г.] // Справочно-правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115048/8f415e850dc9cb0246665bc05a6146b3a19e2c68/. – Дата обращения: 18.07.2020. – Загл. с экрана.

232. Борисова, А.С. Совершенствование информационного обеспечения реализации проектов электронного правительства регионов: дис. … канд. экон. наук: 08.00.05 / Борисова Анна Сергеевна. – Волгоград, 2014. – 270 с.

233. Об электронной подписи [Электронный ресурс]: Закон Донецкой Народной Республики № 60-IHC: [принят Постановлением Народного Совета 19 июня 2015 г.: по состоянию на 18 июля 2020 г.] // Народный Совет Донецкой Народной Республики. – Режим доступа: https://dnrsovet.su/zakon-donetskoj-narodnoj-respubliki-ob-elektronnoj-podpisi/. – Дата обращения: 18.07.2020. – Загл. с экрана.

234. Об утверждении Концепции внешней политики Донецкой Народной Республики [Электронный ресурс]: Указ № 56: [принят Главой Донецкой Народной Республики 01 марта 2019 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0001-56-20190301/ – Дата обращения: 18.07.2020. – Загл. с экрана.

235. Доклад об итогах работы Министерства связи в 2017 году [Электронный ресурс]. – Режим доступа: https://минсвязь.рус/news/viktor-yacenko-

predstavil-parlamentariyam-ezhegodnyy-doklad-o-prodelannoy-rabote. – Дата обращения: 18.07.2020. – Загл. с экрана.

236. Об утверждении Положения о Министерстве внутренних дел Донецкой Народной Республики [Электронный ресурс]: Указ № 110: [принят Главой Донецкой Народной Республики 23 апреля 2020 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0001-110-20200423/. – Дата обращения: 18.07.2020. – Загл. с экрана.

237. Об утверждении Порядка ведения Государственной информационной системы нормативных правовых актов Донецкой Народной Республики и предоставления сведений, содержащихся в ней [Электронный ресурс]: Постановление № 31-3: [принят Постановлением Правительства Донецкой Народной Республики 18 октября 2019 г.: по состоянию на 18 июля 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0030-31-3-20191018/. – Дата обращения: 18.07.2020. – Загл. с экрана.

238. В Республике работает Единая информационная система нотариата [Электронный ресурс]. – Режим доступа: http://goskomzemdnr.ru/novosti-respubliki/v-respublike-rabotaet-edinaya-informatsionnaya-sistema-notariata-yurij-sirovatko/. – Дата обращения: 18.12.2020. – Загл. с экрана.

239. О внесении изменений в отдельные документы в сфере закупок товаров, работ и услуг за бюджетные средства, утвержденные Приказом Министерства экономического развития Донецкой Народной Республики от 26 декабря 2016 г. № 140 [Электронный ресурс]: Приказ № 140: [принят Министерством экономического развития Донецкой Народной Республики 26 декабря 2016 г.: по состоянию на 14 января 2021 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0026-20-20210301/. – Дата обращения: 14.01.2021. – Загл. с экрана.

240. Центральный Республиканский банк запустил систему дистанционного обслуживания – СДО «ЦРБ Онлайн» [Электронный ресурс]. – Режим доступа: https://crb-dnr.ru/news/centralnyy-respublikanskiy-bank-zapustil-sistemu-distancionnogo-obsluzhivaniya-crb-onlayn-sdo-crb-onlayn-dlya-osushchestvleniya-platezhey-fizicheskimi-licami. – Дата обращения: 18.12.2020. – Загл. с экрана.

241. Об организации работы АИС «Лицензионный реестр [Электронный ресурс]: Приказ № 174: [принят Министерством финансов Донецкой Народной Республики 01 июля 2020 г.: по состоянию на 18 декабря 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0025-174-20200701/. – Дата обращения: 18.12.2020. – Загл. с экрана.

242. Временный порядок предоставления доступа к ресурсам электронного сервиса «Личный кабинет плательщика» в Министерстве доходов и сборов Донецкой Народной Республики и его территориальных органах [Электронный ресурс]: Приказ № 228: [утвержден Приказом Министерства доходов и сборов Донецкой Народной Республики 06 июня 2017 г.: по состоянию на 18 декабря 2020 г.] // Государственная информационная система нормативных правовых актов Донецкой Народной Республики. – Режим доступа: https://gisnpa-dnr.ru/npa/0013-170-20160614/. – Дата обращения: 18.12.2020. – Загл. с экрана.

243. UN E-Government Survey 2020 [Электронный ресурс]. – Режим доступа: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020. – Дата обращения: 18.12.2020. – Загл. с экрана.

244. Давосский форум назвал главные риски 2020 года [Электронный ресурс]. – Режим доступа: https://www.forbes.ru/newsroom/obshchestvo/391219-davosskiy-forum-nazval-glavnye-riski-2020-goda. – Дата обращения: 18.12.2020. – Загл. с экрана.

245. Positive Research 2021 [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2021-rus.pdf. – Дата обращения: 18.12.2020. – Загл. с экрана.

246. О концепции формирования в Российской Федерации электронного правительства до 2010 г. [Электронный ресурс]: Распоряжение Правительства Российской Федерации № 632-р от 6 мая 2008 г.: по состоянию на 18 декабря 2020 г. // Справочно-правовая система «КонсультантПлюс». – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/93274/. – Дата обращения: 18.12.2020. – Загл. с экрана.

247. Заявление о конфиденциальности корпорации Майкрософт [Электронный ресурс]. – Режим доступа: https://privacy.microsoft.com/ru-ru/PrivacyStatement. – Дата обращения: 18.12.2020. – Загл. с экрана.

248. База знаний ГОСТ 57580 [Электронный ресурс]. – Режим доступа: https://docs.google.com/spreadsheets/d/13cGGthbgkGix48qOAwlA2gAvbQSRGG1DgLO_Isc1jFA/edit?usp=sharing. – Дата обращения: 18.12.2020. – Загл. с экрана.

249. Statistics, Country ICT Data [Электронный ресурс]. – Режим доступа: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. – Дата обращения: 18.12.2020. – Загл. с экрана.

250. Бегишев, И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук: 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2017. – 204 с.

251. Мирошниченко, К. В. Основные направления обеспечения безопасности информационных систем / К. В. Мирошниченко // Вестник Уральского института экономики, управления и права. – 2018. – № 2. – С. 70-73.

252. Благовещенский, А. Н. Основы организации системы обеспечения информационной безопасности для специальности «Прикладная информатика в экономике» / А. Н. Благовещенский, П. А. Благовещенский // Образовательные технологии и общество. – 2014. – № 3. – С. 634-645.

ПРИЛОЖЕНИЯ

Приложение А
Справки о внедрении результатов исследования

**МИНИСТЕРСТВО СВЯЗИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

ДНР 83050, г. Донецк, Ворошиловский район, бул. Пушкина, 34
приемная: тел. (+38062) 300-23-00, канцелярия: 83015, г. Донецк, ул. Артема, 135, тел. (+38062) 300-23-04
mail: info@msdnr.ru http://минсвязь.рус Идентификационный код 51001667

24.02.2021 № 98
На № от

**Диссертационный совет
Д 01.001.01 при ГОУ ВПО
«Донецкая академия управления и
государственной службы при
Главе Донецкой Народной
Республики»**

СПРАВКА

о внедрении результатов исследований диссертационной работы

Джуры Георгия Сергеевича на тему «Совершенствование системы обеспечения информационной безопасности в органах государственной власти», представленной на соискание ученой степени кандидата экономических наук по специальности 08.00.05 «Экономика и управление народным хозяйством» (по отраслям сферы деятельности, в т.ч.: менеджмент)

Предложенный Джурой Г. С. методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти, предоставляющий возможность выбрать и обосновать эталонные значения критериев состояния системы, а также осуществить оценку уровня ее зрелости, используется в Министерстве связи Донецкой Народной Республики при принятии решений по оптимизации существующей системы обеспечения информационной безопасности.

Практическое использование предложенных научно-методических разработок Джуры Г. С. подтверждает их актуальность и целесообразность к использованию для обеспечения информационной безопасности на всех уровнях государственного управления.

Министр **И. Н. Халепа**

МИНИСТЕРСТВО СВЯЗИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ СВЯЗИ «УГЛЕТЕЛЕКОМ»

р/с в рос.руб. 40602810120260000003 в ЦРБ ДНР,
р/с в рос.руб. 40602810720260000005 в ЦРБ ДНР
БИК 310101001,
ИКЮЛ 51000506

ДНР 83001, г.Донецк, Ворошиловский район,
ул. Постышева, д.60,
приемная: тел. (062) 300-30-48
тел/факс: (062) 302-82-92
E-mail: ugletelecom@ugletele.com

15.02 2021 №370/02
на _____ от _____

В диссертационный совет
Д 01.001.01 при ГОУ ВПО
«Донецкая академия управления и
государственной службы при Главе
Донецкой Народной Республики

СПРАВКА
о внедрении результатов исследований диссертационной работы Джуры Георгия Сергеевича на тему «Совершенствование системы обеспечения информационной безопасности в органах государственной власти», представленной на соискание ученой степени кандидата экономических наук по специальности 08.00.05 «Экономика и управление народным хозяйством» (по отраслям сферы деятельности, в т.ч.: менеджмент)

Учитывая сложные политические и экономические условия Донецкой Народной Республики, актуальность приобретают вопросы обеспечения информационной безопасности как для государства в целом, так и для органов государственной власти.

Предложенный Джурой Г. С. методический подход к оценке рисков информационной безопасности в органах государственной власти внедрен в практическую деятельность ГУП ДНР «Углетелеком» и используется в процессе диагностики системы обеспечения информационной безопасности в органах государственной власти, что подтверждает его актуальность и практическую значимость.

С уважением,
Директор **С.В. Шеховцов**

ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
"ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ"
283001, г. Донецк, ул. Артема, 58 тел.: (062) 337-17-33, 335-75-62, факс: (062) 304-12-78
эл. почта: donntu.info@mail.ru

15.02.21 № 39.2/1188-1

В диссертационный совет
Д 01.001.01
при ГОУ ВПО «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики»

СПРАВКА
о внедрении результатов исследований диссертационной работы Джуры Георгия Сергеевича на тему «Совершенствование системы обеспечения информационной безопасности в органах государственной власти», представленной на соискание ученой степени кандидата экономических наук по специальности 08.00.05 «Экономика и управление народным хозяйством» (по отраслям сферы деятельности, в т.ч.: менеджмент)

Разработанные в ходе исследования Джуры Г. С. основные научные положения и методические рекомендации используются в учебном процессе с целью совершенствования содержательного изложения учебного материала. Результаты диссертационной работы использованы при разработке рабочих программ, методических рекомендаций и конспектов лекций по учебным дисциплинам «Информационно-аналитическое обеспечение государственного и муниципального управления», «Электронная коммерция», «Управление изменениями».

Первый проректор
ГОУ ВПО «Донецкий национальный технический университет» А. А. Каракозов

Приложение Б. Структура основных регуляторных органов Соединенных Штатов Америки в сфере обеспечения информационной безопасности

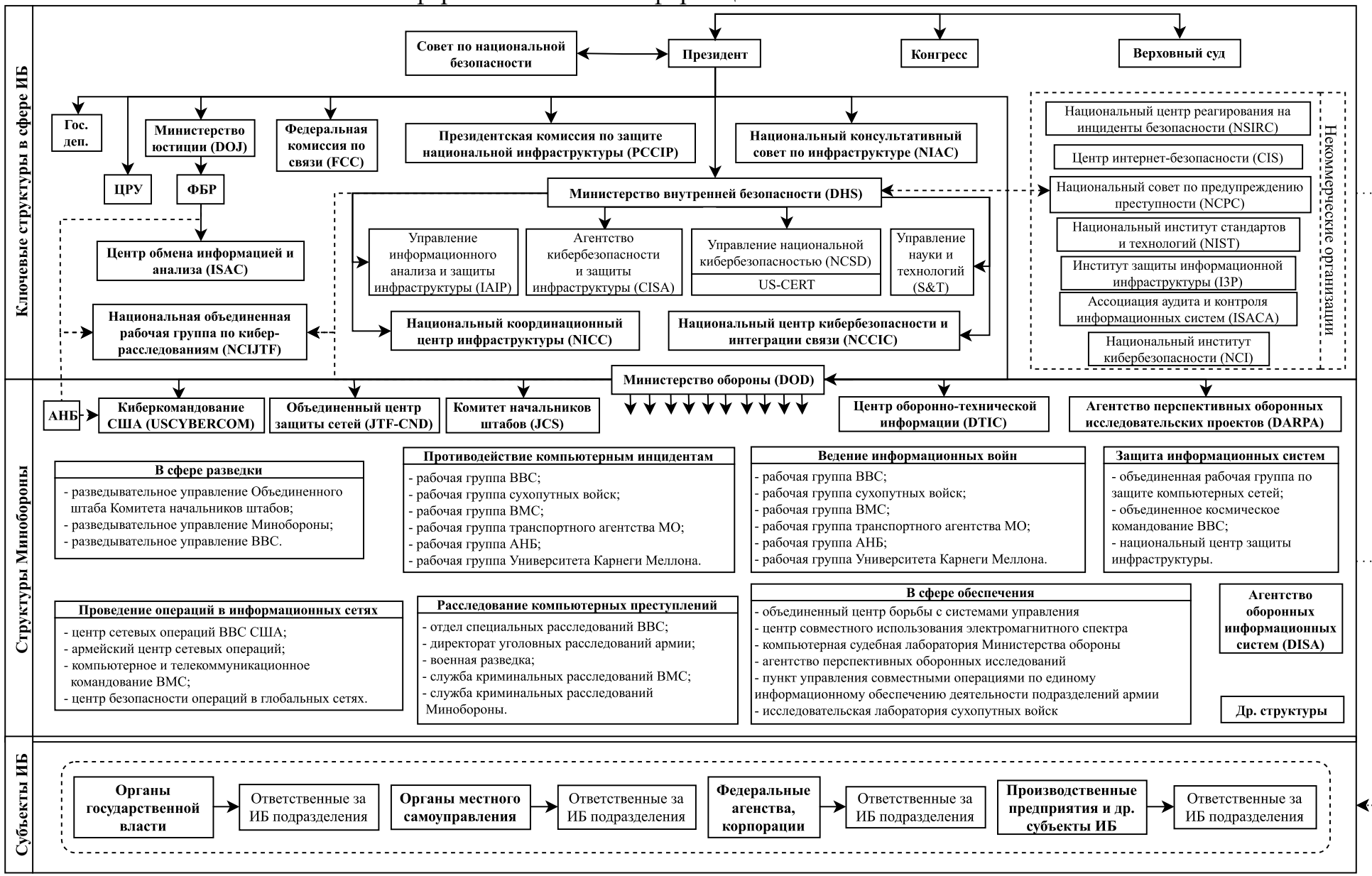

Рисунок Б.1 – Организационная структура СОИБ США

Приложение В. Основные стратегические документы Европейского Союза в сфере обеспечения информационной безопасности

Таблица В.1 – Основные стратегические документы ЕС в сфере обеспечения ИБ

Документ	Цели	Основные положения	Ожидаемые результаты
1	2	3	4
Стратегия кибербезопасности ЕС: Открытое, Безопасное и Надежное Киберпространство	Определение подхода ЕС к оптимальному предотвращению кибератак и реагированию на них, подробно описывая ряд мер по повышению киберустойчивости ИТ-систем, снижению киберпреступности и укреплению международной политики ЕС в области кибербезопасности.	1. Определены принципы обеспечения кибербезопасности. 2. Сформулированы стратегические приоритеты и необходимые действия ЕС в сфере кибербезопасности. 3. Определены роли и обязанности институциональных органов.	1. Повышение киберустойчивости. 2. Сокращение киберпреступности, разработка политики и потенциала киберзащиты, связанных с общей политикой ЕС в области безопасности и обороны (CSDP). 3. Развитие промышленных и технологических ресурсов для обеспечения кибербезопасности. 4. Создание согласованной международной политики ЕС в области киберпространства.
Директива 2016/1148 от 6 июля 2016 г. Европейского Парламента и Совета ЕС (о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза (NIS Directive).	1. Возложение на государства–члены ЕС обязательств по принятию национальной стратегии кибербезопасности, а также назначению национальных компетентных органов и формированию единого контактного пункта по обеспечению кибербезопасности. 2. Установление обязанности по формированию требований государствами-членами ЕС. 3. Содействие стратегическому взаимодействию между государствами-членами ЕС.	1. Сформулирована национальная рамочная программа обеспечения безопасности сетевых и информационных систем. 2. Сформулированы положения о сотрудничестве в сфере кибербезопасности. 3. Сформулированы положения по формированию государствами–членами ЕС требований к ИБ.	1. Стандартизация требований в области кибербезопасности. 2. Достижение единого высокого уровня ИБ в Союзе. 3. Содействие формированию культуры управления рисками и обеспечения соблюдения отчетности о инцидентах. 4. Формирование минимально достаточной ресурсной базы частных и государственных структур. 5. Организация взаимодействия профильных национальных госструктур стран ЕС. 6. Установка сети групп реагирования на инциденты ИБ («CSIRTs»).
Закон о кибербезопасности (Regulation (EU) 2019/881 of the European parliament and of the council of 17 April 2019)	1. Формулирование мандата, ключевых целей, задачи и организационную структуру ENISA. 2. Определение системы сертификации кибербезопасности. 3. Обеспечение условий для сближения законодательств стран–членов ЕС в сфере кибербезопасности.	1. Сформулированы мандат, ключевые цели, задачи, организационная структура и другие аспекты функционирования ENISA. 2. Определена система сертификации в сфере кибербезопасности.	1. Достижение высокого общего уровня кибербезопасности на уровне Союза. 2. Способствование снижению фрагментации внутреннего рынка. 3. Содействие государствам–членам и организациям ЕС в повышении осведомленности, сотрудничестве и обеспечении кибербезопасности; 4. Повышение уровня ИБ за счет сертификации.

Продолжение таблицы В.1

1	2	3	4
Регламент (ЕС) 2016/679 Европейского парламента и Совета О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС. (GDPR)	1. Защита конституционных прав граждан стран–членов ЕС. 2. Установка правил в отношении защиты физических лиц при обработке ПД и правил в отношении свободного обращения ПД. 3. Предоставление физическим лицам инструментов контроля над их ПД.	1. Определять, перечень собираемых ПД, а также порядок их хранения, обработки и использования. 2. Определены: – принципы обработки ПД; – права субъектов данных; – обязанности ответственных за ПД; – статус, компетенция, задачи и полномочия независимых надзорных органов. – механизмы сотрудничества и согласованности – правовые средства защиты ПД, ответственность и санкции.	1. Внедрение современных стандартов защиты ПД. 2. Развитие цифрового пространства ЕС. 3. Обеспечение строгого соблюдения правил защиты ПД граждан стран–участников всеми субъектами их обработки, ЕС. 4. Правовое обеспечение международной передачи ПД.
Регламент европейского парламента и совета об уважении частной жизни и защите персональных данных в электронных сообщениях и отмене директивы 2002/58 / ЕС (Положение о конфиденциальности и электронных сообщениях) (ePrivacy Regulation).	1. Установление правил по защите прав и свобод физических и юридических лиц при предоставлении и использовании электронных услуг. 2. Обеспечение свободного и безопасного обращения ПД и электронных услуг в пределах Союза. 3. Регулирование других технических аспектов циркуляции ПД в электронном виде.	1. Сформулированы положения по защите электронных сообщений физических и юридических лиц и информации, хранящейся в их терминальном оборудовании. 2. Определены права физических и юридических лиц на контроль электронных сообщений. 3. Определены независимые надзорные органы и правоприменение. 4. Определены средства правовой защиты, ответственность и штрафы.	1. Защитить пользователей ИТ–сервисов от спама и навязчивой рекламы и укрепить их контроль над ПД. 2. Дать толчок владельцам сайтов для запроса у посетителей согласия на использование cookie–файлов. 3. Вернуть гражданам контроль над ПД. 4. Показать, что конфиденциальность данных в цифровую эпоху необходима и возможна.
Предложение о Директиве о мерах обеспечения повышенного уровня безопасности сетевых и информационных систем в ЕС от 6 июля 2016 г. (2013/0027 (COD) LEX 1683)	Создание комплексного рамочного подхода к развитию и гармонизации европейского регулирования в сфере обеспечения сетевой и информационной безопасности (NIS) и защиты критической информационной инфраструктуры.	1. Сформулированы национальные основы сетевой и информационной безопасности. 2. Сформулированы аспекты сотрудничество между компетентными органами 3. Определены аспекты безопасности сетей и информационных систем ОГВ и операторов.	1. Формирование минимально достаточной ресурсной базы частными и государственными структурам для обеспечения ИБ стран ЕС. 2. Организация взаимодействия профильных национальных госструктур стран ЕС. 3. Внедрение и развитие культуры управления рисками между частными и государственными организациями.

Приложение Г. Основные законодательные акты Российской Федерации в сфере обеспечения информационной безопасности

Таблица Г.1 – Основные законодательные акты РФ в сфере обеспечения ИБ

Документ	Цели	Основные положения	Ожидаемые результаты
1	2	3	4
Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ	Обеспечение единообразия, системного и обоснованного регулирования в информационной сфере, в частности отношений, возникающих при: – получении, передаче, производстве и распространение информации; – применении информационных технологий; – обеспечении защиты информации.	Определены: – принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации; – аспекты определения информации как объекта правовых отношений; – типы, права и обязанности обладателя информации; – аспекты обеспечения права на доступ к информации; – аспекты ограничения доступа к информации; – аспекты распространение информации или предоставление информации; – обязанности организатора распространения информации в сети интернет; – обязанности оператора поисковой системы; – особенности распространения информации новостным агрегатором; – особенности документирования информации; – особенности государственного регулирования в сфере применения информационных технологий; – виды и аспекты функционирования информационных систем; – аспекты функционирования государственных информационных систем; – аспекты использования информационно-телекоммуникационных сетей; – аспекты обеспечения защиты информации; – ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.	Реализация государственных задач, связанных с построением информационного общества и обеспечением вхождения РФ в мировое информационное пространство.
Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»	Определение: – основных принципов и содержания деятельности по обеспечению государственной, общественной, экологической, безопасности личности и иных видов безопасности, предусмотренных законодательством РФ, – полномочий и функций ОГВ. – статуса Совета Безопасности РФ.	Определены: – основные принципы, содержание деятельности, государственная политика, правовая основа, координация деятельности, международное сотрудничество в области обеспечения безопасности; – полномочия и функции ФОИВ, ОГВ субъектов РФ и органов местного самоуправления в области обеспечения безопасности; – статус Совета Безопасности РФ.	1.Прозрачное и эффективное регулирования в сфере обеспечения безопасности РФ. 2.Определение полномочий и функций ответственных за обеспечение безопасности ОГВ.
Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ	Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.	Определены: – принципы и условия обработки персональных данных; – права субъекта персональных данных; – обязанности оператора при сборе ПД и меры по обеспечению их безопасности; – аспекты государственного контроля и надзора за обработкой ПД.	1. Устранения барьеров в международной торговле со странами Евросоюза. 2. Защита конституционных прав граждан.

Продолжение таблицы Г.1

1	2	3	4
Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1	1. Регулирование вопросов, связанных с защитой государственной тайны в рамках регулирования сферы для ОГВ и допущенных к сведениям лиц. 2. Установка перечня сведений, составляющих государственную тайну и степеней их секретности. 3. Установка требований по защите государственной тайны.	Определены: – перечень сведений, составляющих государственную тайну – аспекты отнесения сведений к государственной тайне и их засекречивания; – аспекты рассекречивания сведений и их носителей; – аспекты распоряжение сведениями, составляющими государственную тайну; – аспекты защиты государственной тайны; – аспекты финансирование мероприятий по защите государственной тайны; – аспекты контроля и надзора за обеспечением защиты государственной тайны.	Обеспечение высокого уровня защиты сведений, составляющих государственную тайну.
Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ	1. Регулирование отношений, возникающих при производстве различных товаров, связанных с разработкой стандартов, оценкой соответствия, аккредитацией, государственного наблюдения принудительных стандартов, технических инструкций и информационных систем. 2. Формирование стандартизации, сертификации и систем менеджмента качества. 3. Стимулирование создания саморегулируемых организаций, национальной системы аккредитации органов, работающих в сфере оценки соответствия и др.	Определены: – принципы технического регулирования; – особенности технического регулирования в отношении различного рода продукции и процессов и деятельности; – цели принятия Содержание и применение порядки разработки, принятия, изменения и отмены технических регламентов; – документы по стандартизации, в результате применения которых обеспечивается соблюдение требований технических регламентов; – особенности подтверждение соответствия; – особенности аккредитации органов по сертификации и испытательных лабораторий (центров); – особенности государственного контроля (надзора) за соблюдением требований технических регламентов; – ответственность, обязанности, права и др. аспекты, связанные с нарушениями требований технических регламентов и отзыва продукции; – особенности функционирования федерального информационного фонда технических регламентов и стандартов; – аспекты финансирования в области технического регулирования.	1. Обеспечение соответствия уровня технического регулирования интересам и уровню национальной экономики, международным нормам, и правилам. 2. Повышение уровня безопасности жизни, здоровья и имущества граждан, охраны окружающей среды, предупреждение действий, вводящих в заблуждение приобретателей, создание конкурентоспособной продукции, стимулирование инновационных процессов.
Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ	Регулирование отношений ОГВ и бизнеса в сфере лицензирования отдельных видов деятельности.	Определены: – цели, задачи лицензирования отдельных видов деятельности и критерии определения лицензируемых видов деятельности; – основные принципы осуществления лицензирования; – полномочия, права и обязанности лицензирующих органов; – методов и порядков лицензирования отдельных видов деятельности; – установления перечней лицензируемых видов деятельности; – вопросы, связанные с лицензионными требованиями; – аспекты финансового обеспечения деятельности лицензирующих органов; – аспекты организации и осуществления лицензирования.	1. Установление единого порядка лицензирования отдельных видов деятельности на территории РФ. 2. Обеспечение единства экономического пространства на территории РФ.

Продолжение таблицы Г.1

1	2	3	4
Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ	Регулирование отношений в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.	Определены: – аспекты правового регулирования отношений в области использования электронных подписей; – принципы использования электронной подписи; – виды электронных подписей; – условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подпись; – аспекты признания электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами; – полномочия федеральных органов исполнительной власти в сфере использования электронной подписи; – аспекты использования простой электронной подписи; – обязанности участников электронного взаимодействия при использовании усиленных электронных подписей; – аспекты признания квалифицированной электронной подписи; – средства электронной подписи; – функции и обязанности удостоверяющих центров; – содержание и аспекты функционирования сертификата ключа проверки электронной подписи; – функции и обязанности аккредитованных удостоверяющих центров, и аспекты их функционирования; – аспекты аккредитации удостоверяющих центров; – содержание и аспекты выдачи квалифицированных сертификатов.	1. Формирование нормативной и методологической базы для внедрения электронной подписи в системы документооборота ОГВ. 2. Предоставление административных услуг в электронной форме. 3. Создание юридической базы для проведения государственных и муниципальных закупок посредством электронных торгов. 4. Регулирование электронного банкинга. 5. Совершенствование процедур подачи электронной отчетности.
Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ	1. Регулирование отношения, связанные с созданием и эксплуатацией сетей и сооружений связи, использованием радиочастотного спектра, оказанием услуг электросвязи и почтовой связи. 2. Защита интересов пользователей услугами связи и субъектов. 3. Содействие внедрению перспективных технологий. 4. Обеспечение эффективной и добросовестной конкуренции на рынке услуг связи.	Определены: – основы деятельности в области связи; – аспекты функционирования и виды сетей связи; – аспекты присоединения сетей электросвязи и их взаимодействие; – аспекты государственного регулирования деятельности в области связи; – аспекты лицензирования деятельности в области оказания услуг связи и оценка соответствия в области связи; – особенности оказания услуг связи, обязанности операторов связи, и др. аспекты регулирования услуг связи; – аспекты обеспечения устойчивого, безопасного и целостного функционирования на территории РФ сети интернет; – аспекты регулирования универсальных услуг связи; – аспекты защиты прав пользователей услугами связи; – аспекты управления сетями связи в отдельных случаях; – ответственность за нарушение законодательства РФ в области связи.	1.Создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи. 2.Создание условий для обеспечения потребностей в связи для нужд ОГВ, обороны, безопасности государства и обеспечения правопорядка.

Продолжение таблицы Г.1

1	2	3	4
Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ	Регулирование отношений, связанных с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет коммерческую ценность.	Определены: – право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации; – сведения, которые не могут составлять коммерческую тайну; – аспекты предоставления информации, составляющей коммерческую тайну в т.ч. прав обладателя информации; – аспектов охраны конфиденциальности информации; – ответственность за нарушение.	Введение и поддержание особых мер по защите конфиденциальности информации, позволяющий её обладателю получить коммерческую выгоду.
Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 № 187-ФЗ	1. Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. 2. Определение полномочий Президента и ОГВ РФ в области обеспечения безопасности критической информационной инфраструктуры.	Определены: – аспекты правового регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры; – принципы обеспечения безопасности критической информационной инфраструктуры; – аспекты функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ; – полномочия Президента и ОГВ РФ в области обеспечения безопасности критической информационной инфраструктуры; – аспекты категорирования объектов критической информационной инфраструктуры; – содержание реестра и аспекты формирования значимых объектов критической информационной инфраструктуры; – права и обязанности субъектов критической информационной инфраструктуры; – основные задачи системы безопасности значимого объекта критической информационной инфраструктуры; – аспекты формирования требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры; – аспекты осуществления оценки безопасности критической информационной инфраструктуры; – аспекты осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.	1. Устойчивое функционирование объектов критической информационной инфраструктуры в случае проведении в отношении них компьютерных атак. 2. Создание государственной системы обнаружения, предупреждения и ликвидации последствий атак на информационные ресурсы страны.

Приложение Д. Структура основных регуляторных органов Российской Федерации
в сфере обеспечения информационной безопасности

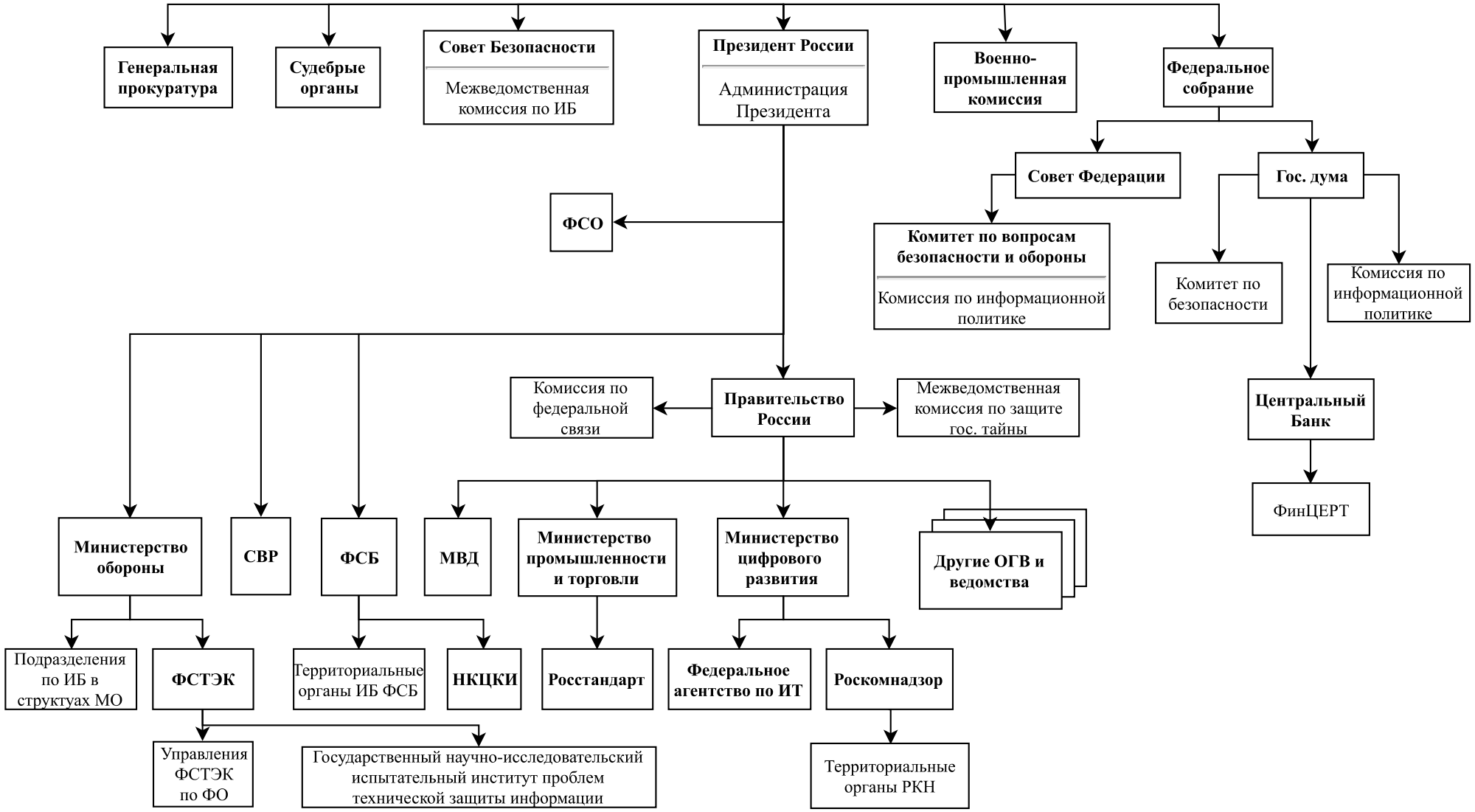

Рисунок Д.1 – Организационная структура системы обеспечения информационной безопасности РФ

Приложение Е. Основные законодательные акты Донецкой Народной Республики в сфере обеспечения информационной безопасности

Таблица Е.1 – Основные законодательные акты ДНР в сфере обеспечения ИБ

Документ	Цели	Основные положения	Ожидаемые результаты
1	2	3	4
Закон ДНР № 71-IНС от 07.08.2015 «Об информации и информационных технологиях»	Обеспечение единообразия, системного и обоснованного регулирования в информационной сфере, в частности отношений, возникающих при: – осуществлении права на поиск, получение, передачу, производство и распространение информации; – применении информационных технологий; – обеспечении защиты информации.	Определены: – принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации; – аспекты определения информации как объекта правовых отношений; – типы, права и обязанности обладателя информации; – аспекты обеспечения права на доступ и ограничения доступа к информации; – аспекты распространение информации или предоставление информации; – обязанности организатора распространения информации в сети интернет; – особенности распространения блогером общедоступной информации – особенности документирования информации; – особенности государственного регулирования в сфере применения информационных технологий; – виды и аспекты функционирования информационных систем; – аспекты функционирования государственных информационных систем; – аспекты использования информационно-телекоммуникационных сетей; – регулирование единого реестра доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, позволяющих идентифицировать сайты в сети интернет, содержащие информацию, распространение которой в ДНР запрещено; – аспекты обеспечения защиты информации; ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. Определены порядки ограничения доступа к: – информации, распространяемой с нарушением авторских и (или) смежных прав – информации, распространяемой с нарушением закона – информационному ресурсу организатора распространения информации в сети интернет – информации, обрабатываемой с нарушением законодательства ДНР в области ПД.	Реализация государственных задач, связанных с построением информационного общества и обеспечением вхождения ДНР в мировое информационное пространство.

Продолжение таблицы Е.1

1	2	3	4
Закон ДНР № 03-IHC от 12.12.2014 «О Государственной тайне»	1. Регулирование вопросов, связанных с защитой государственной тайны в рамках регулирования сферы для ОГВ и допущенных к сведениям лиц. 2. Установка перечня сведений, составляющих государственную тайну и степеней их секретности. 3. Установка требований по защите государственной тайны.	Определены: – полномочия ОГВ и должностных лиц в области отнесения сведений к государственной тайне и их защиты – перечень сведений, составляющих государственную тайну – аспекты отнесения сведений к государственной тайне и их засекречивания; – аспекты рассекречивания сведений и их носителей; – аспекты распоряжение сведениями, составляющими государственную тайну; – органы защиты государственной тайны; – аспекты защиты государственной тайны; – аспекты финансирование мероприятий по защите государственной тайны; – аспекты контроля и надзора за обеспечением защиты государственной тайны.	Обеспечение высокого уровня защиты сведений, составляющих государственную тайну.
Закон ДНР № 04-IHC от 12.12.2014 «О безопасности»	Определение: – основных принципов и содержания деятельности по обеспечению государственной, общественной, экологической, безопасности личности и иных видов безопасности, предусмотренных законодательством ДНР; – полномочий и функций ОГВ; – статуса Совета Безопасности ДНР.	1. Определены: – основные принципы, содержание деятельности, государственная политика, правовая основа, координация деятельности, международное сотрудничество в области обеспечения безопасности. – полномочия и функции ОГВ, и органов местного самоуправления в области обеспечения безопасности. 2. Определен статус Совета Безопасности ДНР.	1.Прозрачное и эффективное регулирования в сфере обеспечения безопасности РФ. 2.Определение полномочий и функций ответственных за обеспечение безопасности ОГВ.
Закон ДНР № 61-IHC от 19.06.2015 «О персональных данных»	Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.	Определены: – принципы и условия обработки персональных данных; – права субъекта персональных данных; – обязанности оператора персональных данных; – аспекты государственного контроля и надзора за обработкой персональных данных в т.ч. ответственность за нарушение требований Закона.	Защита конституционных прав граждан.

Продолжение таблицы Е.1

1	2	3	4
Закон ДНР № 18-IНС от 27.02.2015 «О лицензировании отдельных видов хозяйственной деятельности»	Регулирование отношений ОГВ и бизнеса в сфере лицензирования отдельных видов деятельности.	Определены: – основные принципы государственной политики в сфере лицензирования; – полномочия ОГВ в сфере лицензирования; – аспекты организации и осуществления лицензирования; – аспекты формирования и ведение реестра лицензий, предоставление информации по вопросам лицензирования; – ответственность за нарушение норм Закона.	1. Установление единого порядка лицензирования отдельных видов деятельности на территории ДНР. 2. Обеспечение единства экономического пространства на территории ДНР.
Закон ДНР № 60-IНС от 19.06.2015 «Об электронной подписи»	Регулирование отношений в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.	Определены: – аспекты правового регулирования отношений в области использования электронных подписей; – принципы использования электронной подписи; – виды электронных подписей; – условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подпись; – аспекты признания электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами; – полномочия органов исполнительной власти в сфере использования электронной подписи; – аспекты использования простой электронной подписи; – обязанности участников электронного взаимодействия при использовании усиленных электронных подписей; – аспекты признания квалифицированной электронной подписи; – средства электронной подписи; – функции и обязанности удостоверяющих центров; – содержание и аспекты функционирования сертификата ключа проверки электронной подписи; – функции и обязанности аккредитованных удостоверяющих центров; – аспекты аккредитации удостоверяющих центров; – содержание, аспекты выдачи квалифицированных сертификатов.	1. Формирование нормативной и методологической базы для внедрения электронной подписи в ОГВ. 2. Предоставление административных услуг в электронной форме. 3. Создание юридической базы для проведения государственных и муниципальных закупок посредством электронных торгов. 4. Совершенствование процедур подачи электронной отчетности.

Приложение Ж. Структура основных регуляторных органов Донецкой Народной Республики в сфере обеспечения информационной безопасности

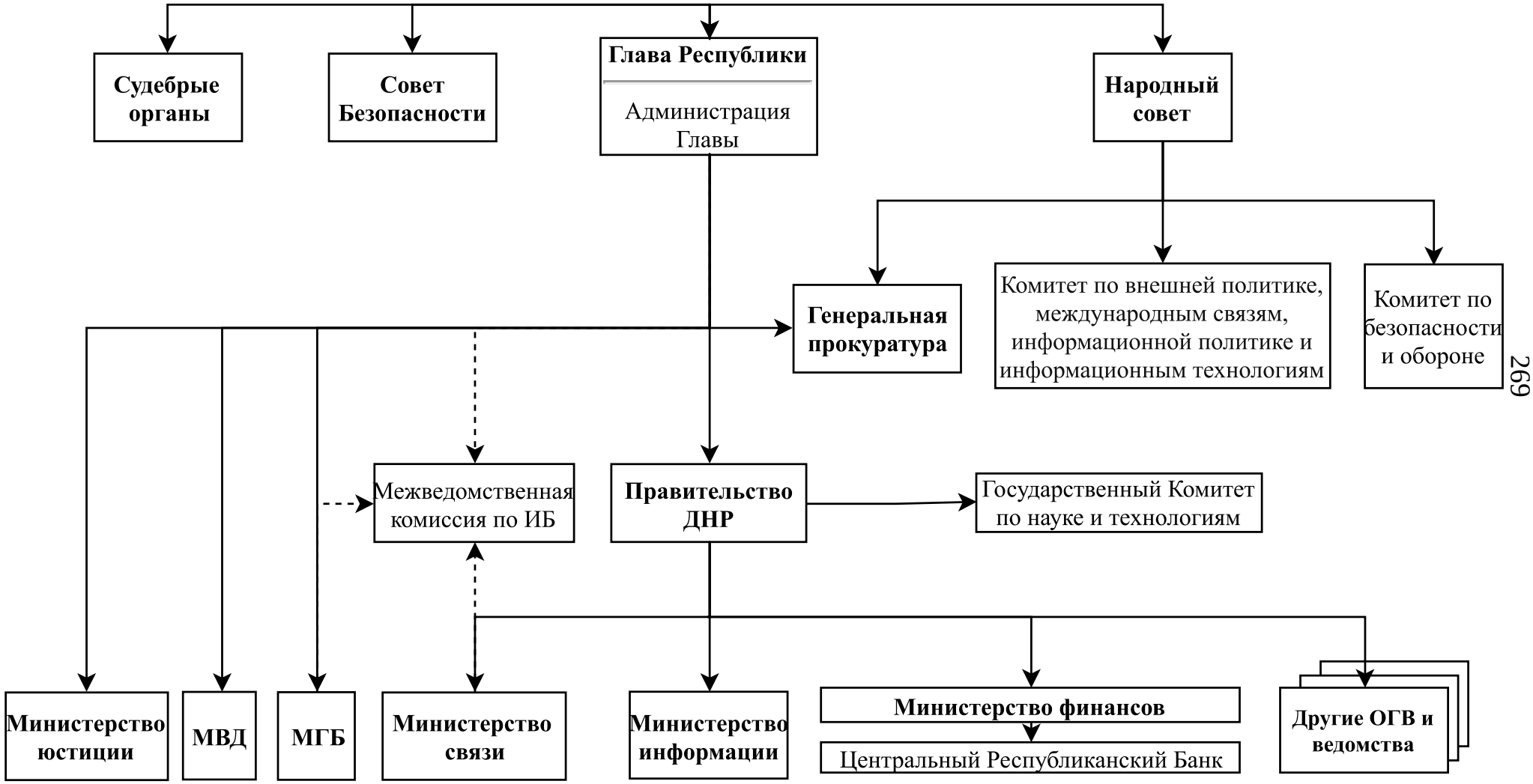

Рисунок Ж.1 – Организационная структура системы обеспечения информационной безопасности ДНР

Приложение И. Сводная таблица результирующих экспертных оценок значений индекса GCI

Таблица И.1 – Экспертные оценки СОИБ ДНР согласно методике расчета индекса GCI

Кластеры	Весовой к-т	Вес	Экспертная оценка				Значение показателя				Значение субпоказателя				Значение микропоказателя			
			2014	2016	2018	2020	2014	2016	2018	2020	2014	2016	2018	2020	2014	2016	2018	2020
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ПРАВОВЫЕ МЕРЫ																		
1. Нормы материального права в области киберпреступности	6	12	-	-	-	-	0,0	1,2	1,2	1,2	-	-	-	-	-	-	-	-
1.1 Имеются ли у вас нормы материального права о противозаконном поведении в сети?	4	4,8	-	-	-	-	-	-	-	-	0,00	0,360	0,360	0,360	-	-	-	-
1.1.1 Имеются ли у вас нормы материального права о противозаконном доступе к устройствам, компьютерным системам и данным?	1,5	0,72	0	1	1	1	-	-	-	-	-	-	-	-	0,00	0,36	0,36	0,36
1.1.2 Имеются ли у вас нормы материального права о противозаконном вмешательстве (посредством ввода, изменения или уничтожения данных) в устройства, данные и компьютерные системы?	2,5	1,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.3 Имеются ли у вас нормы материального права о противозаконном перехвате данных в устройствах и компьютерных системах?	2,5	1,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.4 Имеются ли у вас нормы материального права о краже идентичности и хищении данных в онлайн-среде?	3,5	1,68	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.2 Имеются ли у вас положения о подлоге с использованием компьютерных технологий (пиратство/нарушение авторского права)?	4	4,8	0	0	0	0	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-
1.3 Имеются ли у вас нормы материального права о безопасности в онлайн-среде?	2	2,4	-	-	-	-	-	-	-	-	0	0,84	0,84	0,84	-	-	-	-
1.3.1 Имеются ли у вас положения/правовые меры в отношении преступлений, связанных с материалами расистского и ксенофобского характера в онлайн-среде?	3	0,72	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,36	0,36	0,36
1.3.2 Имеются ли у вас положения/правовые меры, направленные против преследования и нарушения уважения к достоинству/неприкосновенности личности в онлайн-среде?	4	0,96	0	1	1	1	-	-	-	-	-	-	-	-	0,00	0,48	0,48	0,48
1.3.3 Имеются ли у вас положения/правовые меры, направленные на защиту ребенка в онлайн-среде?	3	0,72	0	1	1	1	-	-	-	-	-	-	-	-	0,00	0,36	0,36	0,36
2. Имеются ли какие-либо положения законодательства в области кибербезопасности, относящиеся к следующим вопросам?	4	8	-	-	-	-	0,0	1,8	1,8	1,8	-	-	-	-	-	-	-	-
2.1 Защита персональных данных/ конфиденциальности частной информации	2	1,6	0	1	1	1	-	-	-	-	0,00	0,8	0,8	0,8	-	-	-	-
2.2 Уведомления о случаях утечки данных	0,8	0,64	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.3 Требования проверки кибербезопасности	1,5	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-

Продолжение таблицы И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2.4 Применение стандартов	1	0,8	0	1	1	1	-	-	-	-	0,00	0,4	0,4	0,4	-	-	-	-
2.5 Использование электронных подписей в государственных службах и приложениях	1,5	1,2	0	1	1	1	-	-	-	-	0,00	0,6	0,6	0,6	-	-	-	-
2.6 Сдерживание спама	0,2	0,16	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.7 Выявление и защита критически важных государственных информационных инфраструктур	3	2,4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
ТЕХНИЧЕСКИЕ МЕРЫ																		
1. Национальные/правительственные CIRT/CSIRT/CER	3	6	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
1.1 Имеется ли национальная/государственная CIRT/CSIRT/CERT?	2	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.2 Занимается ли ваша национальная или правительственная CIRT/CSIRT/CERT следующими видами деятельности?	2	1,2	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.2.1 Разработка и реализация мероприятий по повышению осведомленности в вопросах кибербезопасности	2,5	0,3	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.2.2 Проведение регулярных учений по кибербезопасности	2,5	0,3	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.2.3 Распространение общедоступных информационн бюллетеней	2,5	0,3	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.2.4 Содействие обеспечению защиты ребенка в онлайн-среде	2,5	0,3	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.3 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) Форумом групп реагирования на инциденты и обеспечения безопасности (FIRST)?	2	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.4 Связаны ли вышеупомянутые группы CIRT (CSIRT или CERT) с региональной группой CERT?	2	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.5 Был ли уровень развития вышеупомянутых групп CIRT, CSIRT или CERT сертифицирован по схеме сертификации TI в соответствии с TF-CSIRT – SIM3?	2	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2. Отраслевые группы CIRT/CSIRT/CERT	2,5	5	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
2.1 Существуют ли отраслевые группы CIRT/CSIRT/ CERT в вашей стране?	5	2,5	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.2. Занимаются ли ваши отраслевые организации CIRT/CSIRT/CERT следующими видами деятельности?	5	2,5	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.2.1 Подготовка и проведение мероприятий по повышению осведомленности по кибербезопасности в отрасли	3	0,75	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2.2.2 Активное участие в национальных учениях	4	1	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2.2.3 Распространение информации о случившихся в отрасли инцидентах среди отраслевых предприятий	3	0,75	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
3 Национальная система для применения стандартов кибербезопасности	2,5	5	-	-	-	-	0,0	2,5	2,5	2,5	-	-	-	-	-	-	-	-

Продолжение таблицы И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3.1 Имеется ли система для применения/принятия стандартов кибербезопасности?	5	2,5	0	1	1	1	-	-	-	-	0,00	1,25	1,25	1,25	-	-	-	-
3.2 Распространяется ли эта система на международные или другие стандарты?	5	2,5	0	1	1	1	-	-	-	-	0,00	1,25	1,25	1,25	-	-	-	-
4. Защита ребенка в онлайн-среде	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
4.1 Имеются ли какие-либо механизмы и средства подачи сообщений, которые помогают защитить детей в онлайн-среде?	10	4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
ОРГАНИЗАЦИОННЫЕ МЕРЫ																		
1. Национальная стратегия кибербезопасности	4	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1.1 Имеется ли в вашей стране национальная стратегия/политика в области кибербезопасности?	3,5	2,8	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.1.1 Предусматривает ли она защиту критически важных национальных информационных инфраструктур?	1	0,28	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.2 Включает ли она упоминание об устойчивости национальной системы кибербезопасности?	3,5	0,98	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.3 Производится ли пересмотр и обновление национальной стратегии кибербезопасности на постоянной основе?	3	0,84	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.4 Открыта ли стратегия кибербезопасности для консультаций с национальными экспертами в области кибербезопасности в той или иной форме?	2,5	0,7	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.2 Имеется ли установленный план действий/дорожная карта по осуществлению управления в области кибербезопасности?	4	3,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.3 Имеется ли национальная стратегия защиты ребенка в онлайн-среде?	2,5	2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2. Ответственный орган	4	8	-	-	-	-	0,0	1,2	1,2	1,2	-	-	-	-	-	-	-	-
2.1 Имеется ли орган, ответственный за координацию в области кибербезопасности на национальном уровне?	3	2,4	0	1	1	1	-	-	-	-	0,00	1,2	1,2	1,2	-	-	-	-
2.2 Осуществляет ли этот орган контроль в области защиты государственной критической информационной инфраструктуры?	3	2,4	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2.3 Имеется ли национальный орган, контролирующий развитие национального потенциала в области кибербезопасности?	2	1,6	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.4 Имеется ли орган, осуществляющий надзор за реализацией инициатив по защите ребенка в онлайн-среде на национальном уровне?	2	1,6	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3. Показатели кибербезопасности	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-

Продолжение таблицы И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3.1 Проводятся ли какие-либо проверки кибербезопасности на национальном уровне?	5	2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3.2 Существуют ли показатели для оценки рисков, связанных с киберпространством, на национальном уровне?	3	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3.3 Имеются ли показатели для оценки уровня развития кибербезопасности на национальном уровне?	2	0,8	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
РАЗВИТИЕ ПОТЕНЦИАЛА																		
1. Кампании по повышению осведомленности населения в области кибербезопасности	1	2	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
1.1 Проводятся ли кампании по повышению осведомленности населения, ориентированные на определенный сектор, такой как МСП, компании частного сектора и госучреждения?	2	0,4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.2 Проводятся ли кампании по повышению осведомленности населения, ориентированные на гражданское общество?	2	0,4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.3 Проводятся ли кампании по повышению осведомленности населения, ориентированные на граждан?	1	0,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.4 Проводятся ли кампании по повышению осведомленности населения, ориентированные на пожилых людей?	1	0,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.5 Проводятся ли кампании по повышению осведомленности населения, ориентированные на лиц с особыми потребностями?	2	0,4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.6 Проводятся ли кампании по повышению осведомленности населения с участием родителей, педагогов и детей связанные с защитой ребенка в онлайн-среде	2	0,4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2. Подготовка специалистов по кибербезопасности	1	2	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
2.1 Осуществляет ли ваше правительство разработку или проведение курсов профессиональной подготовки по кибербезопасности?	3	0,6	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.2 Имеется ли в вашей стране программа аккредитации специалистов по кибербезопасности?	3	0,6	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для специалистов по кибербезопасности?	4	0,8	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
2.3.1 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников правоохранительных органов?	2,5	0,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00

Продолжение таблицы И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2.3.2 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для сотрудников судебных и других юридических органов?	2,5	0,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2.3.3 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для работников МСП/частных компаний?	2,5	0,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2.3.4 Имеются ли национальные отраслевые образовательные программы/тренинги/курсы для других должностных лиц из государственного сектора и правительственных учреждений?	2,5	0,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
3. Осуществляет ли ваше правительство разработку или поддержку каких-либо образовательных программ или учебных планов в области кибербезопасности	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
3.1 В начальной школе?	3	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3.2 В средней школе?	3	1,2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3.3 В высшей школе?	4	1,6	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
4. Научно-исследовательские программы в области кибербезопасности	2	4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4.1 Проводится ли научно-исследовательская деятельность в области кибербезопасности на общенациональном уровне?	10	4	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
4.1.1 Имеются ли программы НИОКР по кибербезопасности в частном секторе?	4	1,6	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
4.1.2 Имеются ли программы НИОКР по кибербезопасности в государственном секторе?	3	1,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
4.1.3 Вовлечены ли в научно-исследовательскую деятельность высшие учебные заведения, такие как академии и университеты?	3	1,2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
5. Национальная отрасль кибербезопасности	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
5.1 Имеется ли национальная отрасль кибербезопасности?	10	4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
6. Имеются ли какие-либо правительственные механизмы стимулирования	2	4	-	-	-	-	0,0	0,0	1,0	1,0	-	-	-	-	-	-	-	-
6.1 Для содействия созданию потенциала в области кибербезопасности?	5	2	0	0	1	1	-	-	-	-	0,00	0,00	1,0	1,0	-	-	-	-
6.2 Для развития отрасли кибербезопасности?	5	2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
МЕРЫ В ОБЛАСТИ СОТРУДНИЧЕСТВА																		
1. Двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-

Продолжение таблицы И.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1.1 Имеются ли у вас двусторонние соглашения по сотрудничеству в области кибербезопасности с другими странами?	10	4	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
1.1.1 Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?	3,3	1,333	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.2 Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?	3,3	1,333	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
1.1.3 Предусматривает(ют) ли это (эти) соглашение(я) взаимную правовую помощь?	3,3	1,333	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
2. Участие правительства в международных механизмах, связанных с деятельностью в сфере кибербезопасности	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
2.1 Участвует ли ваше правительство/ваша организация в международных механизмах, связанных с деятельностью в сфере кибербезопасности?	10	4	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3. Многосторонние соглашения по кибербезопасности	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
3.1 Имеются ли у вашего государства многосторонние соглашения о сотрудничестве в области кибербезопасности?	10	4	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
3.1.1 Предусматривает(ют) ли это (эти) соглашение(я) обмен информацией?	5	2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
3.1.2 Предусматривает(ют) ли это (эти) соглашение(я) создание потенциала?	5	2	0	0	0	0	-	-	-	-	-	-	-	-	0,00	0,00	0,00	0,00
4. Партнерские отношения с частным сектором (ГЧП)	2	4	-	-	-	-	0,0	0,0	0,0	0,0	-	-	-	-	-	-	-	-
4.1 Участвует ли ваше правительство в ГЧП с местными компаниями?	5	2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
4.2 Участвует ли ваше правительство в ГЧП с иностранными компаниями в вашей стране?	5	2	0	0	0	0	-	-	-	-	0,00	0,00	0,00	0,00	-	-	-	-
5. Межведомственные партнерства	2	4	-	-	-	-	0,0	2,0	2,0	2,0	-	-	-	-	-	-	-	-
5.1 Имеются ли межведомственные партнерства/соглашения между различными правительственными органами, касающиеся кибербезопасности?	10	4	0	1	1	1	-	-	-	-	0,00	2,0	2,0	2,0	-	-	-	-

Приложение К. Перечень предлагаемых к принятию базовых нормативных правовых актов

Таблица К.1 – Комплекс базовых нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры ДНР

Нормативный правовой акт	Содержание	Ожидаемый результат
1	2	3
Закон ДНР «О безопасности критической информационной инфраструктуры Донецкой Народной Республики»	Утверждение принципов, полномочий, прав, обязанностей, аспектов государственного контроля, ответственность за нарушения в области обеспечения безопасности критической информационной инфраструктуры ДНР	Формирование общегосударственной системы обеспечения безопасности критической информационной инфраструктуры ДНР
Закон ДНР «О Внесении изменений в Уголовный кодекс ДНР и Уголовно-процессуальный кодекс ДНР в связи с принятием закона «О безопасности критической информационной инфраструктуры ДНР»	Утверждение положений об ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры ДНР	Формирование регуляторных основ по санкционирующим взыскательные механизмы за нарушение требований законодательства в сфере обеспечения безопасности критической информационной инфраструктуры
Указ Главы ДНР «О Едином государственном центре координации органов государственной власти в сфере обеспечения информационной безопасности»	Утверждение полномочий ЕГЦК в области защиты критической информационной инфраструктуры ДНР, защиты информации ограниченного доступа и др. направлений обеспечения ИБ в ОГВ	Создание единого экспертно-аналитического центра, способствующего развитию правовых, организационных и технических подходов к обеспечению ИБ в ОГВ
Указ Главы ДНР «О создании государственной системы управления информационной безопасностью в органах государственной власти Донецкой Народной Республики»	Утверждение полномочий субъектов ИБ в сфере функционирования системы управления информационной безопасности, связанных со значимыми объектами критической информационной инфраструктуры ДНР	Формирование системного подхода, развитие механизмов скоординированного взаимодействия ключевых субъектов обеспечения ИБ в рамках единого подхода к управлению инцидентами
Постановление Правительства ДНР «Об утверждении Правил предоставления субсидий из республиканского бюджета на создание Единого государственного центра координации органов государственной власти в сфере обеспечения ИБ»	Установка целей, условий и порядка предоставления субсидий из республиканского бюджета на создание Единого государственного центра координации ОГВ в сфере обеспечения ИБ	Способствование созданию и привлечению компетентных специалистов в Единый государственный центр координации ОГВ в сфере обеспечения ИБ
Постановление Правительства ДНР «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры ДНР»	Утверждение аспектов контрольно-надзорной деятельности за обеспечением безопасности объектов критической информационной инфраструктуры ДНР	Утверждение регуляторных основ для осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры ДНР
Постановление Правительства ДНР «Об утверждении правил категорирования объектов критической информационной инфраструктуры Донецкой Народной Республики»	Утверждение порядка и сроков категорирования объектов критической информационной инфраструктуры ДНР, а также перечня показателей критериев значимости	Утверждение структуры и этапов процесса категорирования информационных ресурсов ДНР, способствующего определению значимости объектов подлежащих выполнению требований законодательства
Указ Главы ДНР «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Донецкой Народной Республики»	Требования и состав мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры ДНР	Систематизация требований, способствующая повышению качества подходов к обеспечению безопасности значимых объектов критической информационной инфраструктуры ДНР

Продолжение таблицы К.1

1	2	3
Приказ Министерства государственной безопасности «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»	Утверждение состава и содержания работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, а также требований к форме и содержанию разрабатываемых при организации и проведении таких работ документов	Формирование системы аттестации объектов информатизации в рамках совершенствования подходов к обеспечению контрольно-надзорной деятельности за обеспечением ИБ в ОГВ
Постановление Правительства ДНР «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи ДНР для обеспечения безопасности значимых объектов критической информационной инфраструктуры»	Утверждение единых правил подготовки и использования ресурсов единой сети электросвязи ДНР для обеспечения безопасности значимых объектов критической информационной инфраструктуры ДНР	Утверждение правил защиты сетей связи и передаваемой по ним информации в соответствии с едиными требованиями по защите сетей связи от несанкционированного доступа к ним и передаваемой по ним информации
Указ Главы ДНР «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Донецкой Народной Республики»	Утверждение правил формирования и ведения Реестра значимых объектов критической информационной инфраструктуры с целью учета, осуществления государственного контроля в области обеспечения безопасности значимых объектов	Утверждение единых правил осуществления хранения и предоставления информации в бумажном и электронном виде о значимых объектах критической информационной инфраструктуры ДНР
Указ Главы ДНР «Об утверждении Порядка обмена информацией о инцидентах ИБ между субъектами критической информационной инфраструктуры ДНР и Единым государственным центром координации органов государственной власти в сфере обеспечения ИБ»	Правила обмена информацией об инцидентах ИБ между субъектами критической информационной инфраструктуры ДНР и Единым государственным центром координации ОГВ в сфере обеспечения ИБ	Повышение качества подходов к обеспечению ИБ, способствующих минимизации последствий инцидентов ИБ и предотвращения инцидентов ИБ на объектах критической информационной инфраструктуры
Указ Главы ДНР «Об утверждении требований к средствам государственной системы, управления информационной безопасностью в органах государственной власти ДНР»	Утверждение требований к устанавливаемым и используемым в ОГВ ДНР средствам, предназначенным для взаимодействия в рамках функционирования государственной системы управления ИБ в ОГВ ДНР	Повышение качества подходов к формированию и развитию технических, программных, программно-аппаратных и иных средств, используемых при взаимодействии в рамках государственной системы управления ИБ в ОГВ ДНР
Указ Главы ДНР «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для государственной системы, управления информационной безопасностью в ОГВ ДНР»	Утверждение порядка, технических условий установки и эксплуатации средств, предназначенных для государственной системы управления информационной безопасностью в ОГВ ДНР	Утверждение единого порядка и технических условий установки и эксплуатации средств, предназначенных для государственной системы управления информационной безопасностью в ОГВ ДНР
Указ Главы ДНР «Об утверждении Порядка информирования Единого государственного центра координации ОГВ в сфере обеспечения ИБ об инцидентах ИБ, реагирования на них, принятия мер по ликвидации последствий»	Утверждении Порядка информирования Единого государственного центра координации ОГВ в сфере обеспечения ИБ об инцидентах ИБ, реагирования на них, принятия мер по ликвидации последствий	Повышение уровня скоординированного взаимодействия в рамках функционирования государственной системы управления ИБ в ОГВ при информировании Единого государственного центра координации ОГВ в сфере обеспечения ИБ об инцидентах ИБ, реагировании на них и принятии мер по ликвидации последствий

Приложение Л. Этапы создания и развития систем безопасности критической информационной инфраструктуры

Таблица Л.1 – Этапы формирования систем безопасности критической информационной инфраструктуры в ОГВ

Этап	Задачи	Инструменты	Результаты
1	2	3	4
Создание комиссии по категорированию критической информационной инфраструктуры	Определение персонального состава Комиссии по категорированию критической информационной инфраструктуры для ОГВ	Разработка Положения о Комиссии критической информационной инфраструктуры	Формирование Комиссии критической информационной инфраструктуры в ОГВ
Учет объектов критической информационной инфраструктуры	Формирование и утверждение проектов Перечней объектов критической информационной инфраструктуры в ОГВ. Уведомление ответственных структур о Перечнях объектов критической информационной инфраструктуры.	Инвентаризация информационных ресурсов, которые принадлежат ОГВ. Анализ областей деятельности ОГВ, связанных с функциями объектов критической информационной инфраструктуры.	Определение критичных процессов, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов.
Категорирование значимых объектов критической информационной инфраструктуры	Формирование и утверждение перечня значимых объектов критической информационной инфраструктуры. Направление в ответственный ОГВ уведомления о результатах категорирования.	Создание акта категорирования объекта критической информационной инфраструктуры и иной сопроводительной документации.	Определение целевых уровней безопасности (категорий значимости) объектов критической информационной инфраструктуры. Занесение в реестр значимых объектов.
Проектирование подсистем безопасности значимых объектов критической информационной инфраструктуры	Разработка и утверждение приказа о создании системы безопасности значимых объектов критической информационной инфраструктуры. Приоритизация мер по оптимизации систем безопасности значимых объектов. Оценка состояния СОИБ значимых объектов. Формирование требований к СОИБ значимых объектов ОГВ.	Анализ технического задания на создание подсистемы безопасности значимых объектов. Тестирование подсистемы безопасности значимого объекта. Анализ результатов оценки рисков, моделирования угроз, оценок уязвимостей и требований к категориям значимых объектов.	Определение уровня систем безопасности значимых объектов критической информационной инфраструктуры в ОГВ. Формирования плана совершенствования и оптимизации подходов к обеспечению ИБ в ОГВ.
Разработка эксплуатационной документации	Регламентация и упорядочивание характеристик и требований к безопасности значимых объектов критической информационной инфраструктуры	Описание архитектуры подсистемы безопасности значимых объектов, порядка и параметров настройки программных и программно-аппаратных средств, в том числе средств защиты информации	Разработка организационно-распорядительных документов о правилах и процедурах обеспечения безопасности значимых объектов критической информационной инфраструктуры

Продолжение таблицы Л.1

1	2	3	4
Внедрение организационных и технических мер по обеспечению безопасности значимых объектов	1. Определение персонального состава участников процесса управления инцидентами. 2. Внедрении организационных и технических мер по обеспечению безопасности значимых объектов.	1. Разработка и принятие пакета документов, содержащих организационно-технические меры по управлению инцидентами в ОГВ. 2. Разработка и принятие пакета документов, обеспечивающих внедрение и модернизацию средств автоматизированного взаимодействия с ЕГЦК.	1. Разработка и утверждение подсистемы реагирования на инциденты ИБ в ОГВ. 2. Формализация процедур по подключению технических средств к инфраструктуре ЕГЦК с целью обеспечения автоматизированного взаимодействия.
Модернизация системы безопасности значимых объектов критической информационной инфраструктуры	1. Проектирование, разработка и внедрение систем безопасности значимых объектов критической информационной инфраструктуры ОГВ. 2. Проведение работ по подключению к государственной системе управления информационной безопасностью в ОГВ.	1. Разработка и принятие пакета документов, регламентирующих модернизацию системы безопасности. 2. Аттестация объектов информатизации. 3. Создание защищенных каналов автоматизированного взаимодействия с ЕГЦК.	Совершенствование системы безопасности значимых объектов критической информационной инфраструктуры ОГВ
Повышение уровня знаний работников по обеспечению безопасности критической информационной инфраструктуры	Проведение регулярных мероприятий по повышению уровня знаний ответственных за ИБ сотрудников ОГВ	1. Разработка и принятие пакета документов регламентирующих повышение знаний для ОГВ. 2. Взаимодействие с ЕГЦК.	Повышение уровня знаний ответственных за ИБ сотрудников ОГВ
Внутренний контроль значимых объектов, совершенствование подсистем безопасности значимых объектов критической информационной инфраструктуры	1. Проведение тренировочных мероприятий по отработке инцидентов ИБ в ОГВ. 2. Контроль и мониторинг состояния безопасности значимых объектов критической информационной инфраструктуры.	1. Разработка и принятие пакета документов, регламентирующих контроль и управление инцидентами на объектах критической информационной инфраструктуры ОГВ. 2. Анализ уязвимостей. 3. Моделирование угроз. 4. Оценка рисков. 5. Диагностика СОИБ.	1. Совершенствование СОИБ в ОГВ. 2. Повышение осведомленности и уровня подготовки ответственных сотрудников ОГВ. 3. Обеспечение бесперебойной эксплуатации значимых объектов критической информационной инфраструктуры.

Приложение М. Структура стандарта ГОСТ Р 57580.1-2017

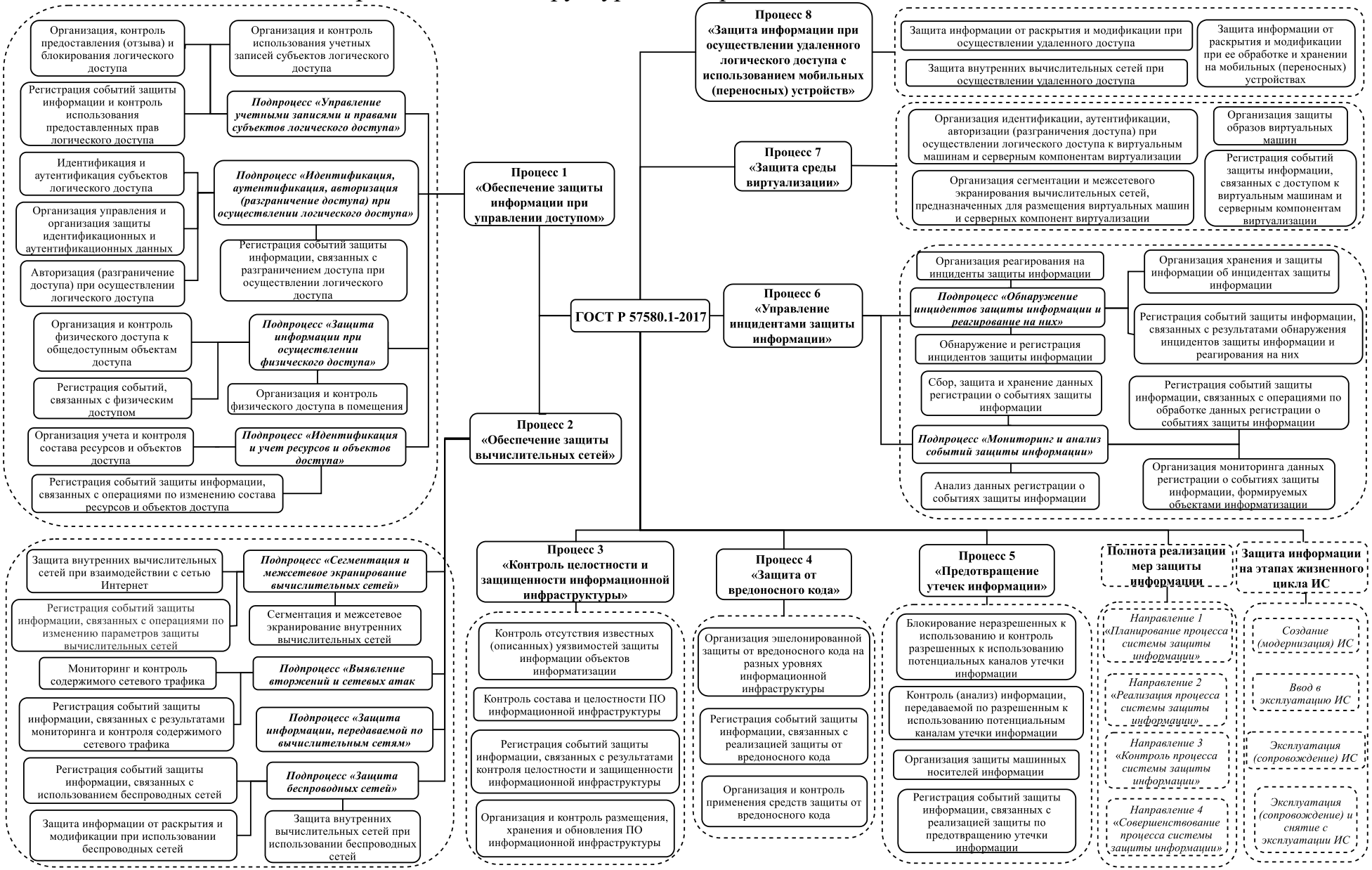

Рисунок М.1 – Структура процессов, подпроцессов и направлений оценки стандарта ГОСТ Р 57580.1-2017

Приложение Н. Фрагмент базы знаний ГОСТ 57580.1-2017

Таблица Н.1 – База знаний ГОСТ 57580.1-2017 с корреляцией в приказы ФСТЭК № 21, 239 (фрагмент)

Условное обозначение и номер меры	Содержание меры	Уровень защиты информации			Возможные способы реализации меры (О-организационный, Т-технический)	Документы, регламентирующие применение данной меры	Меры Приказа ФСТЭК № 21	Меры Приказа ФСТЭК № 239	Свидетельство/описание реализации меры либо описание проблемы с реализацией
		3	2	1					
УЗП.4	Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения	О	О	О	- закрепление данного положения в организационно-распорядительной документации; - применение правил именования учетных записей и ведения их атрибутов, которые позволяют определить целевое назначение.	Частная политика/ Регламент управления правами доступа/ Инструкция по проведению контроля	УПД.1 АНЗ.5	УПД.1	Планы проверок/Акты периодических проверок/ Письма с отчетами о блокировании учетных записей по результатам проверки
УЗП.6	Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа)	О	О	О	- документальное закрепление персональной ответственности за распределение доступа; - разбиение ресурсов на категории с определением и закреплением владельцев, утвердить регламент и в соответствии с ним настроить процедуры согласования заявок на доступ.	Частная политика/ Регламент управления правами доступа/ Приказ о назначении распорядителя доступа либо соответствующие пункты в должностной инструкции	УПД.2	УПД.2	Реестр ресурсов и объектов доступа, в котором в отдельном столбце прописываются владельцы ресурсов/Приказ о назначении владельцев ресурсов
УЗП.13	Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа	О	Т	Т	О - настройка срока действия для учетных записей, контроль учетных записей при увольнении; Т – внедрение системы управления доступом (IDM), осуществляющей контроль срока действия учетных записей.	Частная политика / Регламент управления правами доступа/ Инструкция по проведению контроля	УПД.1	УПД.1	Не все прикладное ПО имеет возможность настройки ограничений по времени действия учетной записи или пароля, необходима сверка локальных учетных записей, учетных записей в прикладном ПО и СУБД
РД.11	Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин	Т	Т	Т	- групповая политика безопасности домена; - настройки блокировки учетных записей в информационных системах (ограничение количества неудачных попыток аутентификации).	Регламент предоставления прав доступа или управления учётными данными	УПД.6	УПД.6	Проверка настроек групповых политик безопасности, объектов информатизации, регламентов и инструкций, формализующих закрепление данного положения