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)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата экономических наук

Донецк – 2021

Работа выполнена в Государственном образовательном учреждении высшего профессионального образования «Донецкий национальный технический университет», г. Донецк.

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

Официальные оппоненты: **Захаров Сергей Викторович,**
доктор экономических наук, доцент,
ООО «Форвардер», заместитель директора по маркетингу и продажам

Гончарова Татьяна Валериановна,
кандидат экономических наук,
Государственная организация высшего профессионального образования «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», доцент кафедры товароведения

Ведущая организация: Государственное образовательное учреждение высшего профессионального образования **«Донецкий национальный университет»**

Защита состоится «15» апреля 2022 года в 14.00 часов на заседании диссертационного совета Д 01.001.01 при Государственном образовательном учреждении высшего профессионального образования «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики» по адресу: 83015, г. Донецк, ул. Челюскинцев, 163а, к. 205. Тел. факс: +38(062) 305-45-36, e-mail: d_01.001.01@donampa.ru.

С диссертацией можно ознакомиться в библиотеке Государственного образовательного учреждения высшего профессионального образования «Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики» по адресу: 83015, г. Донецк, ул. Челюскинцев, 163а, к. 406 (http://donampa.ru/).

Автореферат разослан «__» _____ 20__ г.

Ученый секретарь
диссертационного совета Д 01.001.01,
канд. гос. упр., доцент А.В. Кретова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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 ГОУ ВПО «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).

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 другом издании, 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.

Структура и объем работы. Диссертация состоит из введения, трех глав, заключения, списка литературы из 252 наименований и 12 приложений (объемом 27 страниц). Общий объем диссертации составляет 281 страницу.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

В первой главе **«Теоретические и методические основы формирования системы обеспечения информационной безопасности в органах государственной власти»** раскрыта сущность процесса обеспечения информационной безопасности в органах государственной власти; исследованы подходы к формированию и развитию систем обеспечения информационной безопасности в публичном управлении; изучен зарубежный опыт функционирования систем обеспечения информационной безопасности в органах государственной власти.

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.

По результатам выявления особенностей системы обеспечения информационной безопасности дана уточненная трактовка понятия «информационная безопасность» в органах государственной власти, в контексте которого 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.

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.

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. Сформирована связь структурных элементов публичного управления и электронного правительства (рисунок 1).

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.

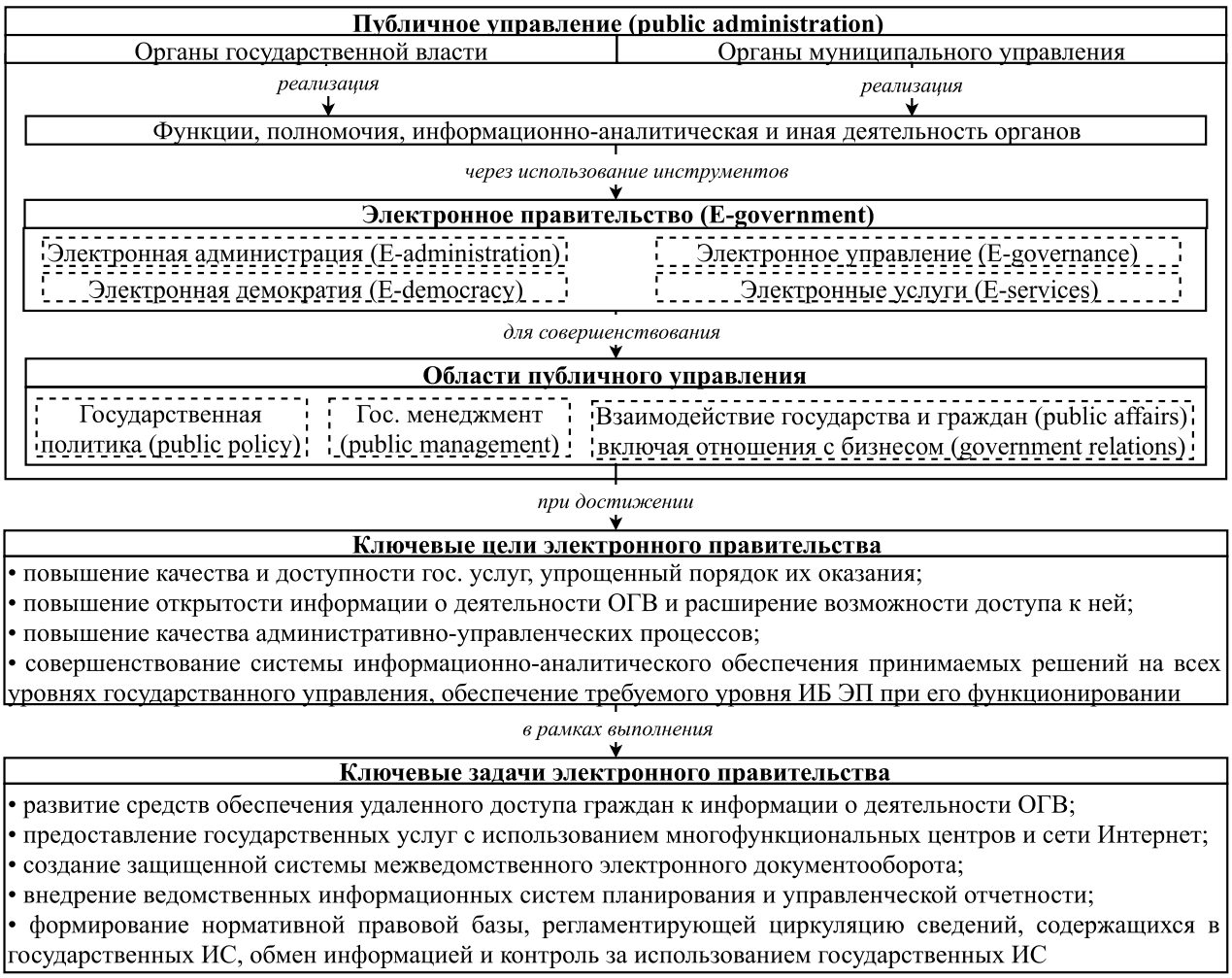

Рисунок 1 – Связь структурных элементов публичного управления и электронного правительства

Сформирована обобщенная инфраструктура электронного правительства (рисунок 2).

Рисунок 2 – Инфраструктура электронного правительства

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 (рисунок 3).

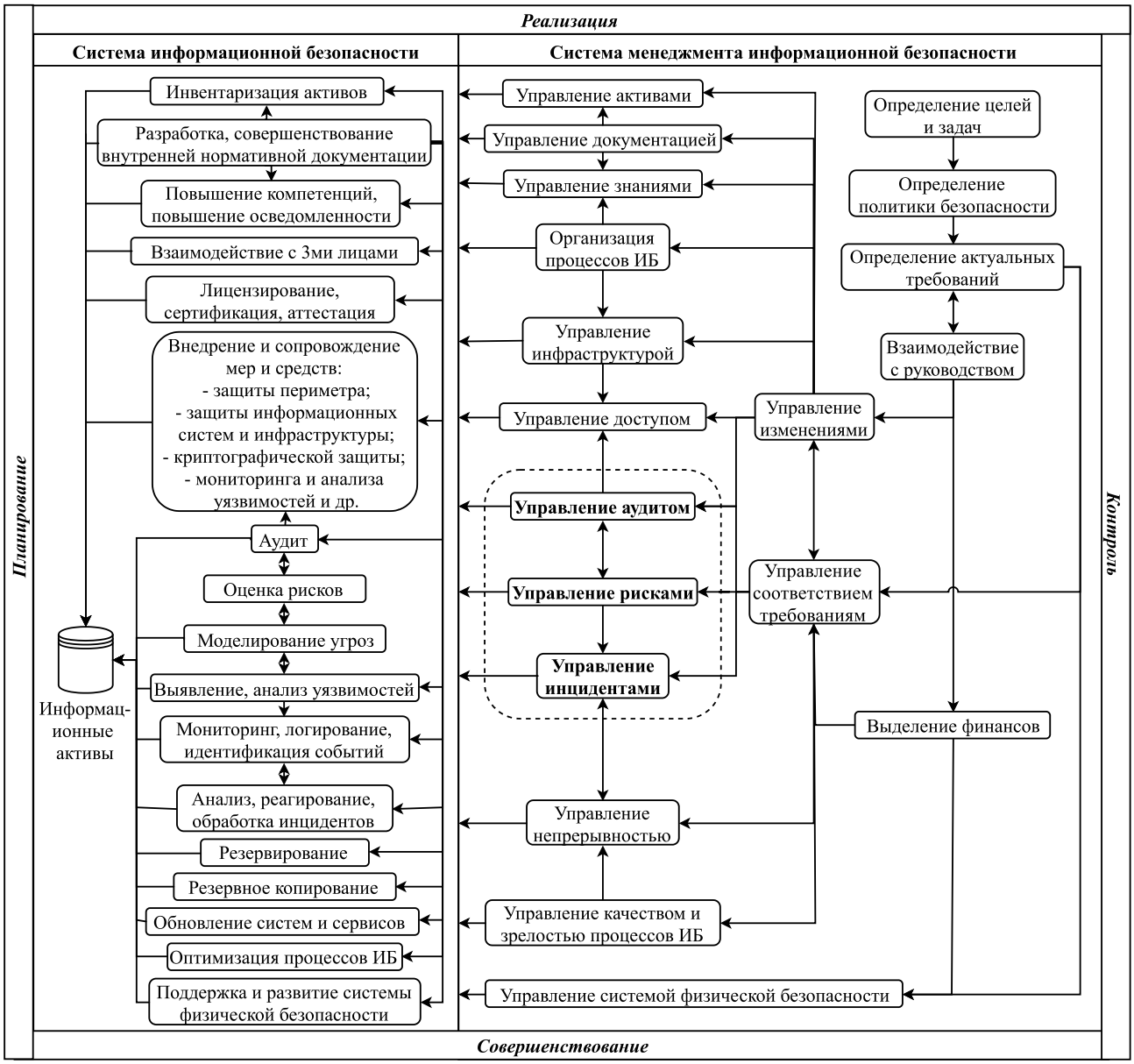

Рисунок 3 – Модель процессов системы обеспечения информационной безопасности согласно серии ГОСТ Р ИСО/МЭК 2700х

Составной частью предложенной модели является выделенная иерархическая структура процессов и их связей, опирающаяся на международные стандарты серии ГОСТ Р ИСО/МЭК 2700х и дополненная набором процессов подсистем и структурно-логических связей между ними, что способствует оптимизации структуры системы обеспечения информационной безопасности и формированию современного видения применения комплексного подхода к ее совершенствованию.

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.

Исследование зарубежного опыта функционирования систем обеспечения информационной безопасности в США, Европейском Союзе, Германии и России позволило установить две основные модели регулирования ключевого направления исследуемой сферы, – 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 (далее – ДНР) 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.

Во второй главе **«Анализ функционирования системы обеспечения информационной безопасности в органах государственной власти»** проведен анализ состояния информационного обеспечения системы публичного управления в ДНР; исследованы современные тенденции развития сферы обеспечения информационной безопасности в ДНР; проведена оценка рисков информационной безопасности в органе государственной власти.

Выявление и анализ ключевых информационных систем органов государственной власти 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. Определено состояние и динамика развития Индекса телекоммуникационной инфраструктуры (Telecommunication Infrastructure Index, TII), являющегося одним из трех составных элементов Индекса развития электронного правительства (E-Government Development Index, EGDI), определяемого Департаментом экономического и социального развития ООН (рисунок 4).

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.

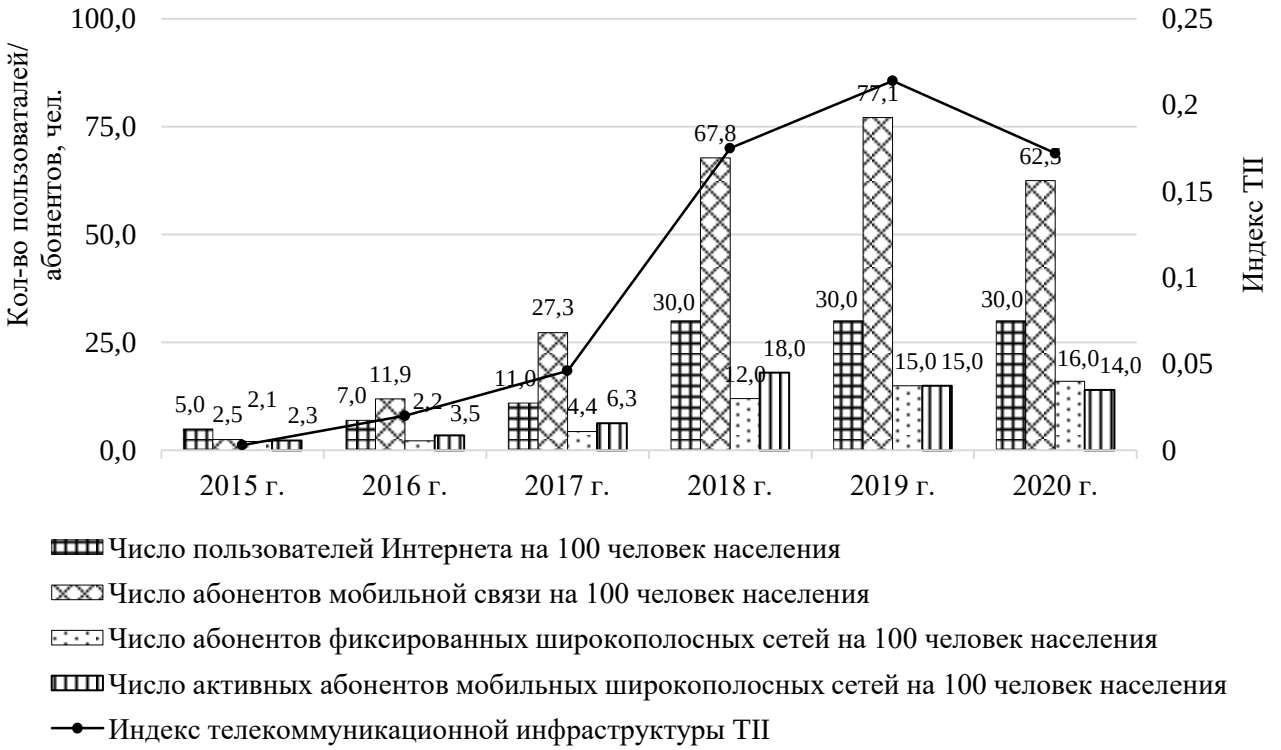

Рисунок 4 – Динамика развития Индекса телекоммуникационной инфраструктуры TII и его составляющих в ДНР, 2015-2020 гг.

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.

Проведенный анализ современного состояния правового и организационного обеспечения позволил выделить ключевые регуляторные и структурные проблемы органов государственной власти в отрасли информационных технологий и сфере обеспечения информационной безопасности.

Систематизация факторов, а также определение актуальных типов угроз, влияющих на безопасность государственных информационных систем позволили выделить основные группы рисков безопасности, свойственных информационным средам органов государственной власти ДНР.

Исследование современных тенденций развития сферы обеспечения информационной безопасности 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 согласно экспертным оценкам не наблюдается (рисунок 5).

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.

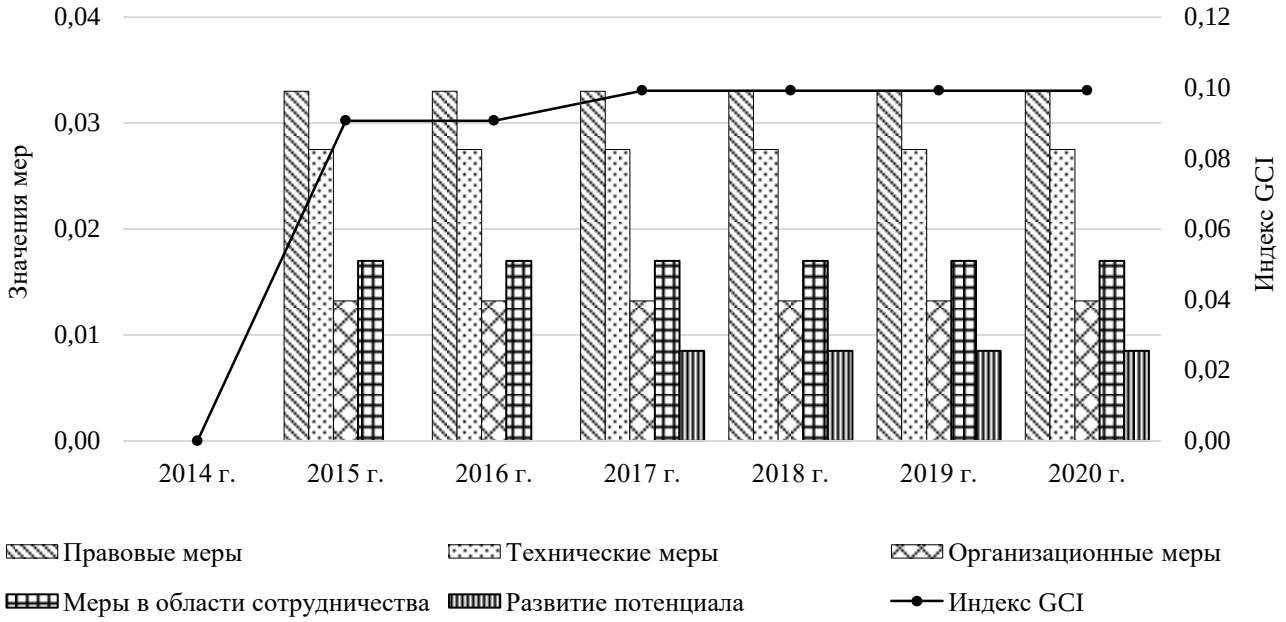

Рисунок 5 – Динамика развития Глобального индекса кибербезопасности (GCI) и его составляющих согласно экспертным оценкам, ДНР, 2014-2020 гг.

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.

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.

Усовершенствован методический подход к оценке рисков информационной безопасности в органах государственной власти. Предложенный подход предусматривает алгоритм, базирующийся на моделировании угроз безопасности информации и оценке уязвимостей информационных активов органа государственной власти и позволяет определить способы реализации выявленных угроз, уровень рисков, связанный с каждой угрозой, и приоритизировать последовательность их обработки (рисунок 6).

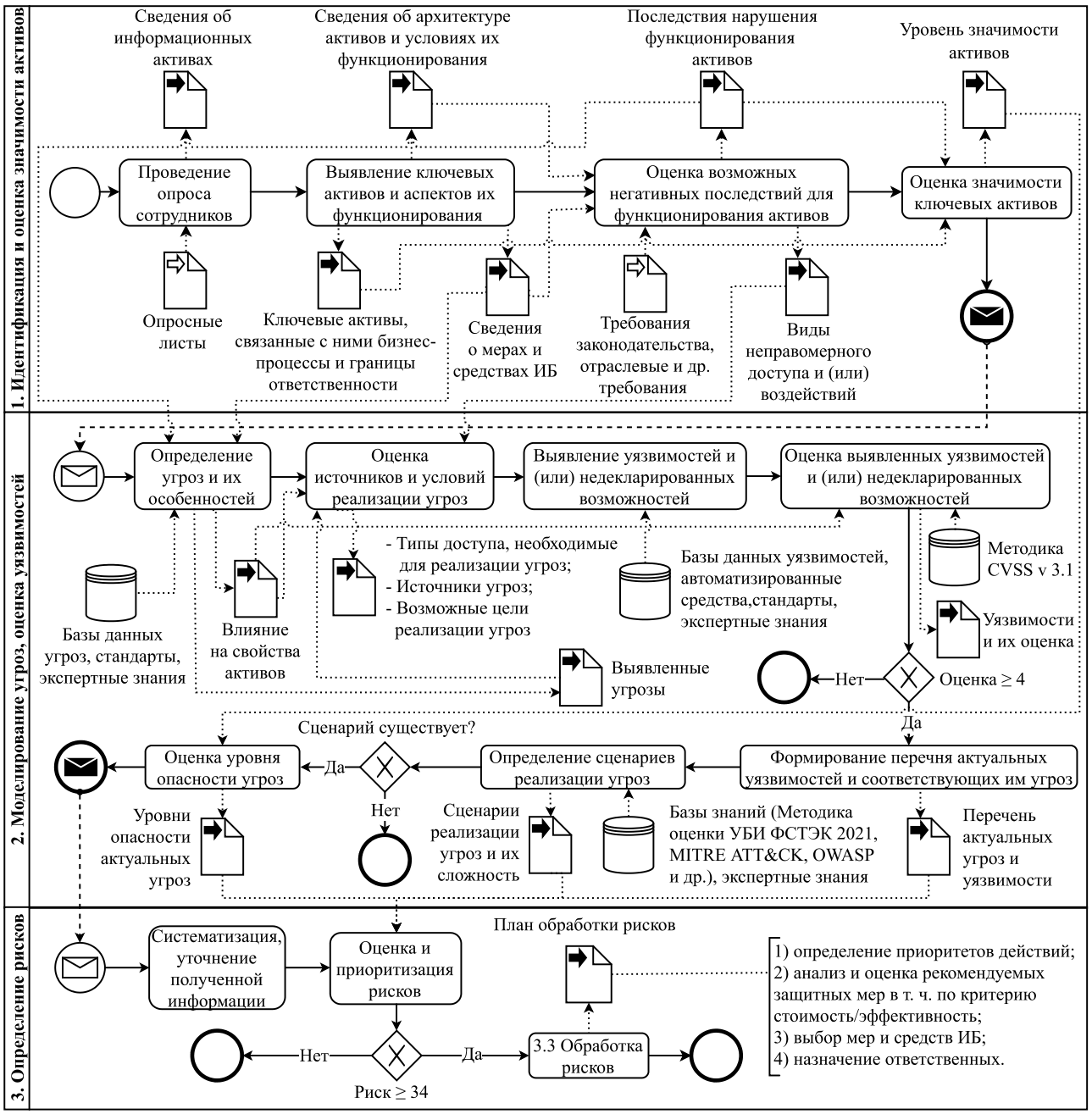

Рисунок 6 – Алгоритм оценки рисков информационной безопасности в органах государственной власти

В таблице 1 представлены результаты оценки рисков информационной безопасности в Министерстве связи ДНР. Чем больше значение риска (K_i), тем выше приоритет его обработки. В случае совпадения значений рисков для разных активов приоритет обработки отдается активу с наибольшим общим риском (O_i).

По результатам расчета определено, что, несмотря на наличие рисков информационной безопасности, большинство из них являются низкими либо средними, что говорит о достаточно высоком организационно-техническом уровне обеспечения информационной безопасности в Министерстве связи ДНР, т.к. несмотря на наличие выявленных экспертами уязвимостей и угроз,

значительное их количество купировано мерами и средствами обеспечения информационной безопасности.

Таблица 1 – Результирующая таблица оценки рисков информационной безопасности в Министерстве связи ДНР (фрагмент)

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			
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	
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	

После приоритизации выявленных рисков на основании полученных от экспертов рекомендаций проведена оптимизация мер и средств обеспечения информационной безопасности.

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 системы обеспечения информационной безопасности, в связи с чем целесообразно провести комплексную диагностику, включающую анализ и оценку процессов системы менеджмента информационной безопасности.

В результате аналитического исследования определены ключевые направления, способы и ориентиры для разработки комплекса рекомендаций по совершенствованию существующих подходов к обеспечению информационной безопасности в органах государственной власти ДНР.

В третьей главе **«Разработка рекомендаций по совершенствованию системы обеспечения информационной безопасности в органах государственной власти»** разработана концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти; обоснована целесообразность формирования архитектуры единого информационного пространства органов государственной власти; разработан методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти.

Предложен теоретико-методический подход к совершенствованию системы обеспечения информационной безопасности в органах государственной власти ДНР за счет разработки концепции совершенствования системы (рисунок 7), 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 системы обеспечения информационной безопасности на общегосударственном уровне и уровне органов государственной власти, 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 органах государственной власти.

Обоснована необходимость создания Единого государственного центра координации органов государственной власти в сфере обеспечения информационной безопасности (далее – ЕГЦК), 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; определены группы сервисов, предоставляемых ЕГЦК для органов государственной власти ДНР; определены этапы создания ЕГЦК.

Определены ключевые цели создания и сформирована архитектура основных систем и субъектов единого информационного пространства органов государственной власти ДНР (далее – ЕИП). Предложенная архитектура учитывает важнейшие системы электронного правительства, обеспечивающие защищенный централизованный обмен данными между органами государственной власти и гражданами и позволяет создать единый механизм предоставления государственных услуг в электронном виде.

Сформирована обобщенная схема организации процесса управления ЕИП, которая предполагает создание центра обработки данных, выполняющего инфраструктурную функцию электронного правительства с последующей поступательной миграцией в его состав ключевых государственных информационных систем.

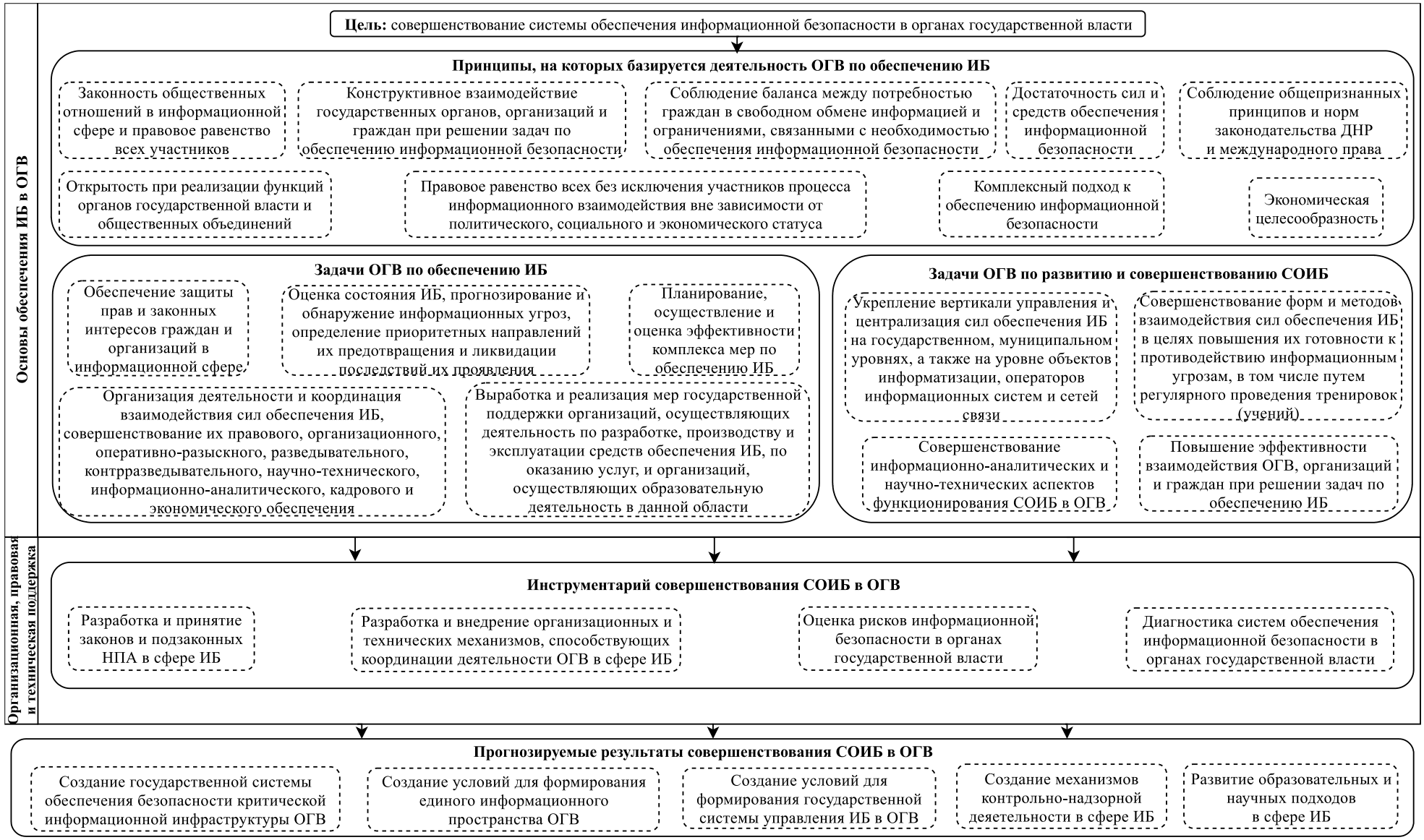

Рисунок 7 – Концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти

Определено, что инфраструктура ЕИП в рамках ролевой модели должна предоставлять сервисы для разных типов пользователей с разным уровнем доступа и набором полномочий, среди которых выделены и описаны ключевые.

Предложены организационные подходы к формированию архитектуры ЕИП 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 органов государственной власти с ЕГЦК в рамках государственной системы управления информационной безопасностью, а также обобщенный план создания ЕИП и выделены основные положения ожидаемого социально-экономического эффекта от его функционирования.

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.

В целях оптимизации процесса оценки эффективности системы обеспечения информационной безопасности в органах государственной власти получил дальнейшее развитие 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.

Сформирована модель выборок процессов из лучших мировых практик в сфере комплексного обеспечения информационной безопасности, способствующая определению перечня необходимых к оценке процессов для

формирования комплексной модели диагностики системы обеспечения информационной безопасности.

Определен перечень специализаций экспертов с соответствующими профессиональными знаниями и навыками, необходимыми для компетентного проведения диагностики в рамках разработанных этапов методического подхода.

С целью отображения основных компонентов диагностики системы обеспечения информационной безопасности в органах государственной власти, их характеристик и взаимосвязей между ними разработана информационная модель элементов комплексной диагностики.

С учетом обозначенных целей разработанной модели выборок процессов из «лучших практик», а также компонентов сформированной информационной модели определены и декомпозированы ключевые этапы, необходимые для проведения всесторонней и адаптированной для органов государственной власти комплексной диагностики системы обеспечения информационной безопасности.

В результате проведенного исследования сформирована поэтапная схема реализации методического подхода к комплексной диагностике, в которой определены основные процессы этапов диагностики, порядок реализации которых оптимизирован и конкретизирован в виде схемы процессов. Структурированная информация, необходимая для поддержки функций комплексной диагностики системы обеспечения информационной безопасности в органах государственной власти, позволила выделить основные этапы ее проведения, проследить корреляционные взаимоотношения между процессами и подпроцессами, а также взаимосвязи активов и производственных процессов и сформировать комплексную модель диагностики.

Определена ресурсоемкость процедуры комплексной диагностики в рамках проведения всех обозначенных этапов. Обоснована важность и приоритетность оценки на соответствие требованиям регуляторов и «лучшим практикам» в рамках комплексной диагностики для органов государственной власти, т.к. данный способ позволяет как провести анализ уровня мер, средств и процессов обеспечения информационной безопасности в органах государственной власти с оптимальной затратой ресурсов, так и выстраивать общегосударственную систему обеспечения информационной безопасности, позволяя осуществить количественную оценку ее уровня с последующим контролем зрелости процессов обеспечения информационной безопасности.

С целью проведения диагностики системы обеспечения информационной безопасности в органе государственной власти ДНР на соответствие ГОСТ Р 57580.1-2017, адаптированному к сфере государственного управления, и с использованием методики, базирующейся на ГОСТ Р 57580.2-2018, автором разработан алгоритм, учитывающий показатели процессов и шкалу определения уровня их зрелости (рисунок 8). С целью систематизации структуры исследованного стандарта сформирована схема, содержащая структуру процессов, подпроцессов и направлений оценки соответствия требованиям данного стандарта.

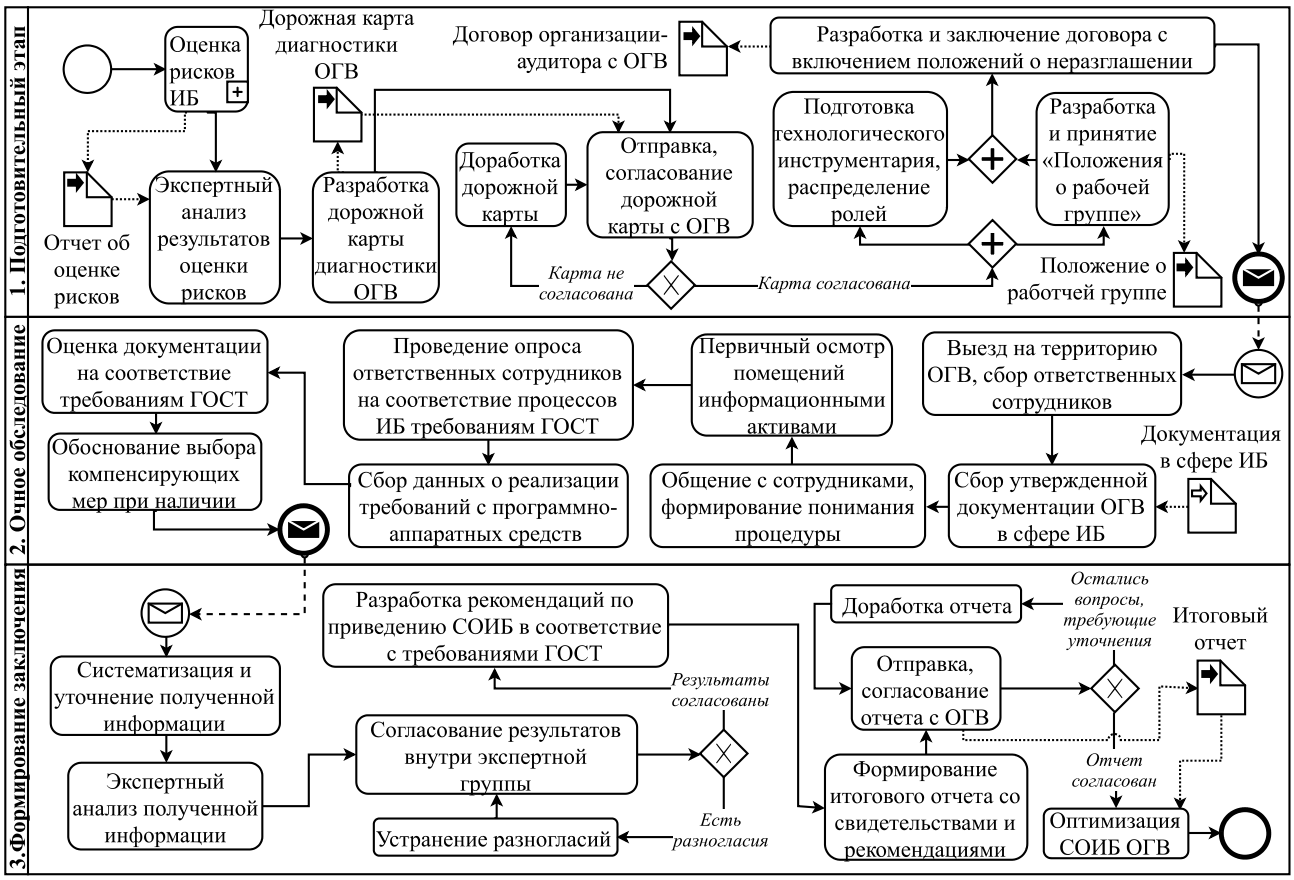

Рисунок 8 – Алгоритм диагностики системы обеспечения информационной безопасности в органах государственной власти на соответствие требованиям стандарта

Приведены показатели, определяющие соответствие системы обеспечения информационной безопасности органа государственной власти адаптированным требованиям стандарта и способы их расчета. Адаптирована шкала определения значений уровней соответствия процессов системы обеспечения информационной безопасности органа государственной власти.

Согласно сформированному алгоритму проведена диагностика системы обеспечения информационной безопасности Министерства связи ДНР. В результате проведения диагностики выявлено, что оценки, характеризующие уровень зрелости процессов системы обеспечения информационной безопасности в Министерстве связи ДНР согласно установленной шкале, определены как высокие (большинство из них соответствует нормативному значению в 0,6 баллов).

На заключительном этапе диагностики сформировано экспертное заключение, в котором формализованы рекомендации по оптимизации исследованной системы обеспечения информационной безопасности.

Проведенное исследование позволило структурировать информацию, необходимую для осуществления комплексной диагностики системы обеспечения информационной безопасности в органе государственной власти, выделить основные этапы ее проведения, проследить корреляционные взаимоотношения между процессами и подпроцессами, а также взаимосвязи

объектов и процессов процедуры и сформировать комплексную модель диагностики, ключевой этап которой декомпозирован, систематизирован и усовершенствован, что позволило сформировать оптимальный механизм определения состояния системы обеспечения информационной безопасности в органах государственной власти.

Усовершенствованный методический подход дал возможность выбрать и обосновать эталонные значения критериев состояния системы обеспечения информационной безопасности органа государственной власти и осуществить объективную оценку уровня ее зрелости, а также определить и классифицировать ее основные процессные составляющие, отличающиеся от существующих тем, что имеют более полную структуру и являются адаптированными под специфику органов государственной власти.

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 РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

Монографии

1. 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. (1,56 / 0,78 п.л.)

Личный вклад соискателя: проведен анализ зарубежного и отечественного опыта формирования системы обеспечения информационной безопасности.

Статьи в рецензируемых научных изданиях

2. 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. (0,62 / 0,31 п.л.)

Личный вклад соискателя: определены основные проблемы безопасности, существующие в информационных системах органов государственной власти.

3. 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. (0,81 / 0,4 п.л.)

Личный вклад соискателя: определены подходы к регулированию в странах Европейского Союза сферы защиты персональных данных.

4. 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. (0,5 п.л.)

5. 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. (0,56 / 0,28 п.л.)

Личный вклад соискателя: уточнено понятие «информационная безопасность» в органах государственной власти.

6. 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. (0,63 п.л.)

7. 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. (0,56 п.л.)

Публикации в других изданиях

8. 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. (0,38 / 0,19 п.л.)

Личный вклад соискателя: определены особенности формирования и развития единого государственного информационного пространства.

Труды апробационного характера

9. 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. (0,19 / 0,1 п.л.)

Личный вклад соискателя: определены задачи и компоненты создания единого государственного информационного пространства.

10. 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. (0,25 / 0,13 п.л.)

Личный вклад соискателя: определены аспекты совершенствования единого государственного информационного пространства.

11. 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. (0,25 / 0,13 п.л.)

Личный вклад соискателя: исследована динамика угроз безопасности информации, связанных с утечками информации в государственных информационных системах.

12. 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. (0,44 п.л.)

13. 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. (0,5 / 0,25 п.л.)

Личный вклад соискателя: исследованы аспекты, связанные с лицензированием в сфере обеспечения информационной безопасности в Российской Федерации.

14. 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. (0,37 / 0,13 п.л.)

Личный вклад соискателя: определены современные аспекты государственного регулирования сферы обеспечения информационной безопасности.

15. 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. (0,44 / 0,22 п.л.)

Личный вклад соискателя: определены тенденции регулирования сферы кибербезопасности.

16. 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. (0,31 / 0,15 п.л.)

Личный вклад соискателя: определены тенденции и вызовы, связанные с кадровым обеспечением цифровой экономики.

17. 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. (0,5 / 0,25 п.л.)

Личный вклад соискателя: определены направления формирования бюджета на оценку уровня кибербезопасности организации.

18. 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. (0,43 / 0,22 п.л.)

Личный вклад соискателя: исследованы основные подходы к оценке эффективности национальных стратегий кибербезопасности.

19. 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. (0,6 п.л.)

АННОТАЦИЯ

Джура Г.С. Совершенствование системы обеспечения информационной безопасности в органах государственной власти. – На правах рукописи.

Диссертация на соискание ученой степени кандидата экономических наук по специальности 08.00.05 – Экономика и управление народным хозяйством. – Государственное образовательное учреждение высшего профессионального образования «Донецкий национальный технический университет», Донецк, 2021.

Диссертация посвящена развитию теоретических положений и научно-методических подходов, разработке практических рекомендаций по совершенствованию системы обеспечения информационной безопасности в органах государственной власти.

Предложена авторская формулировка понятий «информационная безопасность» и «информационный актив» в органах государственной власти. Разработана оптимизированная модель процессов системы обеспечения информационной безопасности. Определена целесообразность применения системного подхода к обеспечению информационной безопасности и объектной модели регулирования, способствующих совершенствованию системы обеспечения информационной безопасности в органах государственной власти ДНР.

Проанализировано состояние информационного обеспечения системы публичного управления в ДНР. Исследованы современные тенденции развития сферы обеспечения информационной безопасности в ДНР. Проанализированы показатели, отражающие состояние общегосударственных подходов к обеспечению информационной безопасности, на основании которых определены основные направления совершенствования объекта исследования. Проведена оценка рисков информационной безопасности органа государственной власти, результаты которой позволили выявить актуальные риски для ключевых информационных активов органа государственной власти.

Разработана концепция совершенствования системы обеспечения информационной безопасности в органах государственной власти. Обосновано создание Единого государственного центра координации органов государственной власти в сфере обеспечения информационной безопасности. Предложена архитектура единого информационного пространства органов

государственной власти. Обоснована целесообразность создания государственной системы управления информационной безопасностью в органах государственной власти. Разработан методический подход к комплексной диагностике системы обеспечения информационной безопасности в органах государственной власти.

Ключевые слова: информационная безопасность, система обеспечения информационной безопасности, орган государственной власти, информационный актив, оценка рисков, единое информационное пространство, методический подход.

ANNOTATION

Dzhura G.S. Improving the information security system in state authorities. – As a manuscript.

Dissertation for the degree of candidate of economic sciences in the specialty 08.00.05 – Economics and management of the national economy. – State Higher Education Establishment «Donetsk National Technical University», Donetsk, 2021.

The dissertation is devoted to the development of theoretical provisions and scientific and methodological approaches, the development of practical recommendations for improving the information security system in state authorities.

The author's wording of the concepts of «information security» and «information asset» in state authorities is proposed. An optimized model of information security system processes has been developed. The feasibility of applying an integrated approach to ensuring information security and an object model of regulation that contribute to the improvement of the information security system in the state authorities of the DPR has been determined.

The state of information support of the public administration system in the DPR is analyzed. The current trends in the development of the sphere of information security in the DPR are investigated. The indicators reflecting the state of national approaches to ensuring information security are analyzed, on the basis of which the main directions of improving the research object are determined. An assessment of information security risks of a public authority was carried out, the results of which made it possible to identify actual risks for key information assets of a public authority.

The concept of improving the information security system in government bodies has been developed. The creation of the Unified State Center for Coordinating Government Bodies in the Field of Information Security has been substantiated. The architecture of a unified information space of public authorities is proposed. The expediency of creating a state information security management system in government bodies has been substantiated. A methodical approach to the complex diagnostics of the information security system in public authorities has been developed.

Key words: information security, information security system, government body, information asset, risk assessment, unified information space, methodical approach.

Подписано в печать 21.01.2022 г.
Формат 60х84х1/16 Усл. печ. л. 1,5.
Печать лазерная. Заказ № ___. Тираж 100 экз.
Отпечатано ФЛП Рыжков Олег Дмитриевич.
Свидетельство о регистрации АА01 № 18228 от 28.10.2014 г.
83092, г. Донецк-92, ул. Независимости, 22/97.
Тел. +38(071) 334-91-79, e-mail: mpvik@3g.ua.