Министерство цифрового развития, связи и массовых коммуникаций
Российской Федерации
Ордена Трудового Красного Знамени федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский технический университет связи и информатики»

На правах рукописи

Маклачкова Виктория Валентиновна

МОДЕЛИ И АЛГОРИТМЫ ОЦЕНКИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И РЕСУРСОВ КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Специальность 2.3.8. «Информатика и информационные процессы»

(технические науки)

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель:

доктор технических наук, профессор

Докучаев Владимир Анатольевич

Москва – 2025 г.

Оглавление

Введение

Актуальность темы исследования. В рамках реализации Национального проекта «Экономика данных и цифровая трансформация государственного управления» во всех сферах экономической жизни возникает большое количество новых задач, решение которых требует качественной обработки всё больших объёмов информации конфиденциального характера, к которой относятся персональные данные (ПДн) субъекта [88]. Это, в свою очередь, ведёт к увеличению как капитальных вложений, так и эксплуатационных затрат на создание и сопровождение соответствующих корпоративных информационных систем (ИС).

В соответствие с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ (далее - Закон № 152-ФЗ) персональными данными считается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)» [135], т.е. ПДн, «*в отличии от остальных типов данных*, связаны с конкретной личностью. Кроме того, законодательство устанавливает для оператора ПДн особые правила для обеспечения безопасной обработки ПДн с целью их защиты от несанкционированного доступа, раскрытия, использования и распространения» [206]. Также в соответствии с Законом № 152-ФЗ и Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» ПДн *выделяются в отдельный класс обрабатываемых данных*. «Поэтому нарушение качества ПДн может привести к серьезным последствиям для оператора и субъекта персональных данных» [23,98].

«Для организаций в условиях цифровой трансформации экономики совокупность вопросов, связанных с автоматизированной обработкой ПДн в ИС, носит, как внутренний, так и внешний характер, т.е. с одной стороны – контроль эффективности использования ресурсов ИС и возникающих в процессе обработки рисков нарушения качества ПДн» [92], а с другой – взаимоотношение с клиентами

и партнерами. Проблема качества персональных данных затрагивает организацию в целом (репутационные, экономические, юридические, имиджевые риски и т.д.) и её работников (репутация, угрозы здоровью и жизни, доходы и т.д.) [43]. Современные информационные системы персональных данных, построенные с использованием передовых информационно-коммуникационных технологий, являются в настоящее время универсальными автоматизированными системами поддержки бизнес- и технологических процессов предприятия, обладающими разнообразной функциональностью и способностью обработки и хранения большого количества персональных данных разных категорий. При этом должны обеспечиваться эффективность использования ресурсов информационных систем и «качество обрабатываемых в них ПДн (полнота, достоверность, конфиденциальность, доступность и целостность)» [44,45,55,125,149].

Под информационной системой персональных данных (ИСПДн) в соответствии с Законом № 152-ФЗ будем понимать корпоративную автоматизированную ИС как совокупность содержащихся в базах данных (БД) ПДн физических лиц, информационных технологий и технических средств для обработки этих ПДн [135]. ИСПДн с учётом требований Закона № 152-ФЗ и нормативных актов федеральных регуляторов предлагается классифицировать по следующим признакам:

1. По правовому статусу оператора персональных данных:

- государственные органы;
- коммерческие организации;
- некоммерческие организации.

2. По цели обработки:

- коммерческая деятельность – сбор и использование данных для маркетинга, оказания услуг, взаимодействия с клиентами и т.п.;
- государственная и муниципальная деятельность – обработка данных в рамках исполнения государственных функций и оказания услуг населению;

− научная и образовательная деятельность – исследование, обучение, статистика и т.п.;

− социальная сфера – здравоохранение, социальное обеспечение, благотворительность.

3. По типу обрабатываемых данных:

− общие ПДн (ФИО, дата рождения, адрес и т.п.);

− специальные категории «ПДн (данные о здоровье, национальности и т.п.);

− биометрические ПДн (отпечатки пальцев, фотографии лица и др.);

− обезличенные ПДн;

− общедоступные ПДн (разрешенные субъектом ПДн для распространения)» [135].

4. По объему обрабатываемых данных:

− большие системы (обрабатывают данные от 100000 субъектов);

− средние системы (обрабатывают данные от 1000 до 100000 субъектов);

− малые системы (обрабатывают данные менее чем 1000 субъектов).

5. По месту хранения и обработки ПДн:

− локальные системы (ПДн хранятся и обрабатываются внутри организации);

− распределенные системы (для хранения и обработки ПДн используются облачные технологии или несколько серверов).

6. По характеру доступа:

− открытые системы (доступ к ПДн возможен через интернет);

− закрытые системы (ограниченный доступ к ПДн внутри корпоративной информационно-телекоммуникационной сети).

В рамках настоящей диссертационной работы исследуются большие открытые корпоративные ИСПДн с мультиоблачной архитектурой, обрабатывающие общие, общедоступные персональные данные и специальные категории персональных данных и предназначенные для коммерческой, научной, образовательной и социальной сфер деятельности коммерческих и некоммерческих организаций.

Для обеспечения безопасных информационных процессов обработки того огромного количества персональных данных, которое организации вынуждены собирать и хранить для выполнения своих бизнес- и технологических процессов (например, в ИСПДн ОАО «РЖД» может обрабатываться и храниться несколько миллиардов любых категорий персональных данных), а также для выполнения требований законодательства в области персональных данных крупные предприятия всё чаще используют в ИСПДн мультиоблачную архитектуру, что ведёт к усложнению контроля за эффективностью функционирования подобных систем и усложнению сценариев обработки запросов к персональным данным [51]. Кроме того, использование мультиоблачной архитектуры в информационных системах способствует расширению ландшафта потенциальных рисков нарушения «качества обработки персональных данных» [79].

Выделение «ПДн в отдельный класс обрабатываемых в ИС данных послужило причиной появления рисков, связанных именно с обработкой таких данных. В последние годы наблюдается резкое увеличение нарушения качества ПДн» [206] (включая их утечки), что оказывает прямое влияние на эффективность бизнес-процессов и может нести экономические, социальные, финансовые, экологические и прочие опасности и угрозы как для организации в целом, так и для субъекта (субъектов) персональных данных [206].

Так, согласно [3] в Российской Федерации доля утечек персональных данных среди всех типов скомпрометированных данных в 2024 г. составила порядка 65%. В 2024 году согласно [15] было официально выявлено 135 фактов утечек персональных данных, содержащих более 710 млн записей. Однако фактическое количество утекших персональных данных согласно [3] существенно выше выявленного - более 1,5 млрд записей в 2024 году (за 2023 г. эта цифра составила 1,2 млрд записей). На сегодняшний день РФ занимает пятое место в мире по количеству утечек персональных данных. По итогам 2024 года ее обгоняют только США, Китай, Индия и Испания [4]. Также отметим, что поменялись и мотивы злоумышленников, когда ими двигают не желание получить финансовую выгоду, а политические цели. Следствием чего становится то, что похищенные данные

оказываются в открытом доступе и ими в преступных целях могут воспользоваться мошенники.

Таким образом в связи с вышеизложенным требуют решения следующие задачи, связанные с автоматизированной обработкой ПДн в корпоративных ИС:

− мониторинг и оценка эффективности использования задействованных в автоматизированной обработке запросов к персональным данным ресурсов ИСПДн с мультиоблачной архитектурой;

− осуществление на постоянной основе оценки рисков нарушения качества обрабатываемых ПДн для оценки эффективности ИСПДн с точки зрения используемых в ней защитных мер, снижающих уровень информационных рисков ПДн в ИСПДн.

Под качеством обработки персональных данных в диссертации понимается обеспечение безопасной реализации процедур их автоматизированной обработки с целью выполнения требований нормативных правовых актов, эффективного использования ресурсов ИСПДн и минимизации рисков нарушения качества персональных данных.

Оценку эффективности использования ресурсов ИСПДн с мультиоблачной архитектурой предложено проводить на основе следующих показателей: способность системы справляться с нагрузкой, время обработки заявок, эффективность загрузки системы.

Под риском нарушения качества персональных данных, или иначе информационным риском персональных данных (далее информационный риск или риск), будем понимать возможность наступления случайного события в ИСПДн в целом или в её отдельных элементах, приводящего к снижению качества ПДн. Результатом «данного события может быть ущерб организации или субъекту ПДн» [46,52,62,122].

Решение выделенных задач возможно путём применения для отслеживания информационных процессов обслуживания запросов на автоматизированную обработку ПДн в ИСПДн [122] и оценки эффективности использования ресурсов ИСПДн соответствующих моделей и алгоритмов, которые позволяют учитывать

особенности обработки ПДн, а для оценки и минимизации рисков нарушения качества ПДн – моделей и алгоритмов, которые позволяют кастомизировать оценку рисков, быстро реагировать на изменяющиеся окружающие условия, а также учитывать новые и нестандартные угрозы и уязвимости.

Степень разработанности темы исследования. В диссертационной работе исследуются и разрабатываются модели и алгоритмы оценки эффективности использования ресурсов корпоративных автоматизированных информационных систем при работе с ПДн, а также оценки и минимизации информационных рисков, возникающих при обработке ПДн в корпоративных ИС. В качестве корпоративных автоматизированных информационных систем рассматриваются информационные системы персональных данных с мультиоблачной архитектурой.

Различным аспектам решения задач оценки эффективности использования ресурсов информационных систем и управления информационными рисками, возникающими при автоматизированной обработке данных в информационных системах, посвящены работы многих российских и зарубежных ученых.

Задачи эффективного использования ресурсов и оценки качества обработки информации в корпоративных ИС и информационно-телекоммуникационных сетях решались в работах советских и российских исследователей (Башарин Г.П., Вишневский В.М., Гайдамака Ю.В., Гольдштейн Б.С., Гребешков А.Ю., Докучаев В.А., Ефимушкин В.А., Казанский Н.А., Курносова Н.И., Кучерявый А.Е., Лазарев В.Г., Лазарев Ю.В., Ледовских Т.В., Мархай Е.В., Метельский Г.Б., Назаров А.А., Наумов В.А., Нейман В.И., Печинкин А.В., Пшеничников А.П., Рогинский В.Н., Ромашкова О.Н., Росляков А.В., Рыкова Т.В., Саксонов Е.А., Самуйлов К.Е., Соколов Н.А., Степанов С.Н., Харкевич А.Д., Цитович И.И., Шнепс-Шнеппе М.А. и др.) [7,8,9,13,18,21,22,24,38,42,60,73,74,77,86,87,89,104-107,111,116,119,128,144, 150, 226,228,230], а также зарубежных исследователей (Дудин А.Н., Bohge M., Capozzi F., Erlang A.K., L. R. Ford Jr., Fulkerson D. R., Iversen B., Kelly F.P., Kleinrock L., Kobayashi H., Palm C., Poisson S.D., Rappaport S., Wang L., Wu D. и др.) [68,69,155,159,197,199,200,234].

Обсуждению и анализу вопросов управления рисками в современных ИСПДн и безопасной обработки персональных данных посвящены публикации российских и зарубежных учёных (Голованова Е.Н., Докучаев В.А., Емельянников М.Ю., Мунтян А.В., Саксонов Е.А., Статьев В.Ю., Шередин Р.В., Шинаков К.Е., Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey, Majid Mollaeefar, Silvio Ranise, Raphaël Gellert, Jakub Breier, Hude Ladislav, F. Kunz and Z. Á. Mann, D. B. Rawat, R. Doku, M. Garuba, C. b. Manjunath Reddy, U. k. reddy, E. Brumancia, R. M. Gomathi, K. Indira, H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao and C. Cheng и др.) [2,23,41,44,47,54,57,85,109,125,140,141,142,143,156,158, 160,166,172,173,182,184,186,195,203,205,206,214,229].

Однако в работах этих авторов не получили достаточного отражения теоретические и практические вопросы разработки алгоритмов, реализующих методы массового обслуживания в дискретном времени, позволяющие провести анализ использования ресурсов ИСПДн, а также вопросы организации безопасной работы с персональными данными в корпоративных информационных системах с мультиоблачной архитектурой в условиях априорных рисков нарушения целостности, конфиденциальности и доступности персональных данных. Вышесказанное обусловливает научную актуальность настоящего исследования, посвящённого разработке и развитию моделей и алгоритмов для обеспечения качества обработки ПДн в автоматизированных ИС.

Объектом исследования в диссертационной работе являются корпоративные автоматизированные ИС территориально распределённых коммерческих и некоммерческих организаций, предназначенные для обработки ПДн, их ресурсы и информационные процессы при автоматизированной обработке ПДн.

Предметом исследования в диссертационной работе являются модели и алгоритмы оценки информационных процессов и ресурсов корпоративных автоматизированных информационных систем персональных данных с мультиоблачной архитектурой.

Целью диссертационного исследования является повышение качества автоматизированной обработки ПДн в ИСПДн с мультиоблачной архитектурой путём оценки эффективности использования ресурсов системы и снижения возникающих при обработке информационных рисков персональных данных с помощью соответствующих моделей и алгоритмов.

Задачи диссертационной работы:

1. Разработка единого системного подхода к организации безопасной обработки ПДн в ИСПДн.

2. Разработка сценариев информационных процессов обслуживания запросов на обработку ПДн в ИСПДн с последующей формализацией задачи оценки эффективности использования ресурсов ИСПДн с мультиоблачной архитектурой.

3. Разработка модели и алгоритма оценки эффективности использования ресурсов ИСПДн при обработке ПДн с учётом её мультиоблачной архитектуры.

4. Разработка модели и алгоритма оценки рисков нарушения качества ПДн при их обработке в ИСПДн с мультиоблачной архитектурой.

Методы исследования. В диссертационной работе для решения задач были применены основные положения теории графов, теории вероятности, теории массового обслуживания и теории управления рисками в информационных системах.

Научная новизна работы заключается в разработке моделей и алгоритмов, направленных на повышение качества процессов автоматизированной обработки персональных данных в корпоративных ИСПДн с мультиоблачной архитектурой.

В результате выполнения диссертационной работы были получены следующие научные результаты:

1. Единый системный подход к организации безопасной обработки персональных данных в ИСПДн за счёт унификации информационных процессов, что, *в отличии от существующих* подходов, *позволяет* в дальнейшем разработать адекватную подсистему обеспечения качества этих процессов с целью выполнения требований нормативных правовых актов, эффективного использования ресурсов

ИСПДн при обработке персональных данных и минимизации рисков нарушения качества ПДн (2.3.8, п.6).

2. Представление информационных процессов обслуживания разного типа запросов на обработку ПДн в ИСПДн в форме сценариев *позволяет* для построения и исследования модели функционирования ИСПДн с мультиоблачной архитектурой использовать графо-матричные модели процессов обработки запросов к ПДн в ИСПДн и анализ систем массового обслуживания в дискретном времени (2.3.8, п.1).

3. Модель оценки эффективности использования ресурсов ИСПДн с мультиоблачной архитектурой при автоматизированной обработке персональных данных, учитывающая, *в отличии от известных моделей*, обработку разного типа запросов к персональным данным на основе сценариев и дискретный характер подобных запросов. Разработанный алгоритм решения системы уравнений равновесия для расчёта основных вероятностно-временных характеристик функционирования ИСПДн *позволяет* снизить трудоёмкость вычислительного процесса (2.3.8, п.1).

4. Модель оценки рисков нарушения качества ПДн, учитывающая, *в отличии от существующих*: особенности и условия функционирования корпоративной ИСПДн с мультиоблачной архитектурой при обработке разных категорий ПДн; такие свойства ИСПДн, как масштабируемость, гибкость, расширяемость; требования организации к допустимости рисков, и *позволяющая* представить задачу оценки допустимости рисков ПДн в виде оптимизационной задачи. Предложенная модель позволяет определить наиболее приоритетные направления минимизации рисков с целью усовершенствования информационных процессов обработки ПДн. Разработанный алгоритм *позволяет* решить поставленную оптимизационную минимаксную задачу как задачу линейного программирования (2.3.8, п.1).

Теоретическая и практическая значимость работы.

Теоретическая значимость работы заключается в применении системы массового обслуживания в дискретном времени, позволяющей провести анализ

эффективности использования ресурсов ИСПДн, и описания проблемной области оценки информационных рисков ПДн в виде семантической модели, позволяющей перейти к решению оптимизационной задачи линейного программирования, ориентированной на использование вычислительной техники.

Практическая значимость заключается в том, что разработанные модели и алгоритмы могут быть использованы в организациях, занимающихся обработкой ПДн, при проектировании и эксплуатации корпоративных ИСПДн с мультиоблачной архитектурой, а также при построении подсистемы обеспечения безопасных информационных процессов обработки ПДн в соответствии с требованиями нормативных правовых актов, бизнес- и технологических процессов и инфраструктуры ИСПДн.

Разработаны программные приложения для:

− анализа показателей эффективности использования ресурсов ИСПДн;

− оценки и минимизации информационных рисков при автоматизированной обработке ПДн в ИСПДн с мультиоблачной архитектурой.

Соответствие паспорту научной специальности. Область исследования и содержание диссертации соответствуют паспорту специальности 2.3.8. «Информатика и информационные процессы» (технические науки) в части:

- п.1 «Разработка компьютерных методов и моделей описания, оценки и оптимизации информационных процессов и ресурсов, а также средств анализа и выявления закономерностей на основе обмена информацией пользователями и возможностей используемого программно-аппаратного обеспечения»;
- п.6 в части «Обеспечение информационных систем и процессов, применения информационных технологий и систем в принятии решений на различных уровнях управления».

Степень достоверности результатов исследования подтверждается: корректным использованием современного математического аппарата; достаточно широкой апробацией результатов, подтверждением адекватности моделей численными экспериментами на базе исследования использования ресурсов ИС

при работе с ПДн, потенциальных рисков, возникающих при обработке ПДн в ИСПДн российских организаций с учётом мультиоблачной архитектуры.

Апробация научных результатов. Основные положения и отдельные результаты диссертации докладывались и обсуждались на международных и всероссийских конференциях: XV, XVI и XVII Международных научно-практических конференциях «Актуальные проблемы и перспективы развития экономики» (Гурзуф, 2016-2018 гг.), XI - XIV Международных отраслевых научно-технических конференциях «Технологии информационного общества» (Москва, 2017-2025гг.), Международной научно-технической конференции «Телекоммуникационные и вычислительные системы-2018» (Москва, 2018г.), XVIII и XXI Международной научно-технической конференции «Проблемы техники и технологий телекоммуникаций» (Казань, 2017 г., 2019 г.), XV и XX Международной научно-практической конференции «Теория и практика экономики и предпринимательства» (Симферополь-Гурзуф, 2018 г., 2023 г.), XXVIII Международный Форум МАС' 2024. ЦИФРОВАЯ ТРАНСФОРМАЦИЯ. СВЯЗЬ БУДУЩЕГО (Москва, 2024г.), Международных научных конференциях «SYSTEMS OF SIGNALS GENERATING AND PROCESSING IN THE FIELD OF ON BOARD COMMUNICATIONS» (Москва, 2018-2020 гг.), Международных конференциях «International Conference on Engineering Management of Communication and Technology, EMCTECH – Proceedings» (Вена, 2020-2023 гг.).

Положения, выносимые на защиту.

1. Единый системный подход к организации процессов автоматизированной обработки персональных данных в ИСПДн, унифицирующий информационные процессы, что даёт возможность разработать подсистему обеспечения качества этих процессов, учитывающую особенности архитектуры ИСПДн и требования нормативных правовых актов к автоматизированной обработке запросов к ПДн.

2. Сценарии обработки разного типа запросов к ПДн, позволяющие построить граф переходов между макросостояниями процесса обработки запроса, что в дальнейшем для формализации задачи оценки эффективности использования

ресурсов ИСПДн с мультиоблачной архитектурой даёт возможность представить рассматриваемый процесс в виде системы массового обслуживания конечной ёмкости в дискретном времени с ординарным неоднородным поступающим потоком заявок, с распределением длительности обслуживания фазового типа в дискретном времени.

3. Модель функционирования ИСПДн с мультиоблачной архитектурой при обслуживании запросов к ПДн, позволяющая учитывать сценарии обработки разного типа запросов к ПДн и найти стационарное распределение вероятностей. Алгоритм решения системы уравнений равновесия для расчёта основных вероятностно-временных характеристик функционирования ИСПДн для оценки эффективности использования ресурсов, снижающий трудоёмкость вычислительного процесса.

4. Модель оценки рисков нарушения качества ПДн при их обработке в корпоративной ИСПДн с мультиоблачной архитектурой, учитывающая особенности и условия функционирования ИСПДн, а также ограничения допустимости рисков, что позволяет обеспечить гибкость процесса оценки рисков ПДн и разработать алгоритм решения задачи по минимизации рисков ПДн как минимаксной оптимизационной задачи. Алгоритм решения задачи, позволяющий свести многокритериальную задачу минимизации рисков нарушения качества ПДн к решению задачи линейного программирования.

Внедрение результатов диссертации.

Результаты диссертационного исследования были использованы при организации бизнес-процессов, связанных с обработкой и хранением ПДн, в ОАО «РЖД» – при разработке технических заданий на создание и модернизацию ИСПДн и в программах повышения квалификации работников, в ООО «ТрастВерс» – для оценки эффективности использования ресурсов ИСПДн и выявления наиболее критичных рисков ПДн, а также в учебном процессе МТУСИ, о чём имеются соответствующие акты – 3 шт.

Разработанное программное обеспечение [114,115] передано в Федеральную службу по интеллектуальной собственности.

Публикации. Основные результаты диссертационного исследования опубликованы в 43 печатных работах, из них: 1 монография (в соавторстве) [45]; 9 учебных изданий; 9 статей, рецензируемых научных журналах, рекомендованных ВАК при Минобрнауки РФ для публикации основных результатов диссертационных исследований [1,40,52,53,55,79,125,170,183]; 7 статей в изданиях, входящих в международную реферативную базу данных и систему цитирования Scopus и Web of Science [149,169,171,172,174,203,206]; 16 – в рецензируемых материалах и трудах всероссийских и международных конференций [5,23,41,43,44,47,48,49,50,51,54,67,91,92,97,117]; 2 свидетельства о государственной регистрации программы для ЭВМ [114,115].

Личный вклад: результаты диссертационной работы получены автором самостоятельно, математические процедуры и программные средства разработаны при непосредственном участии автора.

Структура работы. Диссертация состоит из введения, четырёх глав, заключения, списка литературы из 234 наименований и 7 приложений. Основная часть изложена на 129 страницах машинописного текста, содержит 12 таблиц и 36 рисунков, общий объём диссертации 192 страницы.

Глава 1. Анализ основных информационных процессов обработки персональных данных в корпоративных автоматизированных информационных системах

1.1. Требования к организации информационных процессов обработки персональных данных в информационных системах

В Российской Федерации процедуры и информационные процессы, связанные с обработкой ПДн в ИС, регулируются требованиями Закона № 152-ФЗ [135]. Данные требования касаются всех этапов жизненного цикла ИСПДн (включая инфраструктуру данной системы). Кроме того, если бизнес-процессы компании имеют трансграничный характер, то при работе с ПДн необходимо соблюдать требования, изложенные в [63,71,102], и другие международные нормативные правовые документы, регулирующие правила обработки ПДн субъектов.

Вопросы «правомерности обработки ПДн, соответствия требованиям законодательных и иных нормативных правовых актов РФ, регламентов, нормативно-методических документов федеральных регуляторов и обеспечения безопасности ПДн должны решаться в обязательном порядке их операторами» [2]. Оператор ПДн – «государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн» [135]. Отметим, что «за оператором закреплена обязанность по защите ПДн, соблюдению точности и условий хранения, а также принятию мер по обеспечению качества их обработки в ИСПДн – конфиденциальности, целостности и доступности» [135].

Требования к безопасной работе с ПДн определяются Федеральной службой по техническому и экспортному контролю (ФСТЭК России) и Федеральной службой безопасности Российской Федерации (ФСБ России).

За несоблюдение и нарушение требований законодательства и нормативных документов, регламентирующих вопросы обработки и защиты ПДн, в РФ предусмотрена уголовная, административная, гражданско-правовая, дисциплинарная и материальная ответственность в соответствии с уголовным (ст. 137, ст. 138, ст. 140, ст. 272 УК РФ), административным (ст. 5.39, ст. 13.11, ст. 13.14, ст. 17.13, ст. 19.4, ст. 19.4.1, ст. 19.5, ст. 19.7 КоАП РФ), трудовым (ст. 81, ст. 90, ст. 193, ст. 243 ТК РФ) и гражданским (ст. 24, ст. 151 ГК РФ) кодексами [37,70,131,132,135].

Реализация автоматизированной обработки персональных данных регулируется следующими основными нормативными правовыми документами:

1. Организационно-правовое направление:
   – Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [135];
   – Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [134];
   – Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [136];
   – постановление Правительства РФ от 1 ноября 2012 года № 1119, в котором утверждены требования к защите персональных данных при их обработке в ИСПДн [98].
2. Техническое направление:
   – приказ ФСТЭК России от 18 февраля 2013 года № 21, устанавливающий состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн [101];
   – документы ФСТЭК:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», содержащая единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в ИСПДн [6];
- «Методика оценки угроз безопасности информации», определяющая порядок и содержание работ по определению актуальных угроз безопасности персональных данных при их обработке в ИСПДн [81];

– приказ ФСБ России от 10 июля 2014 года № 378, определяющий состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием средств криптографической защиты информации [100].

На рисунке 1.1 представлена иерархия основных документов.

Согласно действующим нормативным правовым документам для соблюдения принципов и правил организации обработки и обеспечения качества ПДн оператору ПДн необходимо выполнить ряд обязательных правовых, организационных, технических мер и мероприятий, а также осуществлять внутренний контроль и (или) аудит соответствия обработки ПДн действующим федеральным законам и принятым в соответствии с ними нормативным правовым актам, локальным актам оператора и эффективной обработке ПДн с обеспечением их целостности, доступности и конфиденциальности. От «эффективности организации данных мер зависит величина рисков, связанных с нарушением качества автоматизированной обработки ПДн» [206], и ущерба оператору от реализации этих рисков [23,43]. В рамках настоящей диссертационной работы будут исследоваться риски, связанные с нарушением требований Закона № 152-ФЗ [135]. В дальнейшем предполагается, что требования других нормативных правовых актов и документов федеральных регуляторов априори выполняются оператором персональных данных.

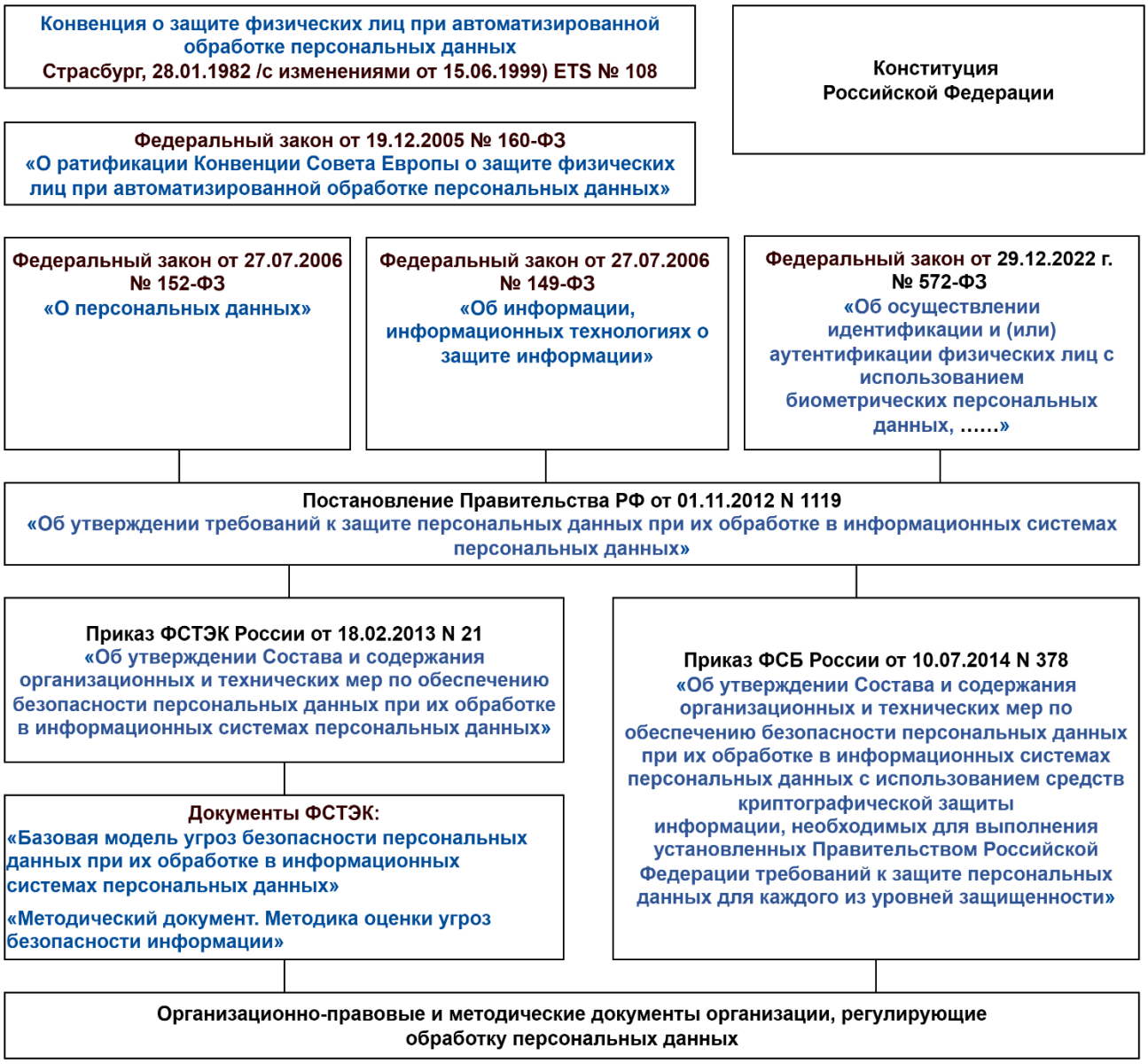


Рисунок 1.1 – Иерархия основных нормативных правовых актов, регулирующие автоматизированную обработку персональных данных

Определим понятие «*персональные данные*» как совокупность зафиксированных на физическом носителе сведений о субъекте персональных данных в форме, пригодной для их постоянного хранения, передачи и обработки.

Беря за основу [29], можно выделить следующие этапы жизненного цикла персональных данных при автоматизированной обработке:

I. *Сбор ПДн из первоначальных источников*. В качестве источников информации могут выступать пользователи информационной системы

персональных данных, другие взаимодействующие с ней системы, а также сама ИСПДн.

II. *Первичная обработка ПДн*: анализ и фильтрация поступающих ПДн, преобразование их во внутренний формат ИСПДн, а также их верификация.

III. *Передача ПДн*: процесс передачи данных от одного источника к другому по каналам связи.

IV. *Использование ПДн*: любая форма обработки ПДн, которая не включает «сбор», «передачу», «хранение», «архивирование» или «уничтожение».

V. *Хранение ПДн*: хранение ПДн с применением соответствующих мер защиты и механизмов для предотвращения несанкционированного доступа, модификации, уничтожения, удаления или иного несанкционированного использования.

VI. *Уничтожение ПДн*: завершающий этап жизненного цикла ПДн (их удаление или уничтожение).

Согласно действующим требованиям, «под *обработкой ПДн* будем понимать любое действие (операцию) или совокупность действий (операций) с ПДн за период их жизненного цикла, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн» [135].

Каждый этап жизненного цикла отличается отдельным набором инструментальных средств и технологий, используемых на нём, применение которых ориентировано на решение следующих основных проблем обработки большого количества персональных данных [92]:

- хранение (ограничения аппаратуры не позволяют хранить большие объёмы информации на одном носителе, поэтому необходимо применять распределённое хранение на нескольких носителях);
- обработка (чаще всего отдельные части информации слабо связаны между собой и их необходимо структурировать);

• анализ (так как основной целью информационных систем является предоставление переработанной информации пользователям, то необходимо наличие методов анализа больших объёмов информации для создания различных отчётов).

К таким средствам и технологиям можно отнести, например, протоколы и форматы обмена данными, инструменты обработки и анализа данных, а также хранилища данных и системы управления базами данных (СУБД) и т.п.

С учётом вышесказанного для обеспечения качества обрабатываемых ПДн в ИСПДн автором «предлагается представить жизненный цикл реализации оператором ПДн процедур их автоматизированной обработки в виде шести основных этапов, каждый их которых состоит из ряда процедур, реализуемым на соответствующем этапе» [43] (таблица 1.1).

Таблица 1.1 – Этапы жизненного цикла реализации процедур автоматизированной обработки персональных данных в информационных системах организации

Этап	**Содержание этапа**	**Процедуры этапа**
I. Создание модели безопасной обработки персональных данных	Разработка документального описания модели безопасной обработки	• Определение признаков обработки персональных данных; • Определение объекта защиты (архитектура, системы, процессы, состав персональных данных); • Определение целевых характеристик обеспечения безопасности персональных данных; • Оценка рисков персональных данных; • Разработка модели нарушителя; • Разработка модели угроз; • Определение (классификация ИСПДн) требуемого уровня защищённости персональных данных; • Разработка технических требований по реализации защиты персональных данных.

Продолжение таблицы 1.1

Этап	Содержание этапа	Процедуры этапа
II. Реализация функций безопасной обработки персональных данных	Определение состава и содержания организационных и технических мер по обеспечению безопасной обработки персональных данных	• Идентификация и аутентификация; • Управление доступом; • Ограничение программной среды; • Защита машинных носителей; • Регистрация событий безопасности; • Антивирусная защита; • Обнаружение вторжений; • Контроль защищённости персональных данных; • Обеспечение целостности; • Обеспечение доступности; • Защита среды виртуализации; • Защита технических средств; • Защита ИСПДн; • Выявление инцидентов; • Управление конфигурацией.
III. Проведение специальных работ	Исследования и проверки в интересах ИСПДн	• Тематические исследования программного обеспечения (при необходимости); • Проведение спецпроверок и специсследований (при необходимости); • Оценка соответствия (аттестационные испытания) заявленному уровню защищённости персональных данных.
IV. Подготовка ИСПДн к вводу в эксплуатацию	Реализация функций защиты на объектах ИСПДн	• Инженерно-техническая защита объекта информатизации (при необходимости); • Защита технических каналов утечки персональных данных (при необходимости).

Продолжение таблицы 1.1

Этап	Содержание этапа	Процедуры этапа
V. Обеспечение эксплуатации ИСПДн	Организация эксплуатации ИСПДн	• Положение о режиме защиты персональных данных; • Должностные инструкции (ответственных и уполномоченных); • Конструкторская и эксплуатационная документация; • Аттестат (заключение) соответствия; • Управление эксплуатацией ИСПДн; • Обучение специалистов; • Аудит (внутренний контроль) режима защиты персональных данных; • Актуализация нормативной базы.
VI. Вывод из эксплуатации и утилизация отдельных элементов или ИСПДн в целом	Организация вывода из эксплуатации и утилизации отдельных элементов или ИСПДн в целом	• Вывод из эксплуатации отдельных элементов или ИСПДн в целом; • Утилизация персональных данных и связанных с ними материалов (электронных носителей информации, ключей шифрования и т.п.) в соответствии с разработанными на предыдущих этапах документах.

Результатом реализации всех этапов и процедур жизненного цикла автоматизированной обработки персональных данных должна стать разработанная адекватная подсистема обеспечения безопасных информационных процессов обработки персональных данных как совокупность правовых, организационных и технических мер, реализуемых с целью выполнения требований нормативных правовых актов, эффективного использования ресурсов ИСПДн при обработке ПДн и минимизации рисков нарушения качества ПДн.

При разработке процедур, обеспечивающих реализацию «жизненного цикла автоматизированной обработки ПДн, необходимо руководствоваться

требованиями по организации обработки и обеспечению качества ПДн и учитывать риски, которые могут возникнуть на любом из этапов жизненного цикла» [43].

Так как в процессе цифровой трансформации организаций широко используются облачная инфраструктура и средства виртуализации, эти ресурсы также необходимо включать в разрабатываемую подсистему безопасной обработки персональных данных. Более подробно обобщённая схема организационной иерархической структуры территориально распределенной корпоративной ИСПДн с облачной архитектурой рассмотрена в разделе 2.1.

1.2. Анализ состава ресурсов информационной системы для обработки запросов к персональным данным

Одним из основных принципов, реализуемых в процессе использования современных информационно-коммуникационных технологий (ИКТ) при работе с ПДн, выступает принцип системной целостности. Он предполагает, что услуги, предоставляемые ИСПДн с определенным уровнем качества, не приводят к нежелательным для их потребителя последствиям в процессе сбора, обработки, хранения информации и выработки на ее основе требуемого решения [1,183]. Данные требования предъявляются к таким характеристикам качества персональных данных, как целостность, доступность, конфиденциальность, достоверность, точность и полнота, полезность и своевременность получения. Актуальность этого принципа возрастает по мере развития цифровых информационных технологий, в рамках которых происходит выделение информационных процессов порождения информации, её отображения, хранения и обработки в отдельное производство, независимое от остальных процессов. Это относится к распределённым базам ПДн, распределённой обработке ПДн, GRID-технологиям, SOA-архитектурам и «облачным» вычислениям, предоставляющих удобный сетевой доступ к конфигурируемым ресурсам обработки и хранения ПДн (сети, серверы, системы хранения данных (СХД), приложения и сервисы и т.п.) [54].

Современные ИС, внедряемые в ходе цифровой трансформации предприятий и работающие с персональными данными клиентов, работников и партнёров предприятия, представляют собой сложный организационно-технический комплекс, включающий в себя информационные системы (под которыми у нас в стране, как правило, понимается программное обеспечение (ПО) типа CRM или ERP), автоматизированные информационные системы для управления бизнес- и технологическими процессами предприятия, а также информационно-телекоммуникационные сети (инфраструктуру), обеспечивающие передачу персональных данных между ИСПДн, подсистемами ИСПДн, зарегистрированными устройствами работников организации и т.п., а также обеспечивающие выход на сети общего пользования. Другими словами, ИСПДн современного предприятия – это множество взаимосвязанных элементов (компоненты системы и информационные ресурсы/активы), реализующих получение, «обработку, хранение и передачу необходимых ПДн в целях эффективного функционирования предприятия» [53].

Как физическая система, ИСПДн представляет собой совокупность аппаратного и программного обеспечения обработки и хранения ПДн; программных средств (систем виртуализации, СУБД и т.д.); информационных технологий; телекоммуникационного оборудования и ПО для управления этим оборудованием; материальных носителей информации; средств защиты информации и других систем и оборудования, обеспечивающих функционирование ИСПДн для обслуживания запросов на обработку ПДн.

Основными элементами (ресурсы/активы ИСПДн) «программно-аппаратного обеспечения ИСПДн являются:

- ПДн, содержащиеся в базах данных, как совокупность информации и её источников, используемых в ИСПДн;
- справочная информация, включающая справочники, нормативные правовые акты, методические указания и т.п.;
- данные, содержащиеся в системе или сети, а также закрытые данные о конфигурации сетей, систем, данные телеметрии и т.д.;

- информационные технологии, как совокупность методов и способов использования компьютерных технологий при обработке ПДн;
- аппаратное обеспечение обработки и хранения ПДн: серверное оборудование, СХД, автоматизированные рабочие места (АРМ – стационарные и мобильные), технологическое оборудование и т.д.;
- программное обеспечение обработки и хранения ПДн;
- программные средства (в т.ч. системы виртуализации, системы управления базами данных и т.д.);
- телекоммуникационное оборудование и различное ПО, выполняющее функции управления таковым оборудованием;
- материальные носители информации;
- средства защиты информации;
- дополнительное оборудование;
- пользователи ИСПДн и интерфейсы взаимодействия с ними;
- системы, обеспечивающие функционирование ИСПДн (источники бесперебойного питания (ИБП), климатическое оборудование и т.п.)» [16,49,81,169].

Возможность нарушения качества ПДн в результате уязвимостей каналов связи, по которым передаются ПДн, должна учитываться при оценке информационных рисков ПДн.

Перечисленные ресурсы (активы) корпоративной ИСПДн являются элементами (элементы воздействия), на которые возможно как внутреннее, так и внешнее воздействия, что может привести к нарушению эффективности использования ресурсов ИСПДн и качества обрабатываемых в ИСПДн персональных данных. Согласно [81] основными видами воздействий являются:

а) отказ в обслуживании элементов (нарушение доступности);
б) утечка (перехват) конфиденциальной информации, в т.ч. ПДн (нарушение конфиденциальности);
в) несанкционированный доступ к элементам, защищаемым ПДн, системным, конфигурационным, иным служебным данным;

г) несанкционированная модификация, подмена, искажение защищаемых ПДн, системных, конфигурационных, иных служебных данных (нарушение целостности);

д) несанкционированное использование вычислительных ресурсов в интересах решения несвойственных им задач;

е) нарушение функционирования (работоспособности) программных и аппаратных средств обработки, передачи и хранения ПДн.

Совокупностью элементов ИСПДн и их интерфейсов определяют границы процесса оценки эффективности использования ресурсов системы и рисков нарушения качества персональных данных [81]. Исследование архитектуры корпоративной ИСПДн, особенно с облачной архитектурой, необходимо для оценки её влияния на эффективность использования ресурсов ИСПДн и качество обработки ПДн.

Нормативные правовые требования на обработку различных категорий ПДн также оказывают влияние на архитектуру ИСПДн. Действующее законодательство РФ предусматривает «четыре категории обрабатываемых ПДн» [98]:

1) общедоступные ПДн;
2) специальные категории ПДн;
3) биометрические ПДн;
4) иные категории ПДн.

Кроме перечисленного, чтобы учесть особенности архитектуры облачной ИСПДн, предлагается категорировать ПДн по критерию взаимоотношения субъекта ПДн и оператора ПДн и выделить следующие их категории (рисунок 1.2):

1) ПДн работников оператора, т.е. лиц, связанных с оператором трудовыми взаимоотношениями;

2) ПДн субъектов, не являющихся работниками оператора, т.е. лиц, которые не являются штатными или внештатными сотрудниками оператора (клиенты, контрагенты, акционеры, пенсионеры, соискатели вакантных рабочих мест и т.д.).

Рисунок 1.2 – Категории персональных данных по различным критериям

Определение категорий обрабатываемых персональных данных и ресурсов программно-аппаратного обеспечения ИСПДн, предназначенных для работы с персональными данными, позволяет выявить и оценить использование ресурсов системы и основные риски нарушения качества обрабатываемых персональных данных в связи с реализацией в ИСПДн неприемлемых для организации событий, способных оказать влияние на качество ПДн и нести за собой негативные последствия как для оператора ПДн, так и для субъекта. Полученные результаты используются для «комплекса мер, направленных на обеспечение качества ПДн, обрабатываемых в ИСПДн, в зависимости от их категорий и соответствующих нормативно-правовых требований» [6,49,81,98,100,101,206].

В связи с выше изложенным для обеспечения эффективного использования ресурсов ИСПДн и качественной автоматизированной обработки персональных данных необходимо решить две задачи: провести оценку эффективности использования ресурсов ИСПДн и оценку рисков нарушения качества обрабатываемых персональных данных с целью минимизации этих рисков и их негативных последствий.

1.3. Общая постановка задачи оценки эффективности использования ресурсов информационной системы при обработке персональных данных

Эффективное использование ресурсов информационной системы является важным фактором для обеспечения ее стабильной и надежной работы, качества обрабатываемых в ней персональных данных, а также для снижения капитальных вложений и эксплуатационных затрат.

Под оценкой эффективности использования ресурсов информационной системы будем понимать процесс анализа того, насколько рационально и результативно используются ресурсы системы для достижения поставленных целей. В общем случае оценка включает в себя как качественные, так и количественные показатели, такие как производительность, надежность, масштабируемость, экономическая эффективность и качество обслуживания. Под эффективностью использования ресурсов в настоящей диссертации будем понимать такие показатели функционирования ИСПДн, как: способность системы справляться с нагрузкой, время обработки заявок, эффективность загрузки системы.

Оценка эффективности использования ресурсов информационной системы производится с помощью методов, направленных на выявление степени полезности и рациональности расходования ресурсов, включая аппаратные средства, программное обеспечение, данные и человеческие ресурсы (основные ресурсы ИСПДн рассмотрены в разделе 1.2). Выбор метода зависит от целей анализа, особенностей системы и приоритетов организации. Важно использовать комбинацию различных подходов, чтобы получить всестороннюю оценку эффективности информационной системы. К ключевым методам оценки относят количественные методы (например, для расчёта метрик и показателей производительности и надёжности ИСПДн), качественные (например, экспертная оценка, SWOT-анализ) и комбинированные методы. Среди количественных методов выделим методы моделирования, которые позволяют с помощью рассчитанных вероятностно-временных характеристик оценить поведение

информационной системы при различных условиях и оценить эффективность как всей системы, так и отдельных её элементов.

Эффективная оценка ресурсов информационной системы позволяет не только снизить затраты, но и повысить надежность системы, удовлетворенность пользователей и соответствие бизнес-целям.

Согласно специфике деятельности многих организаций используемые ими информационные системы персональных данных, которые хранят и обрабатывают персональные данные различных категорий и разного объёма, будут относиться к классу территориально распределённых систем с облачной архитектурой. Под такими ИСПДн будем понимать системы, которые: в интерактивном режиме обслуживают большое и постоянно растущее количество пользователей, которые одновременно генерируют большое количество запросов на обработку персональных данных; обрабатывают большие и, возможно, неструктурированные объёмы данных; построены на разнородном оборудовании, когда некоторые или все сетевые возможности и ресурсы организации размещаются на внешней или частной облачной платформе.

ИСПДн с облачной архитектурой может быть отнесена к классу больших систем по следующим признакам:

− многоуровневое управление – управление многоуровневой инфраструктурой (линии связи, узлы сетевой инфраструктуры, вычислительные и программные ресурсы и т.д.); управление процессами ИСПДн; управление организацией процессов функционирования ИСПДн для достижения целей её создания;

− на каждом уровне управления оценка функционирования системы производится одновременно по нескольким критериям (отказоустойчивость, надежность, производительность, стоимость, качество и т.д.);

− в процессе развития ИСПДн организационная структура постоянно меняется;

− обслуживание рассматриваемой ИСПДн производится людьми, которые часто находятся в ситуации неопределенности;

− вследствие сложности рассматриваемой системы формализация всех технологических процедур и операций на всех уровнях в полном объёме практически невозможна.

Рассматриваемую ИСПДн как сложную систему отличают следующие свойства.

1. Взаимодействие с окружающей средой проявляется не только в непосредственном воздействии окружающей среды на систему, но, в большей степени, во влиянии пользователя на функционирование системы и наоборот. Качество работы ИСПДн зависит от числа запросов, поступающих от пользователей на действия, связанные с персональными данными, а качество её функционирования влияет на поведение пользователей.

2. Стохастичность поведения рассматриваемой ИСПДн обусловлена тем, что запросы, поступающие на ИСПДн от пользователей, являются случайными.

3. Иерархичность структуры ИСПДн заключается в том, что в ней можно выделить отдельные подсистемы, которые находятся в соподчиненности в соответствии с занимаемыми уровнями. Например, по функциональному признаку в рассматриваемой системе выделяются следующие подсистемы технических средств: для хранения, передачи, защиты данных, управления системой, технической эксплуатации ИСПДн и т.д.

4. Рассматриваемая ИСПДн является непрерывно развивающейся системой: растёт количество пользователей, появляются новые категории обрабатываемых персональных данных, увеличивается объём хранимых и обрабатываемых данных, появляются и внедряются новые ИКТ, т.е. происходят количественные изменения, которые накапливаясь, могут приводить к качественным изменениям. На определенном уровне сложности системы начинают проявляться новые, системные закономерности [82]. Поэтому в большой системе нельзя ограничиваться изучением лишь её элементов, а необходим анализ системы в целом.

На рисунке 1.3 представлена обобщённая структурная схема организации ИСПДн с облачной архитектурой как сложной системы.

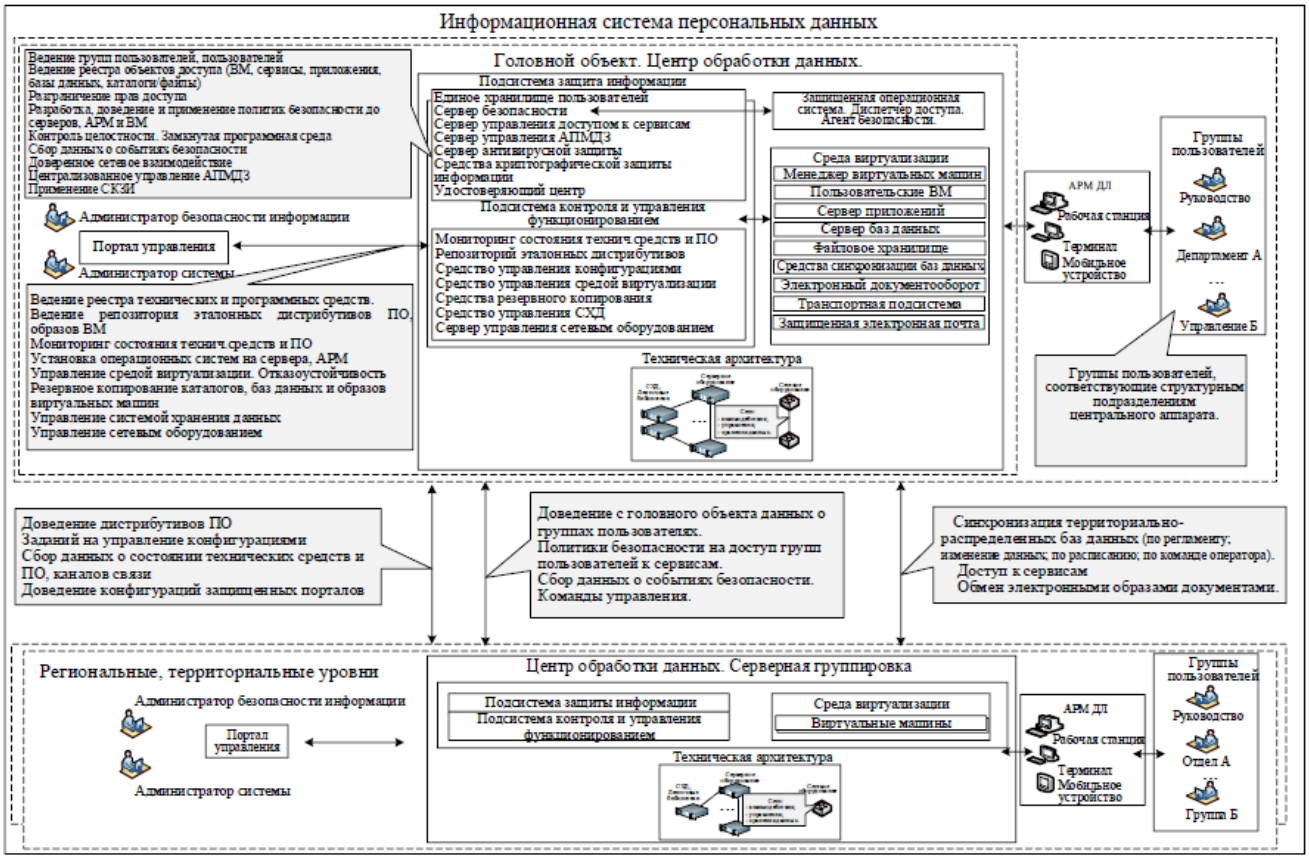


Рисунок 1.3 – Обобщённая структурная схема организации ИСПДн с облачной архитектурой как сложной системы

Выделим ключевые свойства таких ИСПДн [16,49,92,169]:

- многоуровневая иерархическая или сетевая структура;
- единая инфокоммуникационная инфраструктура;
- единая среда виртуализации, отвечающая требованиям по качеству обслуживания;
- единое информационное пространство, отвечающее требованиям по качеству обслуживания;
- распределенные информационные ресурсы;
- сквозная аутентификация и идентификация пользователей.

Исходя из вышеперечисленных особенностей и ключевых свойств, к подобным ИСПДн предъявляется ряд требований, выполнение которых связано с решением различных технических проблем в процессе разработки и поддержки её функционирования [92]. Выделим основные из них:

- обладание достаточным количеством вычислительных ресурсов;
- интерактивность и высокая производительность;
- эффективное хранение и обработка большого объёма ПДн;
- доверенный доступ пользователей к сервисам и ПДн;
- отказоустойчивость.

Чтобы справляться с высокими нагрузками, ИСПДн должна иметь в своём распоряжении достаточное количество вычислительных ресурсов, таких как процессорное время, объём оперативной памяти и дискового пространства и т.д.

Работа системы в интерактивном режиме и необходимость обслуживания большого количества пользователей (например, в ОАО «РЖД» численность работников, занимающихся обработкой персональных данных, составляет порядка 100 тыс. человек) и обработка большого количества персональных данных (до 500 млн. учётных записей повседневно) подразумевают, что она должна обладать свойством интерактивности. То есть процесс обработки пользовательских запросов должен занимать как можно меньше времени. Кроме того, не должны превышаться обозначенные в процессе проектирования системы допустимые лимиты по времени её отклика, времени выполнения запроса и использованию аппаратных ресурсов, то есть ИСПДн должна быть высокопроизводительной. Для примера, количество работников: в ОАО «РЖД» – более 700 тыс. человек; в ПАО «Газпром» – порядка 500 тыс. человек, в ОАО «Аэрофлот» – порядка 17,7 тыс. человек и т.д. Это цифры только по одной категории хранимых персональных данных – работники оператора персональных данных без учёта других категорий персональных данных субъектов.

Под эффективностью хранения и обработки данных понимается соблюдение допустимых лимитов по вычислительным ресурсам и времени, требуемых для данных информационных процессов, а также обеспечение качества данных.

Доверенный доступ пользователей к сервисам и данным зависит от процесса распознавания воздействия на обработку персональных данных в информационной системе и определяется как возможность описания реализации этого процесса

(более подробно рассмотрено в разделе 1.4). Главным результатом данного процесса является возможность предположить его поведение в дальнейшем.

Под отказоустойчивостью облачной архитектуры подразумевается стабильная работа ИСПДн в течение долгого периода времени. Как правило, информационные системы должны обеспечивать бесперебойную работу в режиме 24x7x365 и продолжать стабильно функционировать даже при частичном выходе из строя аппаратной или программной части ИСПДн, то перерыв в работе таких систем может нанести организации огромные финансовые убытки. То есть, по сути, отказоустойчивость ИСПДн – это её способность сохранять работоспособность и обеспечивать качество персональных данных (конфиденциальность, целостность, доступность) при отказе некоторых компонентов ИСПДн.

Реализация отказоустойчивости ИСПДн обеспечивается с помощью наблюдаемости и управляемости [146]. Там же [146] показано, что отказоустойчивость распределённых информационных систем, к которым относятся и современные ИСПДн, значительно выше, чем у централизованных. Кроме того, очевидно, что использование мультиоблачной архитектуры (рассмотрена в последующих разделах настоящей работы) даёт возможность использования в информационных системах сервисных возможностей разных поставщиков облачных услуг, что делает предлагаемую архитектуру ИСПДн крайне перспективной. Численное доказательство этого требует дополнительных исследований, выходящих за рамки данной работы. Отметим, что при использовании такой архитектуры за счёт усложнения процесса обработки персональных данных в ИСПДн повышаются и информационные риски.

Для отслеживания процесса обработки запросов к ПДн в ИСПДн и решения задачи оценки эффективности использования ресурсов ИСПДн целесообразно применять методы моделирования и использовать для представления функционирования ИСПДн систему массового обслуживания (СМО).

Существует большое число моделей оценки эффективности ресурсов ИС. Разработка соответствующих алгоритмов их исследования связана со сложностью их анализа и разнообразием ситуаций их использования.

Анализируя текущее состояние проблемы оценки характеристик использования ресурсов ИСПДн, отметим, что в работах теоретического плана решаются задачи стандартной техники, развитой в теории массового обслуживания. При этом не учитывались особенности, присущие современным ИСПДн: мультиоблачная архитектура ИСПДн, технология взаимодействия отдельных облаков друг с другом при обработке персональных данных, различные сценарии обработки персональных данных, их категории. Перечисленные особенности требуют разработки новых моделей, учитывающих особенности обработки персональных данных в подобных ИСПДн. При этом расчётные алгоритмы следует ориентировать на использование вычислительной техники.

Решение поставленной задачи и было выполнено в последующих главах диссертационной работы.

В [56,65,66,72,75,147,151,152,154,162,167,177-181,185,187,202,204,212,213, 231-233] предлагались приближенные алгоритмы расчета вероятностных характеристик моделей информационно-телекоммуникационных сетей и информационных систем. Одним из результатов, представляющих практический интерес, явилась модель «полнодоступной системы с пуассоновским входным потоком первичных вызовов и экспоненциально распределенным временем обслуживания» [162].

В работах [64,65] была решена проблема численного расчета модели, предложенной в [162]. Модели, предложенные в этих работах, объединяет блочная структура системы уравнений статистического равновесия [126,127,224,225]. В этих работах, а также в [16,110,145] рассмотрены системы с повторными вызовами. В работах [93,94] представлен обзор систем типа *M/G/*1 с групповым обслуживанием заявок, исследованы и уточнены методы анализа времени ожидания начала обслуживания в СМО с переменной и фиксированной длиной группы, найдены аналитические выражения для среднего значения и дисперсии. Полученные результаты ориентированы на решение конкретной разработки модели функционирования протокола управления потоковой передачей (Stream

Control Transmission Protocol, SCTP) и не могут быть непосредственно использованы для решения поставленной в настоящей диссертации задачи.

В [103] представлен обзор ресурсных систем массового обслуживания. Ценной особенностью предложенного метода является значительное упрощение анализа системы и при этом сохранение высокой точности оценки, а в отдельных случаях и отсутствие потери точности в принципе. Предлагаемый математический аппарат предназначен для случая пуассоновского входящего потока и экспоненциального времени обслуживания и не учитывает дискретный характер запросов на обработку персональных данных. Анализ методов исследования СМО для параллельной обработки данных проведен в [25]. Полученные в работе результаты должны учитываться при решении поставленной в настоящей диссертации задачи.

В [108,113] предлагается численный метод расчета вероятностей состояний для однолинейной СМО типа *M/G*/1 с «прогулками», который не учитывает указанные выше особенности мультиоблачной архитектуры.

Классификация моделей обслуживания клиентов в информационных системах, вопросы оценки качества данных в ИС, а также управление потоками данных в многосерверных ИС рассмотрены в работах [39,61,90,111,145] однако они также ориентированы на пуассоновские потоки.

Современные запросы к ПДн субъекта носят цифровой, дискретный характер, что приводит к необходимости исследования поставленной в настоящей диссертации задачи в дискретном времени. Развитие методов анализа СМО ограниченной ёмкости в дискретном времени, позволяющих учитывать как дискретный характер передаваемых данных, так и дискретный характер функционирования реальных ИС, является актуальным. Данной тематике посвящены работы советских, российских и зарубежных исследователей (Башарин Г.П., Боровков А.А., Бочаров П.П., Гайдамака Ю.В., Ефимушкин В.А., Касконе А., Ледовских Т.В., Манзо Р., Парасотченко Д.В., Печинкин А.В., Разумчик Р.В., Ремонтов А.П., Рыкова Т.В., Самуйлов К.Е., Таташев А.Г., Ушаков В.Г., Шоргин С.Я., Bruneel H., Daduna H., Kelly F.P., Kobayashi H., Takagi H., Wu D., и др.

[7,9,10,12,14,17,58,59,76,96,105,150,153,157,168,200,226,227,234]. Следует отметить, что работы, позволяющие провести анализ использования ресурсов ИСПДн в виде СМО сложной структуры в дискретном времени, практически отсутствуют. В работах [83,84,112] рассматривается модель облачных вычислений в виде системы массового обслуживания и предлагается метод расчета времени отклика системы облачных вычислений с несколькими поставщиками услуг, что является одним из первых исследований систем с упрощённой мультиоблачной архитектурой и непрерывным потоком запросов.

К числу одной из первых работ, посвящённых созданию математического аппарата для исследования характеристик «цифровых двойников», которые представляют собой субъект персональных данных физического или юридического объекта, следует отнести работу [60]. В работе рассмотрена модель централизованной информационной системы, которую необходимо развить в части учёта особенностей информационных процессов при обработке данных в ИСПДн с мультиоблачной архитектурой.

Далее для решения задачи оценки эффективности использования ресурсов ИСПДн при обслуживании запросов к ПДн представим ИСПДн в виде СМО с обслуживанием заявок в дискретном времени с ограничением по времени пребывания заявок в очереди. Этот интервал времени равен циклу обработки информации. Предлагаемый подход позволит выявить тенденции поведения ИСПДн с различными параметрами и дать оценку эффективности использования её элементов. Подобное моделирование необходимо для оценки оптимальности использования ресурсов и успешности выполнения задачи по обработке запросов, а также разработки рекомендаций по повышению эффективности использования элементов ИСПДн.

1.4. Общая постановка задачи оценки рисков нарушения качества персональных данных

Автоматизированная обработка персональных данных в ИСПДн сопряжена с определёнными информационными рисками. Информационный риск рассматривается как экономическая, имиджевая, репутационная и т.п. категория, требующая соответствующего уровня управления [5,43,46,52,62]. Реализация событий информационных рисков может привести к следующим последствия [91]:

а) возникновению рисков производственных, финансовых, репутационных или иных рисков для оператора персональных данных;

б) нарушению прав субъектов персональных данных;

в) возникновению ущерба в различных сферах деятельности государства, а также в области обеспечения обороны, безопасности государства и правопорядка.

Данные события определяются применительно к нарушению бизнес- и технологических процессов, выполнение которых обеспечивает ИСПДн, и применительно к нарушению безопасной обработки персональных данных, содержащихся в ИСПДн.

Постановка задачи распознавания воздействия на персональные данные производится в зависимости от уровня имеющейся предопределенной информации о воздействии. При наличии такой информации в достаточном объёме считается, что известна модель развития воздействия. Свойство распознаваемости воздействия по отношению к информационной системе определяется такими свойствами как наблюдаемость состояния процесса воздействия и управляемость процессом [122].

Задачу оценки рисков нарушения качества персональных данных можно представить в виде задачи определения потенциальных рисков персональных данных и минимизации их негативных последствий. Решение данной задачи применительно к ИСПДн с мультиоблачной архитектурой подробно рассмотрено в главе 4 настоящей диссертационной работы.

Присутствие в ИСПДн информационного риска напрямую связано с различными неопределённостями, которые сами по себе неоднородны. Под неопределённостью в данном случае следует понимать неполноту или неточность информации о процессах обработки персональных данных в ИСПДн, которые практически всегда находятся под влиянием внешней среды, поведение которой трудно предопределить с приемлемой точностью.

Любой риск обладает следующими характеристиками: «причина, условие, вероятность, последствия риска (положительные или отрицательные)» [206].

Главная задача процесса управления информационными рисками заключается «в нахождении и описании потенциальных рисков» [206]. Поэтому основными этапами процесса управления информационными рисками являются их идентификация, качественная и количественная оценка. На рисунке 1.4 показана предлагаемая обобщённая схема процесса управления рисками.

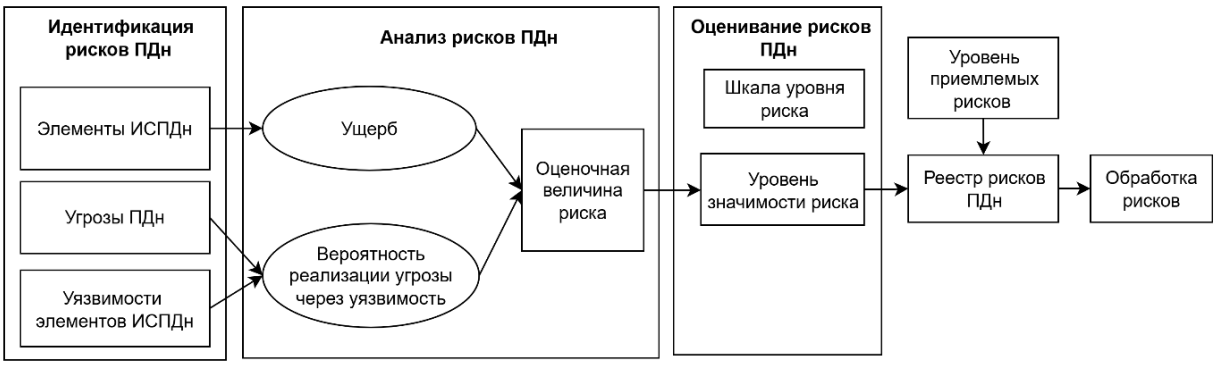


Рисунок 1.4 – Обобщенная схема процесса управления информационными рисками ПДн

Результатом этапа идентификации является составление реестра потенциальных рисков, которые могут возникнуть в ИСПДн, включающего также их причины и возможные последствия.

Выделим категории рисков, которые могут повлиять на ИСПДн:

- технологические риски (нарушение функционирования системы из-за сбоев аппаратных или программных средств; потеря данных; снижение

эффективности их обработки; потеря доступа к данным или нарушение их целостности и т.д.);

- риски информационной безопасности (нарушение функционирования системы из-за несанкционированного вмешательства в её работу и т.д.);
- политические риски (нарушение функционирования системы из-за отсутствия или несоблюдения законодательных норм и т.д.);
- риски, связанные с человеческим фактором (нарушение функционирования системы из-за человеческих ошибок и т.д.);
- инфраструктурные риски (нарушение функционирования системы из-за сбоев внешних информационных организационных структур и т.д.).

Риск нарушения качества персональных данных можно понимать как совокупность всех выделенных категорий рисков.

Оценка рисков может осуществляться количественными или качественными методами. Выбор того или иного подхода зависит от целей мероприятий по оценке рисков, объёма статистической информации, решаемых задач, а также квалификации специалистов, проводящих эту оценку.

В большинстве случаев проведение количественной оценки риска возможно только, если имеются накопленные статистические данные о функционировании ИСПДн. В реальных условиях такие данные либо недостаточны, либо отсутствуют, особенно, если необходимо провести оценку рисков для только вводимой в эксплуатацию информационной системы. В таких ситуациях используются качественные методы оценки, в основе которых лежат методы анализа, основанные на бальных оценках эксплуатации ИСПДн экспертами. Результатом данных методов могут также являться количественные характеристики.

Для оценки рисков количественными методами необходимо иметь статистическую информацию по показателям риска, нуждающихся в оценивании, либо непосредственно по показателям ущерба от риска и вероятности его наступления. Если такая информация имеется и её достаточно для того, чтобы произвести с требуемой точностью оценку риска, то для прогнозирования значений показателя риска применяются методы многомерного статистического анализа. В

случае, если статистической информации недостаточно, то можно использовать вероятностно-статистический или экспертно-статистический методы. В случае полного отсутствия статистических данных, расчет и оценка рисков производятся экспертными методами.

В настоящее время разработаны и в разной мере используются в процессе анализа и оценки информационных рисков ряд стандартов, методик и конкретных инструментов. Основные стандарты, рекомендованные международным сообществом в области управления рисками [161,164,165,175,176,188-194,209,210,215-218,220], позволяют применять обозначенные в них рекомендации при разработке модели оценивания рисков, а также при оценке эффективности её работы.

К наиболее значимым стандартам, имеющих отношение к исследуемой теме, следует отнести следующие российские стандарты [26,27,28,30-36], в которых определяются принципы и правила, применяемые при проведении анализа и оценки рисков, а также по управлению качеством данных.

Ключевые российские стандарты в области управления рисками позволяют учитывать особенности эксплуатации корпоративных информационных систем и аудита рисков в РФ при разработке модели их оценки.

Процесс управления рисками ПДн в ИСПДн состоит из их периодической оценки и выполнения мероприятий по снижению выявленных рисков до приемлемого уровня. В процессе анализа рисков производится совокупное оценивание функционирования ИСПДн с определением количественных (например, в форме денежных ресурсов) и качественных (например, уровни риска: высокий, средний, низкий) показателей риска.

В большинстве случаев для оценки риска используются методики, в основе которых лежит применение следующих величин [92]:

- вероятность угрозы;
- вероятность уязвимости;
- цена потери.

В общем случае риск можно рассчитывать с учётом двух факторов как произведение вероятности угрозы на цену потери [92]:

$$РИСК = (вероятность\ угрозы) * (цена\ потери). \quad (1.1)$$

Количественное оценивание риска, проводимое по формуле (1.1), в реальных условиях затруднено. Не всегда возможно с высокой степенью достоверности говорить о значениях вероятности реализации факторов угроз, ущерба и последствий для ИСПДн. В том случае, если статистические данные представляют собой ограниченные по объёму и времени выборки значений вероятности и ущерба либо прогнозные показатели, можно применять, как сказано выше, статистическую оценку рисков, которая производится на основе оценки или прогноза тяжести ущерба и частоты наступления случаев реализации угроз.

Также информационный риск можно рассчитывать следующим образом [92]:

$$РИСК = (вероятность\ угрозы) * (вероятность\ уязвимости) * (цена\ потери). \quad (1.2)$$

Выражение (1.2) представляет собой формулировку общей задачи в случае использования качественных шкал. Риск может выражаться не только произведением, но и сочетанием величин вероятности и ущерба. Одним из главных примеров метода оценки риска может являться матричный метод, с помощью которого показатели ущерба и частоты повторения угрозы ранжируются в виде матрицы. Ранжирование может производиться как качественным, так и количественным методом, когда значения ущерба и частоты характеризуются словесными описаниями. Каждый риск по каждой из опасностей заносится в одну из ячеек заранее сформированной матрицы, затем оценивается его допустимость или недопустимость в зависимости от его местоположения в матрице.

Проведённый анализ существующих методов и подходов оценки рисков нарушения качества персональных данных в ИСПДн [19,149] позволяет сделать следующие выводы:

1. Исходные данные большинства методологий опираются на экспертные оценки.

2. Качество проводимого процесса анализа рисков нарушения качества ПДн зависит от знания участниками процесса бизнес-модели организации, бизнес-процессов, в которых обрабатываются ПДн и технологических процессов их обработки.

3. Для проведения качественной оценки и анализа рисков нарушения качества ПДн необходимо применение системного подхода, недопускающего неполноту сведений о рисках.

4. Применяемый подход для оценки рисков нарушения качества персональных данных в ИСПДн должен давать возможность «кастомизировать» оценку рисков и быстро реагировать на изменяющиеся окружающие условия, а также учитывать новые и нестандартные угрозы и уязвимости, что, к сожалению, не позволяют делать рассмотренные методологии.

Цель оценки информационных рисков – определить характеристики рисков по отношению к информационной системе (ИСПДн) и её элементами (ресурсами). Результаты проведённой оценки используются для построения подсистемы обеспечения безопасной обработки персональных данных.

При оценке рисков учитываются следующие факторы:

- ценность элементов (ресурсов);
- значимость угроз и уязвимостей;
- эффективность существующих и планируемых контрмер (способов противодействия воздействиям на ИСПДн).

Предлагается в процесс оценки информационных рисков персональных данных включать следующие процедуры: определение ценности элементов (ресурсов) в виде персональных данных с учётом их категорирования, предложенного в разделе 1.2 настоящей работы; оценку угроз и уязвимостей; выбор адекватных контрмер и оценку их эффективности. Такой подход будет соответствовать общим рекомендациям, приведённым в [33]. При реализации угроз ожидаемый ущерб должен сравниваться с затратами на меры и средства защиты, а также штрафные санкции и другие прямые и косвенные затраты, на основании чего принимается решение относительно оцениваемого риска. Для

эффективного управления рисками необходимо выделять только актуальные угрозы ИСПДн, представляющие опасность для процесса обработки персональных данных. Один из способов определения таких угроз – оценка показателей критичности угрозы и реализуемость угрозы [114].

Процесс оценки информационных рисков ПДн состоит из следующих последовательных этапов: идентификация риска; анализ риска; оценивание риска.

При проведении идентификации риска формируется перечень элементов риска: элементов воздействия (ресурсы ИСПДн), угроз и уязвимостей. В качестве исходных данных используются: результаты аудита информационных рисков; данные о произошедших инцидентах (утечки, хищения, несанкционированная модификация персональных данных и т.д.); сценарии воздействия на персональные данные (рассмотрены в Приложении А к настоящей работе); экспертные оценки пользователей и специалистов (ответственные и уполномоченные за обработку персональных данных в организации) и т.д.

Результаты этапа идентификации используются далее для проведения анализа информационных рисков с целью определения:

− возможного ущерба от реализации риска нарушения безопасности элемента воздействия (величина зависит от стоимости элемента, стоимости его восстановления и критичности последствий нарушения его безопасности – нарушения конфиденциальности, целостности, доступности персональных данных);

− вероятности наступления нарушения;

− величины риска (оценивается его уровнем: приемлемый или требующий принятия дополнительных мер по минимизации его влияния на активы оператора ПДн).

Полученные результаты оценки рисков используются для определения стоимости и приоритетности мероприятий по минимизации рисков, а также дают возможность обоснованно принять решение по выбору защитных мер, снижающих уровни информационных рисков ПДн.

Другими словами, цель процесса оценки информационных рисков персональных данных и всего процесса управления рисками – определение минимально необходимого количества мер противодействия, которые позволят уменьшить количество уязвимостей ИСПДн. Схематично обобщённая схема воздействия на персональные данные, которая показывает взаимосвязь потенциальных угроз, уязвимостей, рисков, элементов воздействия и мер противодействия, представлена рисунке 1.5.

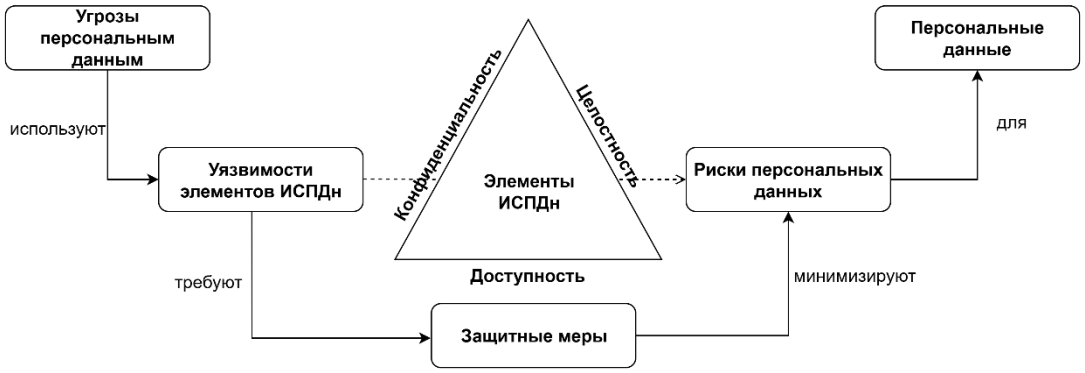


Рисунок 1.5 – Обобщенная схема воздействия на персональные данные

При выборе методики оценки и управления информационными рисками следует в первую очередь обратить внимание на то, насколько она отвечает потребностям организации, её масштабам и позволяет учитывать изменяющиеся условия. Как было показано выше, существующие методики оценки и анализа рисков недостаточно эффективны при оценке рисков нарушения качества ПДн в ИСПДн с облачной архитектурой, особенно если речь идёт о мультиоблачной архитектуре.

Выделим следующие проблемы, которые должны быть рассмотрены при создании модели оценки рисков нарушения качества ПДн [97,149]:

- установление соответствия между объектами предметной области ИС и определёнными для этой системы рисками ПДн. В рамках этой проблемы должен быть описан уровень значимости объекта предметной области с точки зрения рисков ПДн в ИСПДн. Т.е. должна быть отражена связь между обрабатываемыми

запросами, связанными с ПДн, и потенциальными последствиями нарушения одного или нескольких свойств их качества;

- определение степени влияния потенциальных воздействий на элементы (ресурсы) ИСПДн для создания спецификации допустимых и недопустимых воздействий на качество обрабатываемых ПДн в ИСПДн, а также определение степени их критичности;
- определение критичности использования уязвимости при воздействии каждой угрозы по каждому риску ПДн. В рамках этой проблемы определяется возможность осуществления какого-либо события риска ПДн за счёт использования слабых мест ИСПДн при реализации конкретного воздействия на обрабатываемые ПДн;
- описание эффективности мер по уменьшению различных видов уязвимостей, позволяющее описать механизмы противодействия уязвимостям ИСПДн и степень их эффективности. Такие механизмы могут существовать как в рамках самой ИСПДн, так и во внешней среде её функционирования.

Задача по уменьшению рисков при работе с большими объёмами ПДн предполагает совершенствование принимаемых мер по минимизации уязвимостей ИСПДн, необходимость использования которых и объём определяются важностью процессов и элементов, по отношению к которым эти меры применяются. Недостаточность мер влечёт за собой высокую вероятность сохранения потенциального возникновения риска, а избыточность мер – излишние затраты различных ресурсов, что может привести к ухудшению функциональных характеристик ИСПДн. Поэтому использование определённых функциональных средств по реализации этих мер позволяет достичь требуемой полноты всего множества функций по уменьшению вероятности возникновения рисков, а также наиболее эффективную реализацию групп таких функций конкретными средствами с точки зрения качества ПДн в ИСПДн [40]. Таким образом, проблема оценки рисков, согласно исследованию автора, «включает в себя оптимизационную задачу следующего вида:

$$\min_{Z} \max_{T} P_{\Sigma} \quad (1.3)$$

где P_{Σ} – объединённый (консолидированный) риск по оцениваемому множеству объектов (элементов) ИСПДн;

Z – множество принятых мер по уменьшению или устранению риска;

T – множество потенциальных угроз» [97].

При решении данной задачи обязательно учитываются приемлемый ущерб для владельца ИСПДн (оператора ПДн) и допустимые затраты на использование мер противодействия риску нарушения качества ПДн.

Выводы по первой главе

1. Представление жизненного цикла реализации процедур автоматизированной обработки персональных данных в виде этапов позволяет создать единый системный подход к организации безопасной обработки персональных данных в ИСПДн, унифицировав информационные процессы, что в дальнейшем даёт возможность разработать адекватную подсистему обеспечения качества этих процессов с целью выполнения требований нормативных правовых актов, эффективного использования ресурсов ИСПДн при обработке персональных данных и минимизации рисков нарушения их качества.

2. Границы процессов оценки эффективности использования ресурсов ИСПДн и рисков нарушения качества ПДн определяются совокупностью элементов (ресурсов), интерфейсов и архитектурой ИСПДн.

3. При соблюдении принципа системной целостности услуги, предоставляемые ИСПДн с определенным уровнем качества, не приводят к нежелательным последствиям в процессе обработки ПДн и выработки на их основе требуемого решения, т.е. обеспечиваются такие характеристики качества ПДн, как целостность, доступность, конфиденциальность, достоверность, точность, полнота, полезность и своевременность получения.

4. Для отслеживания процесса обработки запросов к ПДн и решения задачи

оценки эффективности использования ресурсов ИСПДн целесообразно применять методы моделирования и использовать для представления функционирования ИСПДн СМО с обслуживанием заявок в дискретном времени с ограничением по времени пребывания заявок в очереди, которая, в отличии от известных моделей, позволяет учитывать дискретную природу современных запросов к персональным данным субъекта.

5. Для решения задачи оценки и минимизации информационных рисков нарушения качества ПДн предложено при применении способов противодействия воздействиям на ИСПДн оценку допустимости информационных рисков свести к решению оптимизационной задачи, что в отличии от известных методов позволит учитывать новые и нестандартные угрозы и уязвимости, а также такие показатели, как приемлемый ущерб для оператора персональных данных и допустимые затраты на использование мер противодействия.

Глава 2. Исследование принципов организации и функционирования информационной системы с мультиоблачной архитектурой

2.1. Принципы организации и функционирования информационной системы при обработке запросов к персональным данным

Как было сказано выше в разделе 1.3 ИСПДн с облачной архитектурой относятся к классу территориально распределённых систем.

С учётом этого следует отметить, что многие организации (например, ОАО «РЖД», ПАО Сбербанк, Google, Cisco и т.п.) строят инфраструктуру, основанную на использовании нескольких центров обработки данных (ЦОД) и/или нескольких облаков от разных поставщиков облачных услуг. Эта тенденция получила своё развитие в появлении новой модели развёртывания облачных вычислений – мультиоблачная модель (мультиоблачная архитектура) [51,207,208,211]. В отличии от других моделей при построении информационной системы с мультиоблачной архитектурой предполагается одновременное использование различных облачных сервисов от разных поставщиков, объединённых в единую цифровую экосистему, для организации распределённой структуры и решения задач, рисунок 2.1. Это позволяет организациям снизить как капитальные вложения (CAPEX) так и операционные расходы (OPEX) за счёт использования арендуемых сервисов в облаках сторонних организаций. Последние рассматриваются как неотъемлемая составляющая мультиоблачной архитектуры информационной системы организации.

Существуют различные сценарии использования организацией мультиоблачной архитектуры, например, это может размещение данных у нескольких облачных поставщиков в разных регионах и/или на собственной распределённой инфраструктуре (корпоративном облаке) для выполнения локальных нормативных правовых требований к обработке персональных данных и обеспечению их качества (конфиденциальность, целостность доступность). Как показано на рисунке 2.1, эта архитектура может включать в себя корпоративную

инфокоммуникационную систему (в том числе и корпоративное облако). При такой компоновке будем считать, что гибридная архитектура – это подмножество мультиоблачной архитектуры [148,207].

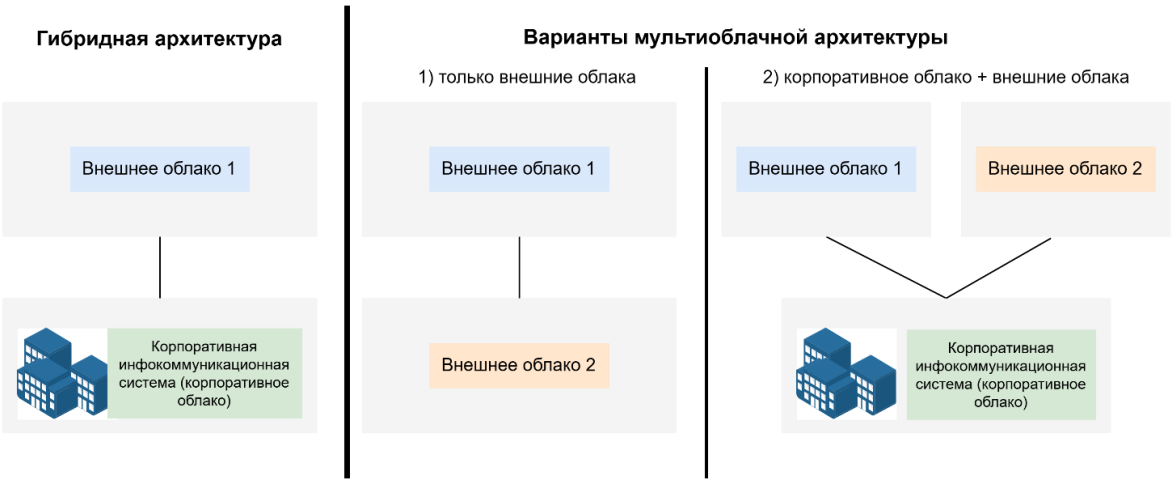


Рисунок 2.1 – Возможные варианты гибридной и мультиоблачной архитектур

Мультиоблачная модель активно используется в крупных территориально распределённых компаниях, которые имеют строгую иерархию и владеют информационно-телекоммуникационной сетью с архитектурой, построенной на базе ЦОД, принадлежащих головному офису (главному вычислительному центру), филиалам и дочерним компаниям, и позволяющей осуществлять хранение большого количества персональных данных в разных облаках (ЦОД) и распределённую обработку данных для достижения целей деятельности лица, принимающего решения (ЛПР). При этом должна обеспечиваться интероперабельность ИСПДн. Под интероперабельностью будет пониматься способность ИСПДн к безопасному обмену данными с другими системами и способность любых взаимодействующих в процессе коммуникации информационных систем одинаковым образом понимать смысл информации, которой они обмениваются.

На рисунке 2.2 представлена обобщённая схема организационной иерархической структуры территориально распределенной корпоративной ИСПДн с мультиоблачной архитектурой.

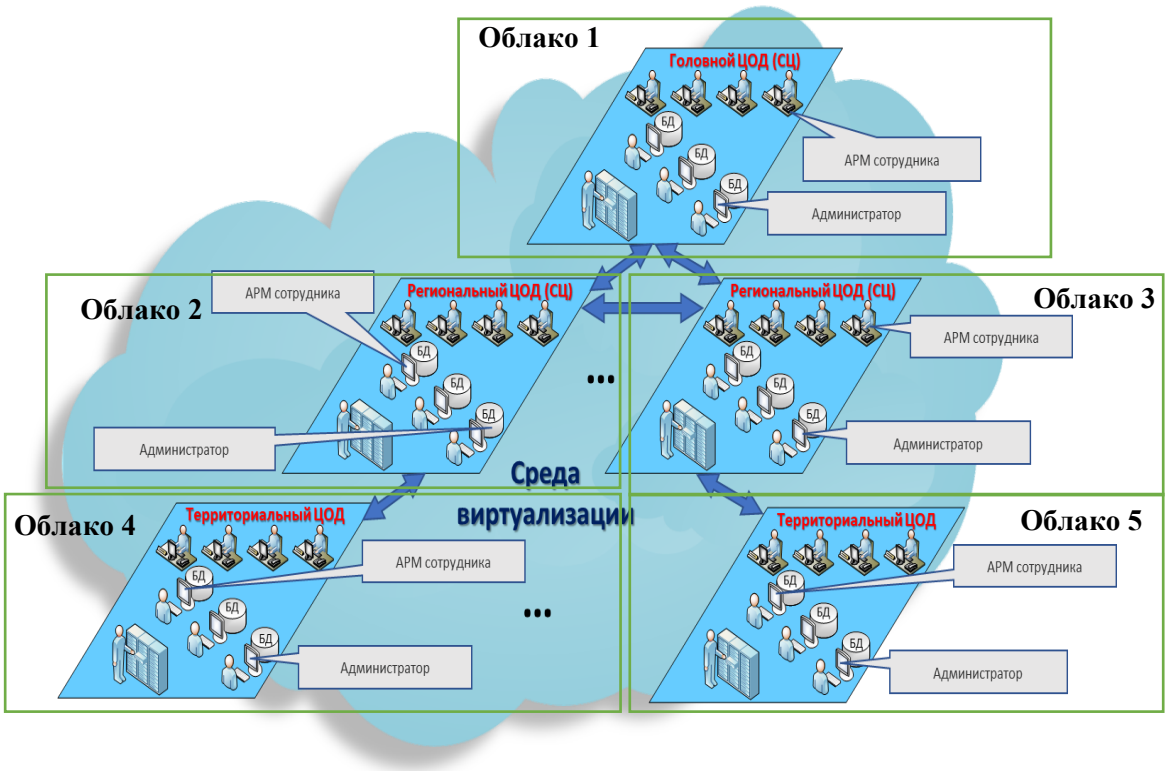


Рисунок 2.2 – Обобщённая схема организационной иерархической структура территориально распределенной корпоративной ИСПДн с мультиоблачной архитектурой

Таким образом ИСПДн с мультиоблачной архитектурой относится к классу больших систем, эффективность функционирования которых оценивается в первую очередь по таким ключевым параметрам, как производительность, масштабируемость, гибкость, доступность, интероперабельность, надёжность, безопасность, отказоустойчивость. К основным системным принципам организации и функционирования ИСПДн с мультиоблачной архитектурой, определяющих перечисленные параметры, опираясь на исследования В.А. Гадасина, И.Е. Ушакова, А.Ю. Гребешкова и др. [20,38,80,129,133,137], можно отнести:

− *производительность* ИСПДн с мультиоблачной архитектурой − способность ИСПДн обрабатывать большое количество одновременных запросов к персональным данным с допустимым временем отклика на запрос;

− *масштабируемость* ИСПДн с мультиоблачной архитектурой − способность ИСПДн справляться с увеличением рабочей нагрузки путём наращивания дополнительных ресурсов горизонтально (увеличение вычислительных ресурсов) и/или вертикально (увеличение мощности существующих ресурсов), используя одновременно ресурсы разных поставщиков облачных услуг;

− *гибкость* – возможность администрирования функциональных параметров ИСПДн в зависимости от внешних или внутренних требований;

− *доступность* ИСПДн с мультиоблачной архитектурой − способность ИСПДн выполнять заданную функцию по требованию пользователя в любое время;

− *интероперабельность* в условиях мультиоблачной архитектуры − способность ИСПДн взаимодействовать с другими информационными системами и обмениваться данными с ними, даже если эти взаимодействующие системы находятся в разных облаках;

− *надёжность* ИСПДн с мультиоблачной архитектурой − способность ИСПДн функционировать без ошибок и отказов за определённый промежуток времени, а также способность противостоять различным внутренним угрозам;

− *безопасность* ИСПДн с мультиоблачной архитектурой − способность ИСПДн обеспечивать качество обрабатываемых персональных данных, эффективность использования ресурсов, а также качество процессов обработки персональных данных;

− *отказоустойчивость* ИСПДн с мультиоблачной архитектурой − способность ИСПДн продолжать работу даже после возникновения сбоев или отказов отдельных компонентов или проблем у одного или нескольких поставщиков облачных услуг.

Большое значение здесь имеет выбор способа организации мультиоблачной

архитектуры ИСПДн. Облака состоят из нескольких подключенных к сети кластеров вычислительных ресурсов, таких как фермы серверов, СХД и т.д., в которых размещаются географически распределённые виртуальные машины и компоненты хранилища, обеспечивающие масштабируемость, надёжность и высокую доступность. На организацию ИСПДн с мультиоблачной архитектурой может влиять способ размещения бизнес- и технологических приложений [148,163,207, 208,211].

С точки зрения распределения приложений и их компонентов выделим архитектуру составную и с резервированием. В составной архитектуре приложения распределяются между двумя или более поставщиками облачных услуг и её предпочтительно использовать, когда производительность является ключевым фактором.

Архитектура с резервированием содержит два или более экземпляра одного и того же приложения и позволяет одному облаку взять на себя управление в случае сбоя другого (т.е. аварийного переключения). Такую архитектуру предпочтительнее использовать, когда доступность и отказоустойчивость приложения являются ключевым фактором. В ней приложения, перенесённые из одного облака в другое, не являются точной репликацией.

В зависимости от используемого шаблона выделим две категории мультиоблачных моделей: распределенного развертывания и избыточного развертывания. В таблице 2.1 представлены наиболее распространённые модели мультиоблачной архитектуры с распределением по категориям шаблонов [196,201,208].

Проведённый анализ показал, что выбор модели зависит в большей степени от бизнес-целей и бизнес-процессов организации, а также от требований, предъявляемых к параметрам и показателям эффективного использования инфокоммуникационных ресурсов. При этом критически важным аспектом для обеспечения бесперебойной работы деятельности организации и поддержания высокого уровня доступности сервисов в мультиоблачной архитектуре является отказоустойчивость.

Таблица 2.1 – Наиболее распространённые модели мультиоблачной архитектуры

Категория шаблонов модели	**Описание шаблона**	**Мультиоблачная модель**
Шаблоны распределенного развертывания	Направлены на распределение рабочих нагрузок и/или компонентов приложений по разным облакам для обеспечения гибкости и производительности	• Многоуровневая гибридная модель (Tiered hybrid pattern) • Разделённая модель (Partitioned multicloud pattern) • Модель облачной аналитики (Analytics hybrid and multicloud pattern) • Модель периферийной гибридной архитектуры (Edge hybrid pattern)
Шаблоны избыточного развертывания	Основаны на избыточных развертываниях рабочих нагрузок с целью обеспечения отказоустойчивости, доступности, надёжности за счёт дублирования сервисов в разных облаках	• Гибридная среда (Environment hybrid pattern) • Модель обеспечения непрерывности бизнеса (Business continuity hybrid and multicloud patterns) • Модель разрыва облака (Cloud bursting pattern)

С точки зрения обеспечения эффективного и отказоустойчивого функционирования информационные системы персональных данных с мультиоблачной архитектурой обладают следующими преимуществами:

1. Распределение ресурсов (вычислительных мощностей, хранилищ данных и др.) между разными поставщиками облачных услуг позволяет избежать зависимости от одного поставщика и минимизировать риски, связанные с возможными сбоями у кого-то из них.

2. Резервирование и репликация данных на ресурсах разных поставщиков облачных услуг позволяет осуществить быстрое восстановления данных после

сбоев и минимизировать риск потери данных. Поскольку при репликации данные доступны сразу в нескольких местах, это обеспечивает высокую доступность услуг ИСПДн. Важное условие - синхронизация данных между различными поставщиками облачных услуг должна происходить в реальном времени или с минимальной задержкой.

3. Автоматизация процессов восстановления ИСПДн после сбоев даёт возможность автоматически перенаправлять запросы к другим ресурсам, сохраняя работоспособность.

4. Размещение инфраструктурных элементов ИСПДн в разных географических регионах снижает вероятность одновременного выхода из строя всех частей системы. Тогда в случае, если один регион столкнется с природным/техногенным катаклизмом или техническим сбоем, другие регионы смогут продолжить обслуживание пользователей ИСПДн.

5. Многоуровневая защита от отказов на аппаратном (например, использование RAID-массивов для хранения данных) и программном уровнях (резервирование серверов, балансировка нагрузки) позволяет ИСПДн восстановить свою функциональность даже в случае отказа отдельных компонентов.

6. Балансировщики нагрузки автоматически распределяют трафик между разными ресурсами поставщиков облачных услуг и направляет запросы к доступным серверам, обеспечивая равномерную нагрузку на каждый ресурс. Это предотвращает перегрузку одной части системы и улучшает общую производительность и поддерживает стабильность работы всей ИСПДн.

7. Системы мониторинга отслеживают состояние всех компонентов ИСПДн и отправляют уведомления об аномалиях или сбоях, что позволяет оперативно реагировать на возникающие проблемы.

8. Возможность обеспечения локализации ПДн.

Можно сделать вывод, что в ИСПДн с мультиоблачной архитектурой реализована технология адаптивной отказоустойчивости, отвечающая следующим требованиям к отказоустойчивости информационных систем [146]:

– в составе ИСПДн отсутствует какой-либо ресурс (элемент), выход из строя

которого приводит к полному отказу всей системы;

– гарантируется решение поставленных задач при соблюдении временных ограничений;

– в системе присутствуют средства, реализующие функции наблюдаемости и управляемости, которые гарантируют реакцию на любое событие, даже ошибку (сбой), что обеспечит работу ИСПДн фактически в любых условиях;

– оперативное восстановление ресурсов;

– обеспечения изоляция модулей программного обеспечения для избежания того, чтобы ни одна из программ не смогла разрушить ни другие модули, ни базовую операционную систему.

Использование адаптивной отказоустойчивости позволяет минимизировать вероятность и продолжительность незапланированных простоев ИСПДн благодаря отсутствию единой точки отказа, т.е. если произойдёт сбой у одного поставщика облачных услуг, ключевые рабочие нагрузки можно будет максимально быстро переместить на ресурсы другого(их) поставщика(ов). Подробно вопросы отказоустойчивости информационных систем рассмотрены в [54,80,92,97,137,169]. Анализ приведённых источников позволяет сделать вывод, что ИСПДн с мультиоблачной архитектурой следует отнести к классу распределённых систем, одним из главных преимуществ которых и является повышенная отказоустойчивость. Более детальное исследование данного вопроса выходит за рамки настоящего исследования.

2.2. Особенности обработки запросов к персональным данным в информационной системе

Главной целью создания ИСПДн, как и любой информационной системы, является поддержка бизнес- и технологических процессов предприятия путём хранения и обработки данных, а также предоставления доступа к ним потребителям. Совокупность всех элементов ИСПДн должна обеспечить качество обрабатываемых персональных данных и соблюдение законодательных норм. Для

потребителей информации одним из наиболее важных требований является качество получаемой информации, поэтому важно обеспечить выполнение данного требования на каждом из этапов обработки ПДн (раздел 1.1 настоящей диссертационной работы).

Выделим следующие определяющие характеристики ПДн, обрабатываемых в ИСПДн:

− объём (физический объём на устройстве хранения, занимаемый данными);

− скорость (скорость прироста новых данных и скорость обработки; означает необходимость обработки большого количества данных за короткий промежуток времени);

− разнообразие (одновременная обработка различных типов структурированных и неструктурированных данных);

− вариативность (изменения в скорости передачи данных, их формате/структуре, семантике и/или качестве, которые влияют на поддерживаемое приложение; подразумевает необходимость увеличения или уменьшения виртуализированных ресурсов для эффективного управления дополнительной нагрузкой на обработку).

Одной из главных особенностей больших объёмов обрабатываемых персональных данных является то, что невозможно организовать эффективную работу с ними на одной вычислительной машине, поэтому в этом случае традиционные инструменты обработки данных не подходят.

Предлагается структура для управления, хранения, обработки и анализа персональных данных большого объёма, отображённая на рисунке 2.3. Она представляет собой совокупность 5 компонентов:

• Центральный системный компонент. Обеспечивает требования, которые должна выполнять система, включая политику, управление, архитектуру, ресурсы и бизнес-требования, а также мониторинг или аудит, чтобы гарантировать, что система соответствует этим требованиям.

• Поставщик данных. Предоставляет данные для себя или для других. Компонент может быть частью внутренней или внешней системы. После того, как данные поступают в локальную систему, запросы на получение необходимых данных будут сделаны компонентом прикладных процессов, а затем переданы компоненту предоставления инфраструктуры.

• Компонент предоставления прикладных процессов. Выполняет манипуляции с жизненным циклом данных в соответствии с требованиями, установленными центральным системным компонентом, а также отвечает требованиям безопасности и конфиденциальности.

• Компонент предоставления инфраструктуры. Имеет общие ресурсы или службы, которые будут использоваться поставщиком данных при создании конкретного приложения. К ним относятся вычислительные и сетевые ресурсы, а также ресурсы необходимые для хранения и обработки.

• Потребитель данных. Получает выходные данные системы в виде различных отчетов, визуализированных представлений. Кроме того, данный компонент обеспечивает поиск, извлечение, анализ и экспорт данных.

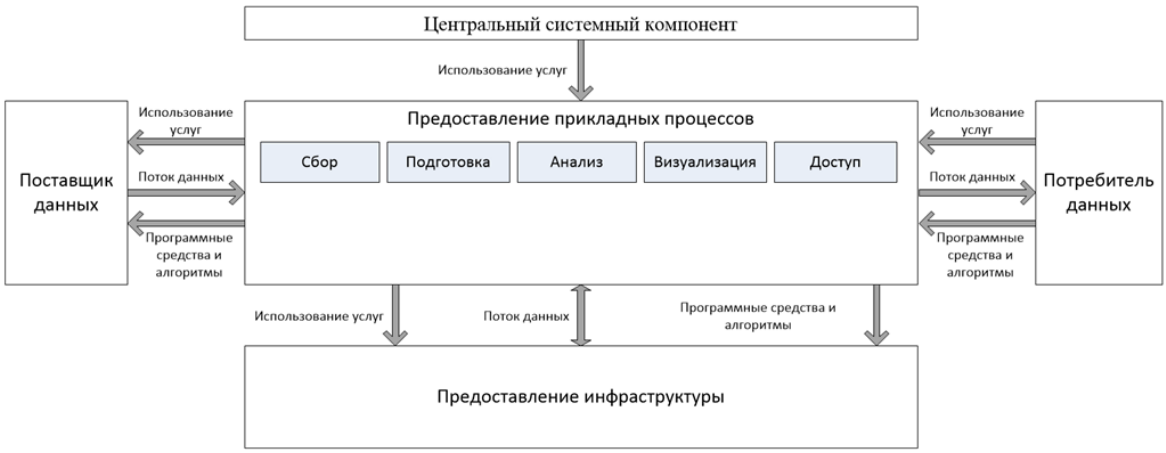


Рисунок 2.3 – Структура для управления, хранения, обработки и анализа персональных данных большого объёма

Таким образом, использование для обработки больших объёмов персональных данных технологии мультиоблачных вычислений, позволяющей

обеспечить ИСПДн необходимым количеством аппаратно-программных ресурсов по запросу, обоснованно. Мультиоблачные вычисления обладают значительным потенциалом для повышения эффективности обслуживания запросов на обработку персональных данных, поступающих с разных подсистем ИСПДн, находящихся в разных облаках, за счёт того, что при мультиоблачной архитектуре ИСПДн все услуги и ресурсы, получаемые от нескольких поставщиков облачных услуг, интегрированы в единую цифровую экосистему [163,211].

В условиях развития информационных технологий возрастает актуальность применения риск-ориентированного подхода к оценке эффективности использования ресурсов ИСПДн и рисков нарушения качества обрабатываемых в ИСПДн персональных данных [41,47,54,55,125,172].

Проведенный в разделе 2.1 анализ принципов построения ИСПДн с мультиоблачной архитектурой позволил выделить ключевые особенности ИСПДн с мультиоблачной архитектурой, которые оказывают влияние на процессы обработки запросов к персональным данным:

1. В ИСПДн с мультиоблачной архитектурой данные и процессы могут быть распределены по нескольким облачным платформам, что усложняет обработку данных, поскольку каждая облачная платформа имеет свои собственные стандарты хранения, API и форматы данных. При этом важно учитывать, что:

- использование нескольких облаков может увеличивать задержки передачи данных, что может быть критичным для задач реального времени;
- для уменьшения задержек данные часто распределяются по регионам, ближайшим к пользователям;
- в мультиоблачной архитектуре часто используют различные технологии хранения, включая реляционные базы данных и NoSQL-решения, требующие для переноса данных между такими хранилищами конвертации форматов и решений для интеграции.

2. В ИСПДн с мультиоблачной архитектурой существует проблема согласованности данных между различными облаками. Могут использоваться разные модели согласованности, например:

- традиционная модель ACID (*англ.* Atomicity, Consistency, Isolation, Durability), которая требует полной согласованности между транзакциями, что при работе в мультиоблачной архитектуре может стать сложной задачей из-за необходимости координации транзакций между различными облаками;
- модель BASE (*англ.* Basically Available, Soft state, Eventual consistency) позволяет асинхронно реплицировать данные между облаками, обеспечивая высокую доступность и время достижения согласованности после обновления данных от 100 до 500 миллисекунд.

3. В мультиоблачной архитектуре необходимо обеспечивать оркестрацию и распределение нагрузок между различными облаками. Например:

- использование контейнеров (например, Docker) и оркестрации (например, Kubernetes) позволяет легко управлять распределенными рабочими нагрузками, обеспечивая эффективное распределение задач между различными облаками;
- балансировка нагрузки с помощью балансировщика позволяет распределять запросы пользователей между облаками, направляя их к наиболее производительным облакам с учетом текущей нагрузки и/или близости к конечным пользователям.

4. Проблема обеспечения безопасности и контроля доступа, поскольку каждое облако имеет свои политики безопасности и методы аутентификации, такие как:

- единая система аутентификации (SSO), которая позволяет пользователям входить в систему через единую точку доступа;
- шифрование данных при передаче и хранении, так как данные пересекают границы различных облаков.

Результаты проведённого сравнительного анализа обработки запросов к персональным данным в ИСПДн с различной архитектурой: централизованной, распределённой и мультиоблачной приведены в Приложении Б.

Как показывает анализ данных, приведённых в таблице П.Б.1, увеличение задержки передачи обрабатываемых данных и времени обработки в мультоблачной архитектуре при сравнении с их обработкой в традиционной архитектуре (централизованной и распределённой) компенсируется за счёт согласованности обрабатываемых данных для минимизации задержек, а также очень высокой доступностью используемых ресурсов. Отметим, что процесс организации безопасной обработки персональных данных в мультиоблачной модели более сложный и более дорогостоящий [163,198,221]. Однако это компенсируется повышением масштабируемости и производительности за счёт выбора лучших предложений от разных поставщиков облачных услуг, а также отказоустойчивости за счёт применения адаптивной технологии отказоустойчивости, отсутствия зависимости от одного поставщика и возможности выбора сервисов, в том числе по обеспечению качества обработки персональных данных (например, связанных с необходимостью локализации данных).

2.3. Варианты развертывания ИСПДн с мультиоблачной архитектурой

Архитектуры мультиоблачных приложений, которые обращаются к базам данных, зависят от сценария использования. Архитектурная абстракция мультиоблачного приложения состоит из базы данных, прикладных сервисов и клиентов приложений. Для определения сценариев использования мультиоблачных архитектур используется общая архитектура приложений, как показано на рисунке 2.4 [148].

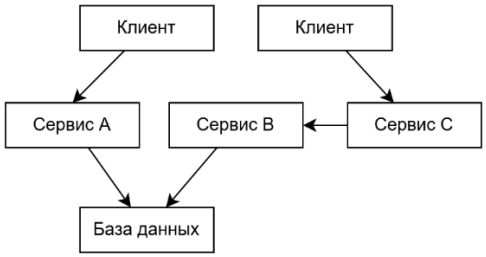


Рисунок 2.4 – Общая архитектура приложений в мультиоблачной среде

Проведённый анализ показал, что база данных может быть одноэкземплярной, многоэкземплярной или распределённой, размещённой на вычислительных узлах или доступной в виде облачного сервиса.

Прикладные сервисы объединяются в приложение, реализующее бизнес-логику. Приложение может быть контейнерным (прикладные сервисы - микросервисы в Kubernetes), монолитным на одной большой виртуальной машине и т.д. Некоторые сервисы приложений могут получать доступ к базе данных. Каждый сервис приложений можно развернуть несколько раз, каждое развертывание сервиса приложений является экземпляром этого сервиса.

Клиенты приложений получают доступ к функциям, предоставляемым службами приложений, с АРМ на компьютере, ноутбуке, мобильном телефоне или через браузер.

Каждая стрелка между компонентами (рисунок 2.4) представляет собой связь по сетевому соединению – например, клиент приложения, обращающийся к сервису приложения. Соединение может быть внутри облака или между облаками. В мультиоблачных средах важным фактором является сетевое взаимодействие между облаками. Предполагается, что между облаками существует безопасное сетевое соединение, а базы данных и их компоненты могут взаимодействовать друг с другом.

С точки зрения управления данными предлагается выделить следующие основные варианты использования мультиоблачных архитектур:

- Разделённые данные. Каждая часть приложения имеет свою собственную базу данных (отдельный раздел), и ни одна из баз данных не связана напрямую с

другими. Приложение, управляющее данными, записывает любые данные, которые должны быть доступны в обеих базах данных (разделах), дважды.

• Асинхронно реплицируемая база данных. Асинхронная репликация используется, если данные из одного облака должны быть доступны в другом облаке. Например, если аналитическому приложению требуется тот же набор данных или его часть для бизнес-приложения, последний набор данных может быть реплицирован между облаками.

• Транзакционно-синхронизированная база данных. Такие базы данных позволяют сделать данные доступными для обеих частей приложения. Каждое обновление в каждом из приложений является транзакционно согласованным и немедленно становится доступным для обеих баз данных (разделов). Транзакционно-синхронизированные базы данных фактически действуют как единая распределённая база данных.

При использовании асинхронной реплицированной базы данных существует риск того, что один и тот же элемент данных будет изменен в двух местах развертывания одновременно. Чтобы определить, какое из двух конфликтующих изменений является окончательным согласованным состоянием, необходимо реализовать стратегию разрешения конфликтов, что зачастую вызывает трудности и требует ручного вмешательства для восстановления данных в согласованное состояние.

Данные в транзакционно-синхронизированной базе данных согласованы во всех местах развёртывания, поэтому такая база данных является наилучшим вариантом для развертывания экземпляров сервисов.

Для вышеперечисленных сценариев использования мультиоблачных архитектур были определены следующие возможные основные виды связей (схем развёртывания) между базами данных, расположенных в разных местах развёртывания:

- разделение без зависимости между базами данных;
- асинхронная однонаправленная репликация;
- двунаправленная репликация с разрешением конфликтов;

– полностью активная-активная синхронизированная распределенная система.

Каждый вариант использования можно сопоставить с одной или несколькими из четырёх схем развёртывания. В зависимости от сценария использования балансировщик нагрузки применяется для динамического перенаправления запросов клиентов к приложениям, как показано на рисунке 2.5.

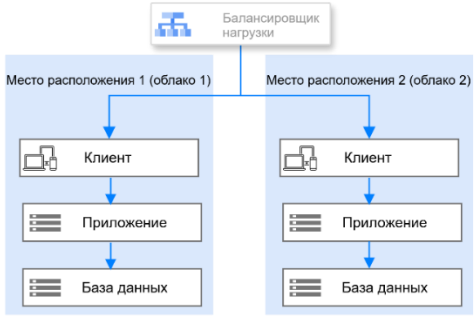


Рисунок 2.5 – Перенаправление запросов клиентов в одно из доступных расположений приложения

Схема взаимодействия «разделение без зависимости между базами данных» является самой простой схемой развёртывания: каждое местоположение приложения (облако) имеет базу данных, которые содержат разделённые наборы данных (сегменты), независимые друг от друга. Элемент данных хранится только в одной базе данных. Каждый раздел (сегмент) данных находится в своей собственной базе данных, что обеспечивает разделённый набор данных без репликации между ними.

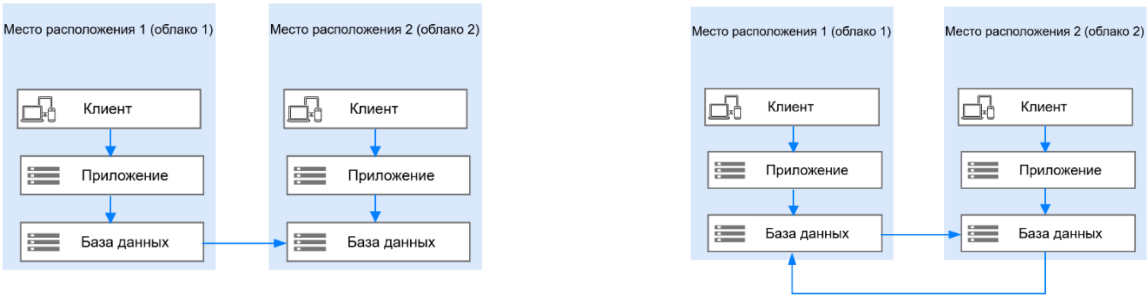
Альтернативный вариант развёртывания для баз данных с разделением заключается в том, что набор данных полностью разделён на сегменты, но при этом хранится в одной и той же базе данных. Существует только одна база данных, содержащая все наборы данных. Наборы данных, хранящиеся в одной и той же базе данных, полностью разделены (на сегменты) и изменение одного из них не приводит к изменениям в другом. На рисунке 2.6 показаны схемы развертывания «разделение на сегменты без зависимости между базами данных».

а) полностью разделённые приложения б) с использованием общей БД

Рисунок 2.6 – Разделение на сегменты без зависимости между базами данных

В схеме развёртывания «асинхронная однонаправленная репликация» есть основная база данных, которая реплицируется в одну или несколько дополнительных баз данных. Дополнительную базу данных можно использовать, например, для доступа на чтение. При этом варианте организации связи надо обязательно учитывать потенциальную задержку репликации. На рисунке 2.7 (а)) приведён вариант, когда одна из двух баз данных является копией другой. Стрелка на схеме указывает направление репликации: данные из системы баз данных в месте расположения 1 (облако 1) реплицируются в систему баз данных в месте расположения 2 (облако 2).

В схеме развёртывания «двунаправленная репликация с разрешением конфликтов» используются две основные базы данных, которые асинхронно реплицируются друг в друга. Если в каждую базу данных одновременно записываются одни и те же данные (например, один и тот же первичный ключ), это может привести к конфликту при записи. Из-за этого риска необходимо предусмотреть разрешение конфликтов, чтобы определить, какое состояние является последним во время репликации. Этот шаблон можно использовать в ситуациях, когда вероятность конфликта при записи невелика. На рисунке 2.7 (б)) показаны два приложения, обращающиеся к базам данных с двусторонней репликацией: две репликации независимы друг от друга, что показано двумя отдельными синими стрелками.



а) асинхронная однонаправленная репликация

б) двунаправленная репликация с разрешением конфликтов

Рисунок 2.7 – Схемы развертывания с репликацией баз данных

В схеме развёртывания «полностью активная-активная синхронизированная распределенная система» используется одна база данных с настройкой «активный-активный» («основной-основной»). При настройке «активный-активный» обновление данных в любой основной БД является согласованным с точки зрения транзакций и синхронно реплицируется. Примером использования этого шаблона являются распределённые вычисления. На рисунке 2.8 показаны два приложения, обращающихся к полностью синхронизированной «основной-основной» БД.

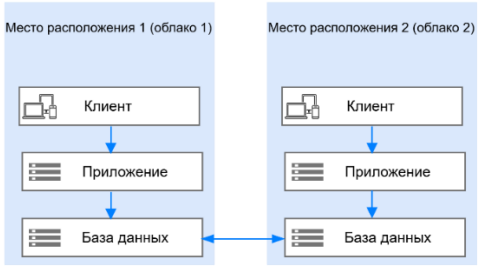


Рисунок 2.8 – Полностью активная-активная синхронизированная распределенная система

При такой схеме развёртывания гарантируется, что каждое приложение всегда получает доступ к последнему согласованному состоянию без задержек и риска конфликта. Изменение в одной базе данных немедленно отражается в другой базе данных. Любое изменение отражается в обеих базах данных при фиксации транзакции.

Кроме того, в мультиоблачных средах можно организовать контекстно-зависимое развертывание, разделив клиентов на группы по определённым критериям.

Таким образом анализ вариантов развёртывания и использования ИСПДн с мультиоблачной архитектурой показал, что для обеспечения максимальной полноты поиска персональных данных интерес, с точки зрения управления данными, будет представлять архитектура с транзакционно-синхронизированными базами данных со схемой развёртывания «полностью активная-активная синхронизированная распределенная система», исследование которой является самостоятельной задачей, выходящей за рамки данного исследования.

2.4. Обобщённые сценарии запросов на обработку персональных данных в информационной системе

Для отслеживания информационных процессов автоматизированной обработки ПДн и построения моделей этих процессов необходимо определить основные типы запросов на обработку ПДн в ИСПДн и разработать соответствующие сценарии для каждого типа запроса.

Рассмотрим «обобщённые сценарии различных типов запросов на обработку ПДн, которые могут храниться и обрабатываться в различных подсистемах ИСПДн. Данные подсистемы могут контролироваться и управляться различными службами организации» [171]. На рисунке 2.9 представлен типичный набор информационных систем персональных данных бизнес-процессов верхнего уровня крупной транспортной компании.

Рисунок 2.9 – Информационные системы персональных данных бизнес-процессов верхнего уровня транспортной компании

В общем случае в компании может быть несколько десятков ИСПДн. Кроме того, учитывая, что число персональных данных может составлять десятки миллионов, на практике они могут храниться в информационных подсистемах, объединяемых мультиоблачной архитектурой. На рисунке 2.10 представлен вариант организации ИСПДн на базе мультиоблачной модели.

Рисунок 2.10 – Вариант организации ИСПДн на базе мультиоблачной модели

На рисунке 2.11 представлен пример функциональной схемы ИСПДн с мультиоблачной архитектурой, отражающей процесс взаимодействия пользователей с системой при обработке запросов к персональным данным.

Определим категории пользователей, инициирующих запросы к ИСПДн:

– работник организации, имеющий легитимное право доступа к ИСПДн (далее работник), – может отправлять запросы на обработку ПДн в ИСДН либо в замкнутом контуре со своего АРМ, либо со своего устройства по VPN;

– внешний пользователь (неработник) – может отправлять запросы в ИСПДн по Интернет через веб-приложение. Это могут быть клиенты, партнёры и др.

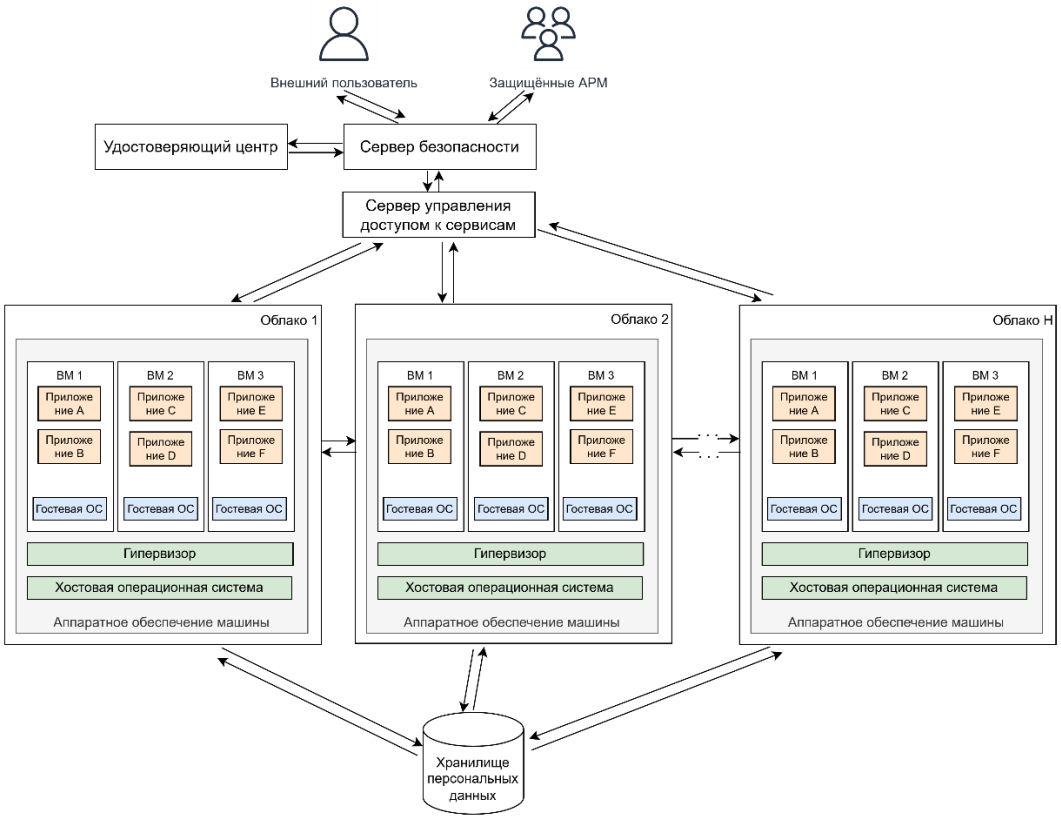


Рисунок 2.11 – Вариант функциональной схемы ИСПДн с мультиоблачной архитектурой

Проведенный анализ показал, что тип запроса зависит от категории пользователя, инициирующего запрос к ИСПДн, цели и содержания запроса.

Со стороны работника в зависимости от его должностных обязанностей запросы можно классифицировать на две группы, в рамках которых и определяются типы запросов:

1. *Операционные запросы*, связанные с целями деятельности организации. К основным типам запросов этой группы относятся: доступ к ПДн субъекта; поиск информации о ПДн; создание цифрового профиля субъекта ПДн; извлечение ПДн; систематизация ПДн; внесение изменений в ПДн (цифровой профиль) субъекта ПДн; экспорт (передача) ПДн; блокирование ПДн; удаление ПДн (цифрового профиля) субъекта ПДн; уничтожение ПДн; архивирование ПДн; обезличивание ПДн.

2. *Обеспечивающие запросы*, напрямую несвязанные с целями деятельности организации и ненаправленные на непосредственную работу с содержанием ПДн, но необходимые для обеспечения качества ПДн. Это запросы, связанные с обеспечением информационной безопасности ПДн, администрированием, техподдержкой и т.п. В рамках настоящей диссертационной работы эта группа запросов не исследуется.

Если внешним пользователем ИСПДн является клиент организации, то с его стороны возможны следующие типы запросов: создание своего цифрового профиля; доступ к своим ПДн; поиск информации о своих ПДн; внесение изменений в свои ПДн; запрос на удаление своих ПДн; запрос на ограничение обработки ПДн; запрос на передачу (перенос) своих ПДн.

Если внешним пользователем ИСПДн является, например, бизнес-партнёр организации, то с его стороны возможна инициация следующих типов запросов: запрос на передачу ПДн для осуществления совместной деятельности; запросы на ПДн с целью проведения совместных маркетинговых кампаний; запросы на проверку ПДн клиентов; запросы на интеграцию ИС с целью синхронизации различных ИСПДн и т.д.

В свою очередь со стороны ИСПДн к пользователю могут быть следующие типы запросов:

- оповещение пользователя;
- уточнение запроса пользователя или действий.

Допускается, что работники имеют право в рамках своих должностных обязанностей и назначенных прав доступа запрашивать и получать информацию, содержащую ПДн, в любом ресурсе мультиоблачной архитектуры организации.

На рисунке 2.12 представлен предлагаемый обобщённый сценарий запроса в ИСПДн с мультиоблачной архитектурой на создание цифрового профиля субъекта ПДн. Здесь, на рисунке, «Человек» – это работник оператора ПДн, «Облако» – облачный ресурс ИСПДн, «Сервер» – сервер безопасности и управления доступом. Отметим, что один запрос представляет из себя последовательность запросов, указанных выше, поскольку при его выполнении активируются и другие запросы.

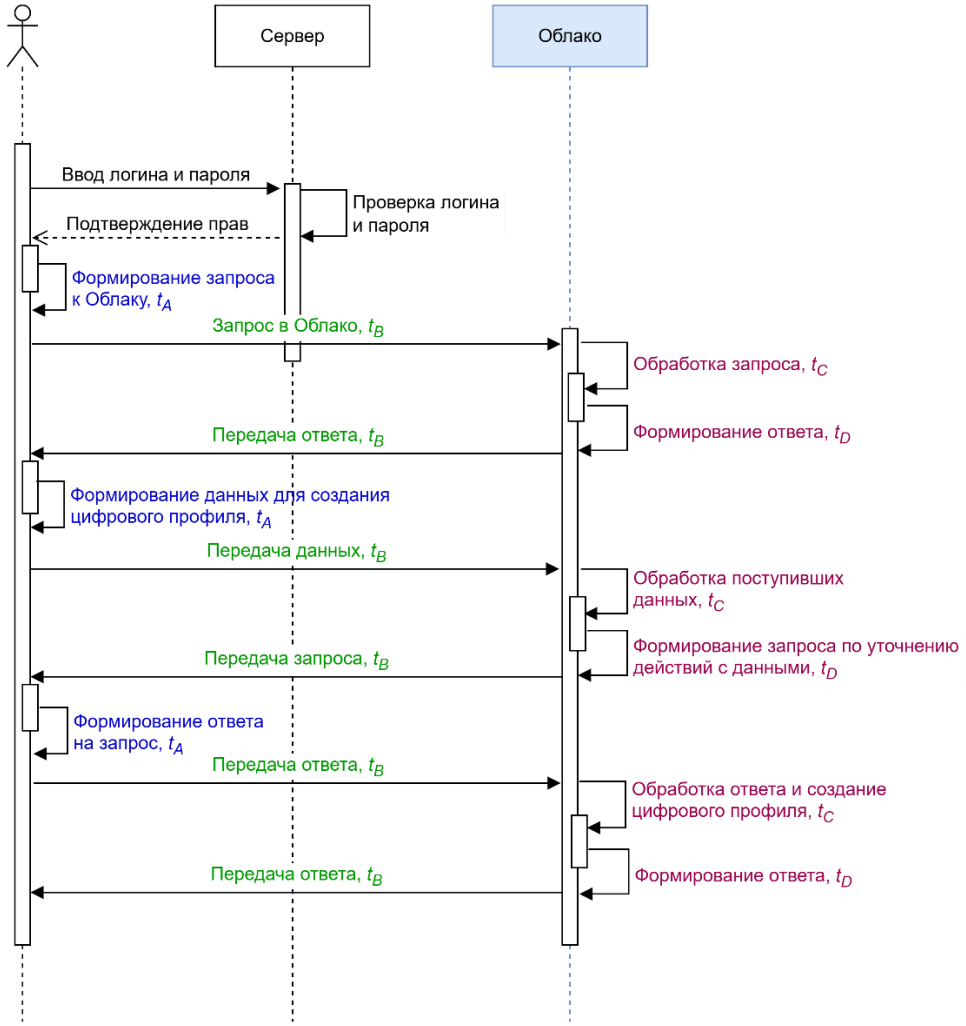


Рисунок 2.12 – Обобщённый сценарий запроса в ИСПДн с мультиоблачной архитектурой на создание цифрового профиля субъекта персональных данных

На рисунке 2.13 представлен «обобщённый сценарий процесса обработки запроса на поиск информации о ПДн в ИСПДн, предполагающего формирование в ИСПДн ответа на основе имеющихся данных в одном облаке (например, Облако 1), а также, в случае недостаточности – данных, полученных от подсистем ИСПДн, которые могут находиться в других облаках (Облако i, $i = \overline{1, H}$)» [171].

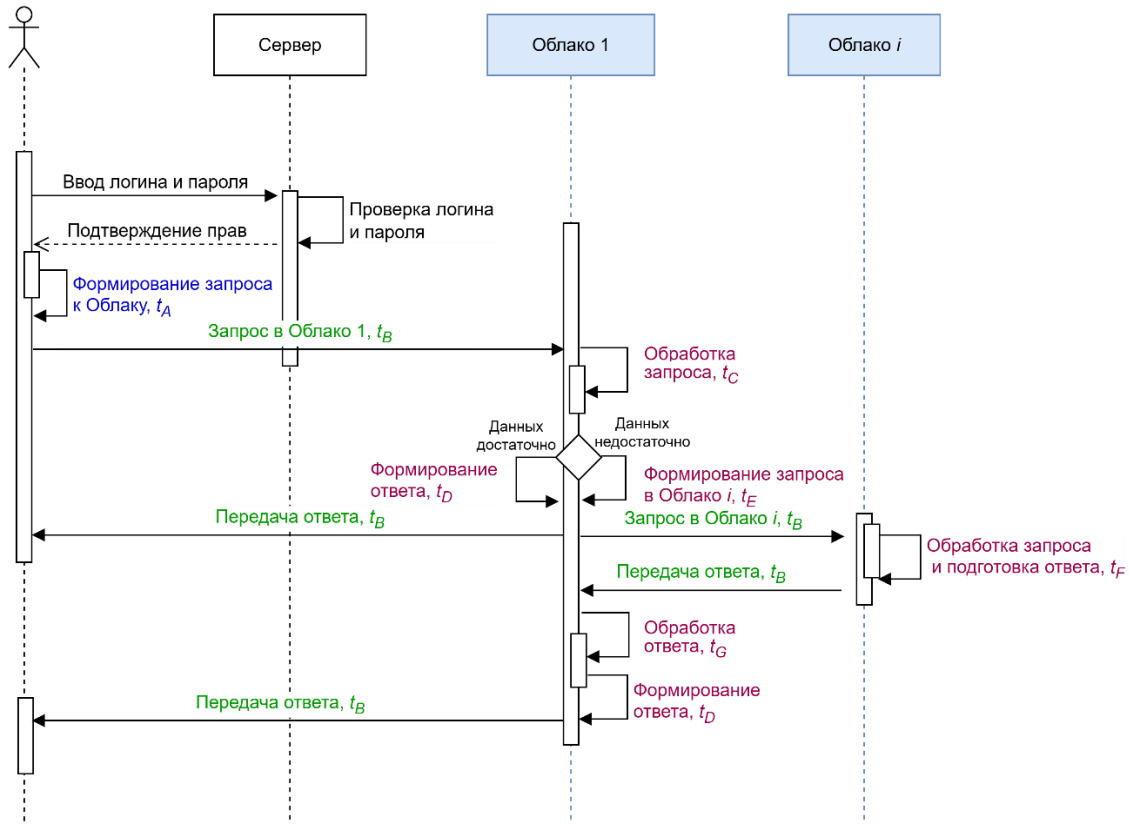


Рисунок 2.13 – Обобщённый сценарий запроса в ИСПДн с мультиоблачной архитектурой на поиск информации о персональных данных

Предложенные сценарии позволяют выделить участников всех этапов инициации и обработки запроса, этапы его обработки и для каждого этапа дать краткое описание и указать формирование задержек на этих этапах. Это позволяет построить граф переходов между макросостояниями процесса обработки запроса к персональным данным в информационной системе, на базе которого будет построена аналитическая модель, представленная в главе 3.

Выводы по второй главе

1. ИСПДн с мультиоблачной архитектурой отличаются от традиционных ИСПДн с распределённой архитектурой возможностью одновременного использования различных облачных сервисов от разных поставщиков,

интегрированных в единую цифровую экосистему. При этом процессы, связанные с автоматизированной обработкой запросов к персональным данным, в подобных информационных системах обладают рядом особенностей, которые оказывают влияние на показатели эффективности использования ресурсов.

2. Анализ вариантов развёртывания и использования ИСПДн с мультиоблачной архитектурой показал, что архитектура с транзакционно-синхронизированными базами данных со схемой развёртывания «полностью активная-активная синхронизированная распределенная система» обеспечивает максимальную полноту поиска персональных данных с точки зрения управления данными.

3. Разработанные в настоящей диссертационной работе обобщённые сценарии обработки разного типа запросов к персональным данным позволяют выделить участников всех этапов инициации и обработки запросов, для каждого этапа дать краткое описание и указать формирование задержек на этих этапах. Это позволяет построить граф переходов между макросостояниями процесса обработки запроса к персональным данным в информационной системе.

4. Представление процесса обработки запроса к персональным данным в виде графа позволит построить аналитическую модель информационных процессов обработки персональных данных в ИСПДн, которая, в отличии от известных, учитывает мультиоблачную архитектуру системы.

Глава 3. Разработка модели и алгоритма оценки эффективности использования ресурсов информационной системы с мультиоблачной архитектурой при обработке персональных данных

3.1. Формализация задачи оценки эффективности использования ресурсов информационной системы с мультиоблачной архитектурой при обработке запросов к персональным данным

Одной из основных задач оператора персональных данных является обеспечение эффективного использования ресурсов ИСПДн при выполнении запросов к персональным данным. Это достигается путём применения различные методов и подходов для обеспечения непрерывной работы ИСПДн. Задача эта становится ещё более актуальной в мультиоблачных моделях для поддержания значений показателей с учётом тех особенностей функционирования ИСПДн и обработки запросов, проанализированных в разделах 2.1 и 2.2.

Для формализации процесса оценки эффективности использования ресурсов информационной системы используем подход «основанный на графо-матричной модели процесса обработки запросов к ПДн в ИСПДн и анализе отображающей их СМО с фазовым распределением процесса обслуживания в дискретном времени» [60]. С учётом вышесказанного построим соответствующую модель для оценки эффективности использования ресурсов ИСПДн с мультиоблачной архитектурой [7,58,59,60,169,171].

Рассмотрим построение модели функционирования ИСПДн с мультиоблачной архитектурой [169,171] в общем абстрактном виде на примере разработанного в разделе 2.4 обобщённого сценария процесса обработки запроса на поиск информации о ПДн в ИСПДн (рисунок 2.13). Предполагается, что базы данных соответствуют требованиям согласованности и целостности и время на их блокировку при выполнении запроса далее не учитывается. Опишем данный процесс: уполномоченный работник оператора (инициатор запроса) отправляет со своего АРМ (с любого разрешённого устройства) запрос в ИСПДн на получение

персональных данных субъекта из базы данных. Сервер безопасности проверяет права доступа и полномочия работника на совершение действий с персональными данными. В случае неправомерности доступа работник получает отказ. При наличии прав запрос для дальнейшего распределения поступает на сервер управления распределением сервисов. Далее запрос поступает в одно из облаков в соответствии с используемым сценарием. Если в этом облаке нет запрашиваемой информации или она неполная, то запрос в соответствии со сценарием перенаправляется далее в другие облака, пока не будет сформирован полный ответ на запрос. После этого ответ передаётся инициатору запроса на АРМ. При этом, если это требуется, возможен интерактивный диалог работника и ИСПДн для уточнения действий.

Введём для построения графа переходов «множество макросостояний процесса обработки запроса $S = \{A, B, C, D, E, F, G\}$» [171], где «макросостояния имеют следующий смысл:

A – формирование человеком запроса о ПДн в ИСПДн;

B – передача запроса/ответа и ожидание его обработки (макросостояние может быть декомпозировано на несколько макросостояний при необходимости учёта времени ожидания обработки)» [171];

C – обработка запроса о ПДн в облаке ИСПДн;

D – формирование облаком ИСПДн ответа или уточняющего запроса человеку;

E – формирование облаком ИСПДн запроса о ПДн к подсистемам ИСПДн, «которые могут находиться в другом облаке (Облако *i*) для получения нужной информации;

F – обработка поступившего запроса в Облако *i* и подготовка ответа (время подготовки ответа занимает незначительное время по отношению к времени обработки запроса; данное макросостояние может быть декомпозировано на несколько макросостояний);

G – обработка/анализ ответа о тех или иных параметрах цифрового профиля от подсистем ИСПДн из другого облака.

Будем считать, что с вероятностью b_1 ПДн в БД Облака 1 достаточно и из макросостояния C процесс переходит в макросостояние D для формирования ответа на запрос. В противном случае с дополнительной вероятностью $\overline{b_1}$ для получения необходимых данных формируется запрос к внешним подсистемам ИСПДн в другом облаке (макросостояние E). В результате обработки ответа от внешних подсистем ИСПДн (макросостояние G) полученные данные являются достаточными с вероятностью b_2, либо может потребоваться повторный запрос с вероятностью $\overline{b_2}$ в одну из внешних подсистем ИСПДн» [171]. Граф переходов между макросостояниями процесса обработки запроса на поиск ПДн представлен на рисунке 3.1.

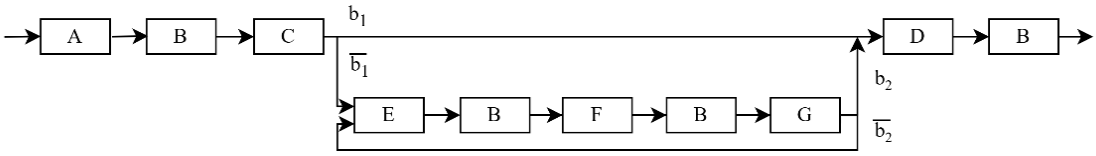


Рисунок 3.1 – Граф переходов между макросостояниями процесса обработки запроса на поиск ПДн

Далее для анализа показателей эффективности организации обслуживания запросов в ИСПДн с мультиоблачной архитектурой (в частности, использование ресурсов) предлагается и исследуется однолинейная система конечной ёмкости в дискретном времени с ординарным неоднородным поступающим потоком заявок, распределенным по геометрическому закону, с фазовым распределением процесса обслуживания.

Выбор данной модели объясняется тем, что передача запросов к персональным данным реализуется с помощью технологий с коммутацией пакетов, которые используются в современных информационно-телекоммуникационных

сетях. Это делает проблематичным использование для их исследования моделей СМО в непрерывном времени (пуассоновский входящий поток и экспоненциальное время обслуживания). Отметим, что дискретные СМО функционируют в дискретном времени, которое измеряется в фиксированных интервалах (тактах). Каждое макросостояние образуется микросостояниями, длительность каждого из которых – один такт дискретного времени. Случайные величины времени пребывания запроса в каждом макросостоянии могут быть описаны разными вариантами распределения. Воспользуемся утверждением, что «время t_B обработки запроса в макросостоянии B описывается геометрическим распределением (Geom), а время t_F в макросостоянии F – дискретным распределением Кокса (ED)» [58,60]. Используем «типовые варианты распределений в дискретном времени, которыми могут описываться случайные величины времени пребывания в макросостояниях из множества S» [58,60,171]. Если в графе, представленном на рисунке 3.1, макросостояния заменить на модели генерации распределений случайных величин времени пребывания в этих макросостояниях, тогда «случайные величины общего времени обработки запроса можно описать распределением фазового типа. Таким образом, в общем случае случайные величины времени пребывания процесса обработки запроса в любом макросостоянии можно описать распределением фазового типа в дискретном времени (PHD)» [60]. Предположим, что длительность каждого из микросостояний (образующих макросостояние) – один такт дискретного времени длительностью $h,\ h > 0$. Все возможные изменения в системе происходят в моменты времени $nh,\ n = 1,2,\ldots$.

3.2. Построение аналитической модели функционирования информационной системы при обработке запросов к персональным данным

В предлагаемой далее в качестве модели СМО будем под заявкой рассматривать запрос определённого типа на осуществление действий с персональными данными, рассмотренные в разделе 2.4 данной работы; для каждого типа заявки разрабатывается сценарий обработки; в качестве прибора

рассматривается ИСПДн как совокупность облаков; в качестве этапов обработки заявки – отдельные облака из H облаков в ИСПДн, в которых реализуются процессы обработки запросов к персональным данным в соответствии с регламентами сценариев; буферный накопитель (БН) – сервер буферизации запросов и управления доступом к сервисам (облакам). Входящий поток характеризуется случайными моментами поступления заявок в систему и типом поступающей заявки. Отметим, что в предлагаемой модели принято следующее допущение: облако – совокупность ресурсов, задействованных для обработки запросов к персональным данным; канал передачи данных при организации межоблачной связи принят в качестве абсолютно надёжного, поэтому не учитывается.

Будем считать, что на систему поступают заявки N-типов с интервалами, распределенными по геометрическому закону со средним $1/a$ $(0<a<1)$; поступившая заявка является i-заявкой, соответствующей запросу одного из рассматриваемых типов, $a_i = g_i a$, с вероятностью g_i $(i=\overline{1,N})$, $g_\cdot = 1$ («точка вместо индекса означает полную сумму переменной по этому индексу» [60]).

Будем полагать, что БН для хранения заявок имеет конечную ёмкость равную r $(r<\infty)$. Одновременно в системе может находиться общее число заявок равное $R = r+1$. Введём следующее допущение: поступившая на переполненную СМО заявка получает отказ и не оказывает влияния на дальнейшее функционирование системы и входящий поток.

Считаем, что окончание обслуживания заявки происходит раньше поступления заявки в БН в случае наступления этих событий в одном такте постоянной длины h в силу того, что последовательность событий в системе имеет значение, т.к. $r<\infty$.

Рассмотрим функционирование СМО при следующей последовательности событий в момент nh:

- окончание обслуживания заявки;
- поступление заявки из БН на обслуживание;

- освобождение БН от одной заявки;
- поступление новой заявки в БН;
- фиксация состояния системы.

Для лучшего понимания функционирования рассматриваемой СМО в дискретном времени на рисунке 3.2 представлена диаграмма последовательности событий.

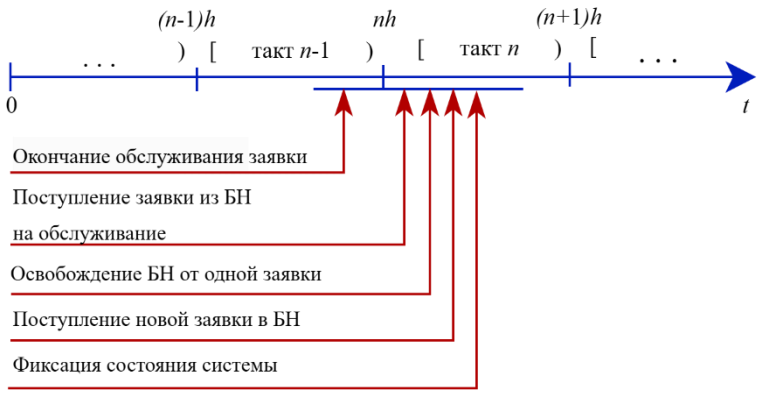


Рисунок 3.2 – Диаграмма последовательности событий в СМО в дискретном времени

В разработанной СМО распределение длительности обслуживания *i*-заявки, соответствующей запросу одного из рассматриваемых типов, на приборах фазового типа с PHD-представлением $(c_i, \mathbf{B}_i)$ порядка $K_i\,(i=\overline{1,N})$, $K=1,2,3,...,H$, с параметрами $\mathbf{c}^T=\left(c_1,c_2,...,c_K\right)$ постановки на этапы, $c_i\geq 0;\ i=\overline{1,K};\ c.=1;$ $\mathbf{B}=\left\|b_{ij}\right\|_{i,j=\overline{1,K}}$ – субстохастической матрицей переходов между этапами такой, что $\mathbf{d}=\left(d_1,d_2,...,d_K\right)^T=\left(\mathbf{I}-\mathbf{B}\right)\mathbf{1}\neq 0$ [11,60,171]. Соответственно, вероятность обслуживания в течение *l* тактов вычисляется по формуле, приведённой в [11,60]:

$$s_l=\boldsymbol{c}^T\boldsymbol{B}^{l-1}\boldsymbol{d},\ l=1,2,3,... \qquad (3.1)$$

Таким образом, рассматриваемая СМО ИСПДн с мультиоблачной архитектурой относится к классу $Geom_N\left|PHD_N\right|1\left|r<\infty\right|f_0$, где f_0 – множество бесприоритетных дисциплин выбора заявок из БН на обслуживание. Предлагаемая однолинейная СМО в дискретном времени с ординарным неоднородным поступающим потоком заявок разного типа, распределенным по геометрическому закону, с распределением длительности обслуживания фазового типа в дискретном времени и БН конечной ёмкости приведена на рисунке 3.3.

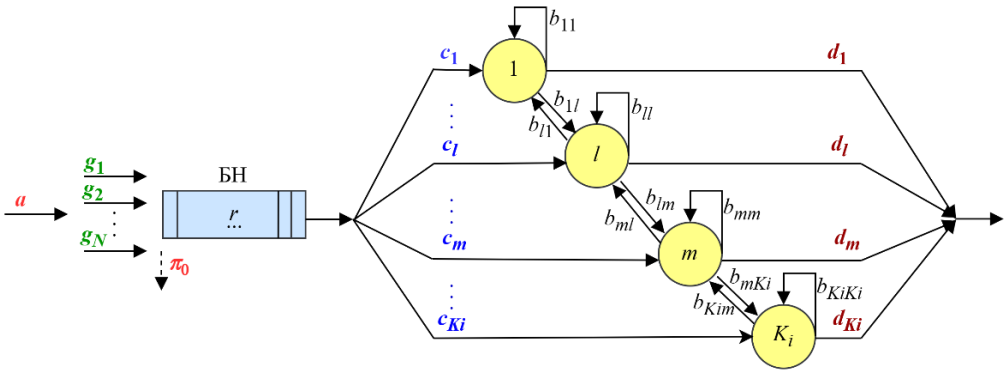


Рисунок 3.3 – Однолинейная СМО в дискретном времени $Geom_N\left|PHD_N\right|1\left|r<\infty\right|f_0$, с N типами заявок, K этапами

Функционирование предложенной СМО $Geom_N\left|PHD_N\right|1\left|r<\infty\right|f_0$ описывается «однородной цепью Маркова φ_n по моментам $nh\,(n\geq 0)$, над пространством состояний: $X=\left\{(0),(i,k,q):k=\overline{1,K_i},\ i=\overline{1,N},\ q=\overline{1,R}\right\}$, где (0) – отсутствие заявок в СМО, i – номер типа обслуживаемой заявки, k – номер этапа, на котором находится i-заявка, q – общее число заявок в системе. В сделанных предположениях $\varphi_n\,(n\geq 0)$, неразложима и апериодична, поэтому стационарное распределение вероятностей существует» [11,58,60].

Пусть **P** – матрица переходных вероятностей рассматриваемой цепи Маркова для пространства состояний X, **I** – единичная матрица, $\mathbf{0}^T = (0,...,0)$, $\mathbf{1}^T = (1,...,1)$.

Стационарное распределение вероятностей можно найти из системы уравнений равновесия (СУР):

$$
\begin{aligned}
&-ap_0 + \bar{a}\sum_{i=1}^{N}\mathbf{p}_{i1}^T\mathbf{d}_i = 0;\\
&\mathbf{p}_{iq}^T\left(\bar{a}\mathbf{B}_i - \mathbf{I}\right) + u\left(2-q\right)a_i p_0\mathbf{c}_i^T + u\left(q-1\right)a\mathbf{p}_{i,q-1}^T\mathbf{B}_i + a_i\sum_{j=1}^{N}\left(\mathbf{p}_{jq}^T\mathbf{d}_j\right)\mathbf{c}_i^T +\\
&+\bar{a}g_i\sum_{j=1}^{N}\left(\mathbf{p}_{j,q+1}^T\mathbf{d}_j\right)\mathbf{c}_i^T = 0,\ \text{где } q=\overline{1,r};\ i=\overline{1,N};\ i\neq j;\\
&\mathbf{p}_{iR}^T\left(\mathbf{B}_i - \mathbf{I}\right) + a\mathbf{p}_{i,R-1}^T\mathbf{B}_i + a_i\sum_{j=1}^{N}\left(\mathbf{p}_{jR}^T\mathbf{d}_j\right)\mathbf{c}_i^T = 0,\ \text{где } i=\overline{1,N};\ i\neq j;
\end{aligned}
\tag{3.2}
$$

и нормировочного условия:

$$
p_0 + \sum_{i=1}^{N}\sum_{q=1}^{R}\mathbf{p}_{iq}^T 1 = 1, \tag{3.3}
$$

где

$$
\mathbf{p}_{iq}^T = \left(p_{i1q}, p_{i2q}, ..., p_{iKq}\right);
$$

$$
\mathbf{d}_i = \left(\mathbf{I} - \mathbf{B}_i\right)\mathbf{1};
$$

$$
u\left(q\right) = \begin{cases} 0, & q \le 0; \\ 1, & q > 0; \end{cases}
$$

размерности $\mathbf{I} = diag\left\{1,1,...,1\right\}$ и $\mathbf{1}^T = \left(1,1,...,1\right)$ ясны из контекста.

Нахождение стационарного распределения вероятностей из (3.2) и нормировочного условия (3.3) позволит получить основные вероятностно-временные характеристики (ВВХ) функционирования ИСПДн при обслуживании заявок на обработку ПДн. Рассмотрим алгоритм решения СУР.

3.3. Алгоритм решения СУР для расчёта вероятностно-временных характеристик

Для снижения трудоёмкости решения СУР (3.2) и (3.3) проведём следующие преобразования этих формул, ориентированных на использование вычислительной техники.

Шаг 1. Определим:

$$\mathbf{B} = diag\{\mathbf{B}_1, \mathbf{B}_2, ..., \mathbf{B}_N\},\ \mathbf{c}^T = \left(g_1\mathbf{c}_1^T, g_2\mathbf{c}_2^T, ..., g_N\mathbf{c}_N^T\right),\ \mathbf{d}^T = \left(\mathbf{d}_1^T, \mathbf{d}_2^T, ..., \mathbf{d}_N^T\right);$$

$$\mathbf{p}_q^T = \left(\mathbf{p}_{1q}^T, \mathbf{p}_{2q}^T, ..., \mathbf{p}_{Nq}^T\right),\ q = \overline{1,R}.$$

Шаг 2. Рассчитаем при введённых ограничениях (φ_n $(n \geq 0)$, неразложима и апериодична, поэтому стационарное распределение вероятностей существует [11,58]) стационарное распределение **p** по следующим формулам:

$$p_0 = \left[\mathbf{v}\left(\mathbf{I} + \sum_{q=2}^{r}\mathbf{W}^{q-1} + \mathbf{W}^r\tilde{\mathbf{W}}\right)1\right]^{-1}; \tag{3.4}$$

$$\mathbf{p}_q^T = \begin{cases} p_0\mathbf{v}, & q = 1, \\ p_0\mathbf{v}\mathbf{W}^{q-1}, & q = \overline{2,r}, \\ p_0\mathbf{v}\mathbf{W}^r\tilde{\mathbf{W}}, & q = R \end{cases} \tag{3.5}$$

где

$$\mathbf{v} = a\mathbf{c}^T\mathbf{H}^{-1}(\overline{a}),$$

$$\mathbf{W} = a\mathbf{B}\mathbf{H}^{-1}(\overline{a}),$$

$$\tilde{\mathbf{W}} = a\mathbf{B}\left(\mathbf{I} + \frac{a}{\overline{a}}1\mathbf{c}^T\right)\mathbf{H}^{-1}(1);$$

$$\mathbf{H}^{-1}(z) = (\mathbf{I} - z\mathbf{B})^{-1} + \frac{\overline{z}}{\sum_{i=1}^{N} g_i B_i(z)}(\mathbf{I} - z\mathbf{B})^{-1}1\mathbf{c}^T(\mathbf{I} - z\mathbf{B})^{-1};$$

$$B_i(z) = z\mathbf{c}_i^T(I - z\mathbf{B}_i)^{-1}\mathbf{d}_i,\ i = \overline{1,N}.$$

Шаг 3. Вычислив по (3.4) и (3.5) стационарное распределение вероятностей, рассчитаем основные ВВХ для оценки эффективности использования ресурсов ИСПДн для обслуживания заявок на обработку персональных данных.

Вероятность $\pi_{потерь}$ потерь заявок в системе:

$$\pi_{потерь} = \mathrm{p}_R . \tag{3.6}$$

Доля потерянных заявок $Q_{потерь}$ в системе за такт:

$$Q_{потерь} = a\mathrm{p}_R . \tag{3.7}$$

Среднее время T пребывания заявки в системе рассчитывается по формуле Литтла:

$$T = \frac{Q}{a(1-p_R)}, \text{ где} \tag{3.8}$$

$Q = \sum_{q=1}^{R} q \sum_{i=1}^{N} \sum_{k=1}^{K} p_{iqk}$ - среднее число заявок в системе;

$p_R = \sum_{i=1}^{N} \sum_{k=1}^{K} p_{iRk}$.

Вероятность $\pi_{простоя}$ простоя системы:

$$\pi_{простоя} = p_0 . \tag{3.9}$$

Коэффициент U использования системы:

$$U = 1 - p_0 . \tag{3.10}$$

3.4. Анализ вероятностно-временных характеристик функционирования информационной системы с мультиоблачной архитектурой при обработке персональных данных

Будем рассматривать представленные выше ВВХ в качестве основных показателей эффективности функционирования ИСПДн при обработке запросов, касающихся информации о персональных данных. Для получения численных

результатов и их анализа был разработан программный комплекс на языке MatLab [115].

Рассмотрим следующие варианты организации мультиоблачной архитектуры ИСПДн для получения полной, точной, достоверной информации о субъекте ПДн:

- вариант С1 – ИСПДн организована на базе единственного корпоративного облака (вырожденная мультиоблачная (централизованная) архитектура);
- вариант С2 – ИСПДн организована на базе двух корпоративных облаков (территориально распределённая архитектура);
- ИСПДн организована на базе двух корпоративных и n внешних облаках, сервисные ресурсы которых в случае необходимости используются для получения информации о субъекте ПДн (мультиоблачная архитектура): вариант С3 $n = 1$; вариант С4 $n = 3$; вариант С5 $n = 3$.

Расчеты ВВХ (3.6) – (3.10) проводились для функционирования ИСПДн рассматриваемых вариантов архитектур при двух разных сценариях.

Сценарий А. Предположим, что i-заявка с равной вероятностью c_i попадает на обработку на любой этап k из K этапов. Тогда заявка при обслуживании будет последовательно проходить все этапы, пока не будет получен требуемый результат (ответ на запрос). На рисунке 3.4 приводится алгоритм функционирования ИСПДн с мультиоблачной архитектурой при обработке запроса на поиск информации о персональных данных по сценарию А.

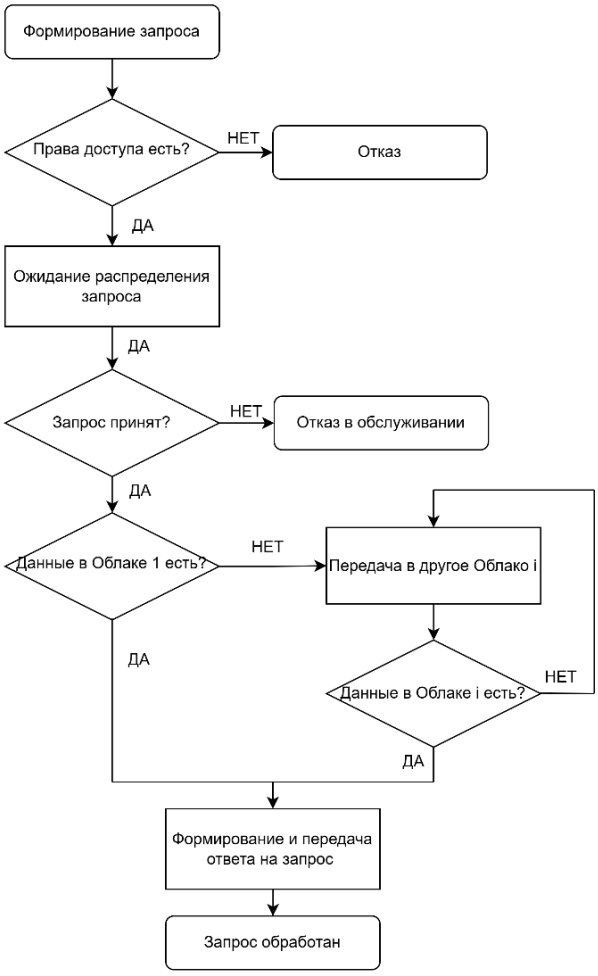


Рисунок 3.4 – Обобщённый алгоритм функционирования ИСПДн при обработке запроса на поиск информации о персональных данных по сценарию А

На рисунках 3.5 – 3.9 представлены графики для рассчитанных показателей (3.6) – (3.10) исследуемых вариантов организации ИСПДн с мультиоблачной архитектурой при изменении вероятности поступления a заявки за такт для сценария А.

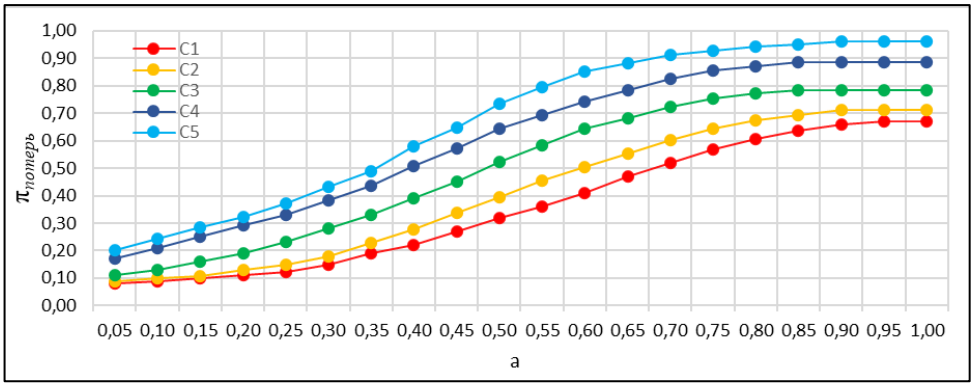


Рисунок 3.5 – Зависимость вероятности потерь заявок ($\pi_{потерь}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий А)

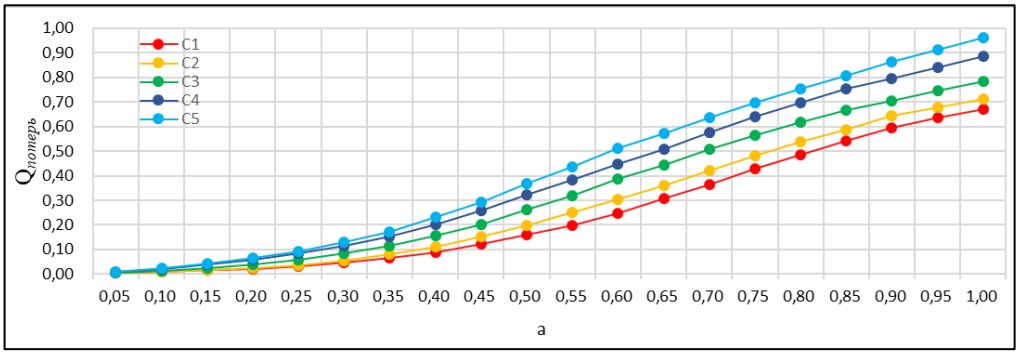


Рисунок 3.6 – Зависимость доли потерянных заявок за такт ($Q_{потерь}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий А)

Результаты расчётов представлены в таблицах 3.1 – 3.2.

Таблица 3.1 – Результаты расчётов $\pi_{потерь}$ для сценария А

a	$\pi_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,0801	0,0891	0,1106	0,1709	0,2009
0,10	0,0895	0,0990	0,1307	0,2111	0,2450
0,15	0,1012	0,1089	0,1608	0,2513	0,2842
0,20	0,1103	0,1287	0,1910	0,2915	0,3234
0,25	0,1211	0,1485	0,2312	0,3317	0,3724
0,30	0,1504	0,1782	0,2814	0,3819	0,4312
0,35	0,1895	0,2277	0,3317	0,4372	0,4900
0,40	0,2198	0,2772	0,3920	0,5075	0,5782
0,45	0,2701	0,3366	0,4523	0,5729	0,6468
0,50	0,3197	0,3960	0,5226	0,6432	0,7330
0,55	0,3612	0,4554	0,5829	0,6935	0,7936
0,60	0,4103	0,5049	0,6432	0,7437	0,8526
0,65	0,4711	0,5544	0,6834	0,7839	0,8820
0,70	0,5189	0,6039	0,7236	0,8241	0,9114
0,75	0,5701	0,6435	0,7538	0,8543	0,9290
0,80	0,6079	0,6732	0,7739	0,8697	0,9408
0,85	0,6378	0,6930	0,7839	0,8844	0,9506
0,90	0,6596	0,7138	0,7839	0,8844	0,9604
0,95	0,6701	0,7138	0,7839	0,8844	0,9604
1,00	0,6701	0,7138	0,7839	0,8844	0,9604

Таблица 3.2 – Результаты расчёта $Q_{потерь}$ для сценария А

a	$Q_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,0040	0,0045	0,0055	0,0085	0,0100
0,10	0,0090	0,0099	0,0131	0,0211	0,0245
0,15	0,0152	0,0163	0,0241	0,0377	0,0426
0,20	0,0221	0,0257	0,0382	0,0583	0,0647
0,25	0,0303	0,0371	0,0578	0,0829	0,0931
0,30	0,0451	0,0535	0,0844	0,1146	0,1294
0,35	0,0663	0,0797	0,1161	0,1530	0,1715
0,40	0,0879	0,1109	0,1568	0,2030	0,2313
0,45	0,1215	0,1515	0,2035	0,2578	0,2911
0,50	0,1599	0,1980	0,2613	0,3216	0,3665
0,55	0,1987	0,2505	0,3206	0,3814	0,4365
0,60	0,2462	0,3029	0,3859	0,4462	0,5116
0,65	0,3062	0,3604	0,4442	0,5095	0,5733

Продолжение таблица 3.2

a	$Q_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,70	0,3632	0,4227	0,5065	0,5769	0,6380
0,75	0,4276	0,4826	0,5653	0,6407	0,6968
0,80	0,4863	0,5386	0,6191	0,6958	0,7526
0,85	0,5421	0,5891	0,6663	0,7517	0,8080
0,90	0,5936	0,6424	0,7055	0,7960	0,8644
0,95	0,6366	0,6781	0,7447	0,8402	0,9124
1,00	0,6701	0,7138	0,7839	0,8844	0,9604

Рисунки 3.5 и 3.6 подтверждают, что рассматриваемые варианты системы с различными вариантами архитектур (C1 – C5) действительно являются системами с отказами, приводящими к потере заявок на обработку персональных данных. При этом наиболее устойчивой к потерям выглядит вариант C1, варианты C4 и C5 худшие по этому параметру (рисунок 3.5). Можно отметить, что с увеличением количества облаков потери возрастают. Такое поведение системы при различных вариантах архитектур может объясняться тем, что в вариантах C4 и C5 больше этапов обработки заявки, что приводит к увеличению времени, когда в БН не поступают новые заявки, и они теряются. Однако в реальных условиях функционирования ИСПДн с мультиоблачной архитектурой вполне допустимо, что вычислительные мощности облаков (варианты C3, C4 и C5), намного превышают мощности ИСПДн, построенной по вариантам C1 и C2, и тогда, соответственно, потери в таких системах (варианты C3, C4, C5) возникают при значительно большей поступающей нагрузке, чем в системах, построенным по другим вариантам (C1 и C2). Кроме того, системы с архитектурой по вариантам C1, C2 обладают низкой, по сравнению с другими вариантами, отказоустойчивостью. Мультиоблачные архитектуры вариантов C3, C4, C5 наиболее предпочтительны с точки зрения высокой отказоустойчивости и доступности за счёт возможности в подобных информационных системах оперативного перераспределения рабочих нагрузок с одного облака на другое и реализации технологии адаптивной отказоустойчивости.

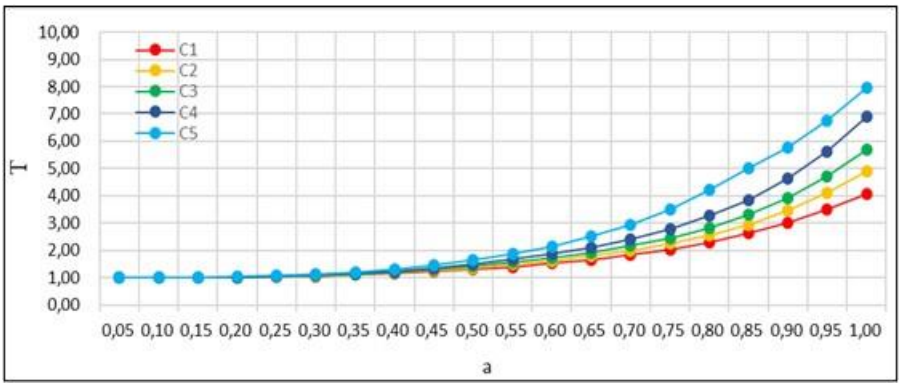


Рисунок 3.7 – Зависимость среднего времени пребывания заявки в системе (T) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий А)

Результаты расчётов представлены в таблице 3.3.

Таблица 3.3 – Результаты расчёта T для сценария А

a	***T***				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	1,00	1,00	1,00	1,00	1,00
0,10	1,00	1,00	1,00	1,00	1,00
0,15	1,00	1,00	1,00	1,01	1,01
0,20	1,01	1,01	1,01	1,02	1,03
0,25	1,03	1,03	1,03	1,05	1,07
0,30	1,06	1,07	1,08	1,10	1,13
0,35	1,10	1,12	1,13	1,17	1,21
0,40	1,15	1,18	1,20	1,25	1,32
0,45	1,22	1,26	1,30	1,36	1,46
0,50	1,30	1,36	1,42	1,50	1,65
0,55	1,40	1,48	1,56	1,67	1,87
0,60	1,52	1,62	1,72	1,87	2,15
0,65	1,66	1,79	1,92	2,12	2,50
0,70	1,84	2,00	2,16	2,42	2,95
0,75	2,04	2,25	2,45	2,78	3,50
0,80	2,30	2,56	2,82	3,26	4,20
0,85	2,62	2,95	3,30	3,85	5,00
0,90	3,02	3,45	3,90	4,65	5,78
0,95	3,50	4,10	4,70	5,60	6,75
1,00	4,05	4,90	5,70	6,90	7,95

Анализ тенденций зависимостей на рисунке 3.7 показывает, что заявка обрабатывается при варианте С1 быстрее, чем при других вариантах: во-первых, этапов обработки меньше и, во-вторых, не требуется интеграция и синхронизация сервисов различных поставщиков облачных услуг, которые могут приводить к задержкам при обработке данных.

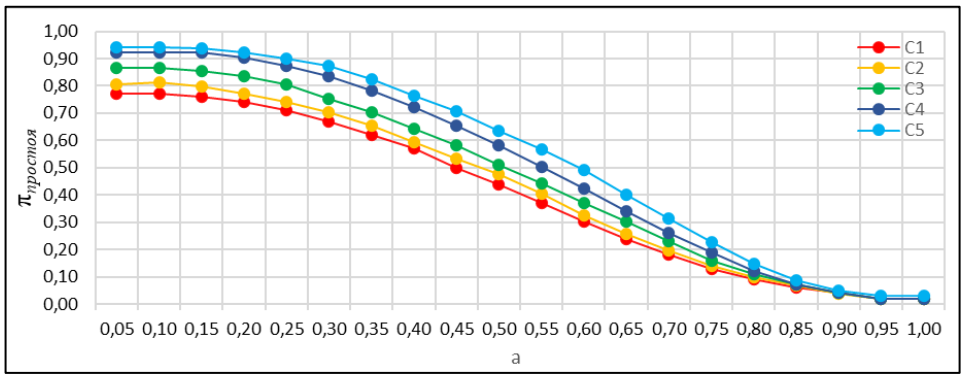


Рисунок 3.8 – Зависимость вероятности простоя системы ($\pi_{простоя}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий А)

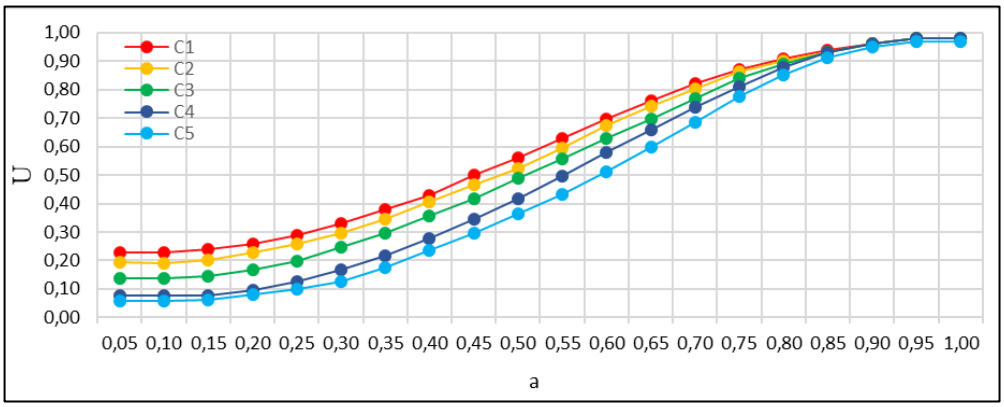


Рисунок 3.9 – Зависимость коэффициента использования системы (U) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий А)

Результаты расчётов представлены в таблицах 3.4 – 3.5.

Таблица 3.4 – Результаты расчёта $\pi_{простоя}$ для сценария А

a	$\pi_{простоя}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,7701	0,8066	0,8643	0,9246	0,9408
0,10	0,7719	0,8113	0,8643	0,9246	0,9408
0,15	0,7605	0,7970	0,8543	0,9246	0,9386
0,20	0,7408	0,7722	0,8342	0,9045	0,9212
0,25	0,7107	0,7425	0,8040	0,8744	0,9016
0,30	0,6688	0,7029	0,7538	0,8342	0,8722
0,35	0,6206	0,6534	0,7035	0,7839	0,8232
0,40	0,5704	0,5940	0,6432	0,7236	0,7644
0,45	0,4997	0,5346	0,5829	0,6533	0,7056
0,50	0,4407	0,4752	0,5126	0,5829	0,6370
0,55	0,3702	0,4059	0,4422	0,5025	0,5684
0,60	0,3034	0,3267	0,3719	0,4221	0,4900
0,65	0,2403	0,2574	0,3015	0,3417	0,4018
0,70	0,1801	0,1980	0,2312	0,2613	0,3136
0,75	0,1289	0,1386	0,1608	0,1910	0,2254
0,80	0,0907	0,0990	0,1106	0,1206	0,1470
0,85	0,0602	0,0693	0,0704	0,0704	0,0882
0,90	0,0404	0,0396	0,0402	0,0402	0,0490
0,95	0,0201	0,0198	0,0201	0,0201	0,0294
1,00	0,0201	0,0198	0,0201	0,0201	0,0294

Таблица 3.5 – Результаты расчёта U для сценария А

a	***U***				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,2299	0,1934	0,1357	0,0754	0,0592
0,10	0,2281	0,1887	0,1357	0,0754	0,0592
0,15	0,2395	0,2031	0,1458	0,0754	0,0614
0,20	0,2592	0,2278	0,1659	0,0955	0,0788
0,25	0,2893	0,2575	0,1960	0,1257	0,0984
0,30	0,3312	0,2971	0,2463	0,1659	0,1278
0,35	0,3794	0,3466	0,2965	0,2161	0,1768
0,40	0,4296	0,4060	0,3568	0,2764	0,2356
0,45	0,5003	0,4654	0,4171	0,3468	0,2944
0,50	0,5593	0,5248	0,4875	0,4171	0,3630
0,55	0,6298	0,5941	0,5578	0,4975	0,4316
0,60	0,6966	0,6733	0,6282	0,5779	0,5100
0,65	0,7597	0,7426	0,6985	0,6583	0,5982
0,70	0,8199	0,8020	0,7689	0,7387	0,6864

Продолжение таблицы 3.5

a	*U*				
	C1	**C2**	**C3**	**C4**	**C5**
0,75	0,8711	0,8614	0,8392	0,8091	0,7746
0,80	0,9093	0,9010	0,8895	0,8794	0,8530
0,85	0,9398	0,9307	0,9297	0,9297	0,9118
0,90	0,9596	0,9604	0,9598	0,9598	0,9510
0,95	0,9799	0,9802	0,9799	0,9799	0,9706
1,00	0,9799	0,9802	0,9799	0,9799	0,9706

Рисунки 3.8 и 3.9 демонстрируют, что при всех вариантах архитектур при увеличении *a* наблюдается тенденция уменьшения вероятности простоя системы, рисунок 3.8, и увеличения коэффициента использования, рисунок 3.9. Однако при этом при архитектуре по варианту C1 коэффициент использования, рисунок 3.9, выше, чем при других вариантах. Варианты C2 и C3 показывают приблизительно одинаковую тенденцию. Наибольшая вероятность простоя и низкий показатель использования системы прослеживается при архитектуре по вариантам C4 и C5. При увеличении числа облаков вероятность того, что для обработки заявки будут использованы все облака, уменьшается, и, соответственно, снижается коэффициент использования системы.

Проведенный анализ показал, что при таком подходе к обработке запросов к персональным данным (сценарий А) – без задания точного сценария порядка следования этапов обработки – ресурсы ИСПДн с мультиоблачной архитектурой используются неэффективно, что ведёт при увеличении количества облаков к увеличению: среднего времени обслуживания заявки, вероятности потерь и доли потерянных заявок за такт. При этом коэффициент использования системы снижается.

Для наиболее полного учёта преимуществ мультиоблачной архитектуры предлагается *сценарий Б*, предусматривающий ранжировку обрабатываемых запросов, исходя из типов запросов и категории персональных данных, с помощью классического метода экспертных оценок (данная задача не является предметом исследования данной диссертации). В этой ситуации вероятность c_i направления

заявки на k облако (этап) будет тем выше, чем функциональные возможности этого k облака больше соответствуют параметрам запроса. На рисунке 3.10 приводится алгоритм функционирования ИСПДн при обработке запроса на поиск информации о персональных данных по сценарию Б.

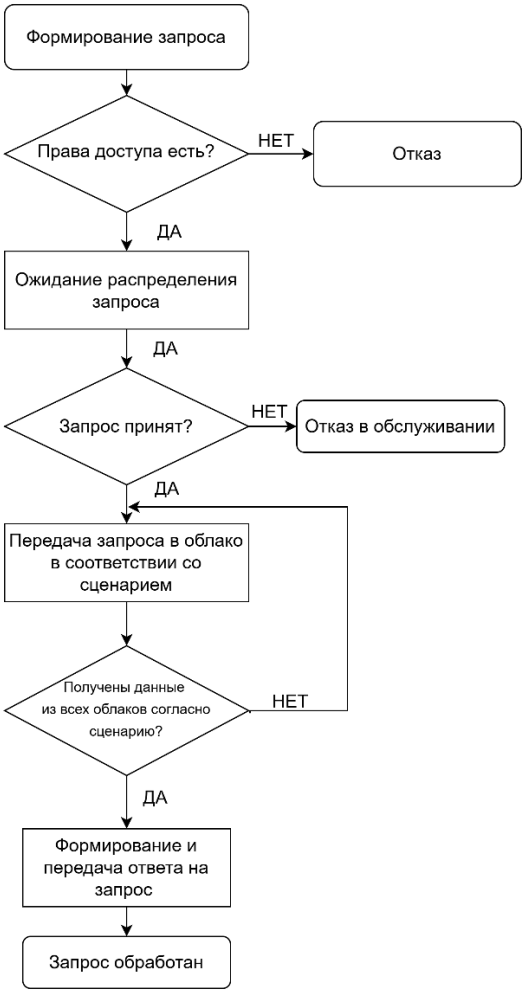


Рисунок 3.10 – Обобщённый алгоритм функционирования ИСПДн при обработке запроса на поиск информации о персональных данных по сценарию Б

Ниже, на рисунках 3.11 – 3.15, представлены графики для рассчитанных показателей по (3.6) – (3.10) исследуемых вариантов организации ИСПДн с мультиоблачной архитектурой при изменении вероятности поступления a заявки за такт для сценария Б.

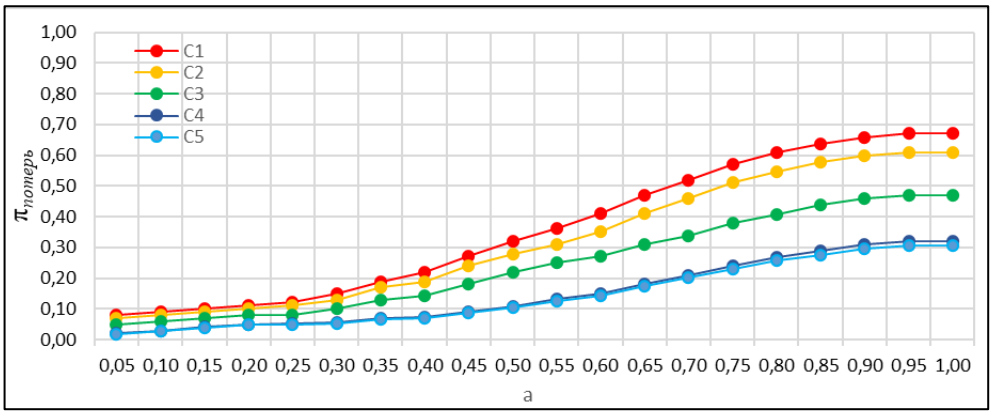


Рисунок 3.11 – Зависимость вероятности потерь заявок ($\pi_{потерь}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий Б)

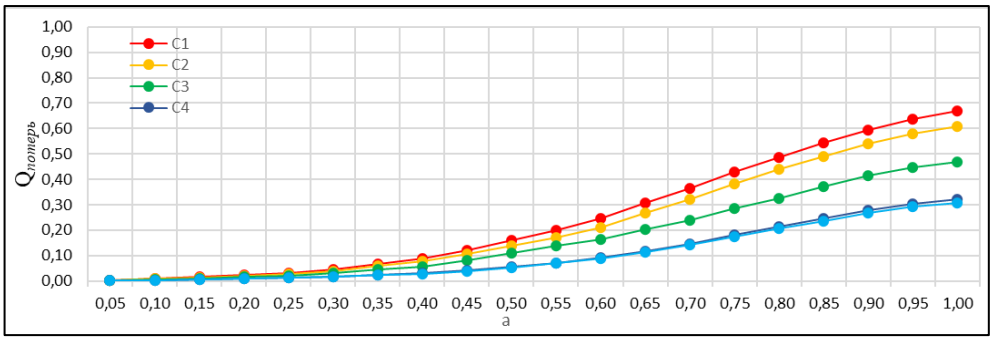


Рисунок 3.12 – Зависимость доли потерянных заявок за такт ($Q_{потерь}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий Б)

Результаты расчётов представлены в таблицах 3.6 – 3.7.

Таблица 3.6 – Результаты расчётов $\pi_{потерь}$ для сценария Б

a	$\pi_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,0801	0,0701	0,0501	0,0201	0,0193
0,10	0,0895	0,0795	0,0595	0,0295	0,0283
0,15	0,1012	0,0912	0,0712	0,0412	0,0396
0,20	0,1103	0,1003	0,0803	0,0503	0,0483
0,25	0,1211	0,1111	0,0811	0,0511	0,0491
0,30	0,1504	0,1304	0,1004	0,0563	0,0540
0,35	0,1895	0,1695	0,1295	0,0695	0,0667

Продолжение таблицы 3.6

a	$\pi_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,40	0,2198	0,1898	0,1426	0,0738	0,0708
0,45	0,2701	0,2401	0,1801	0,0901	0,0865
0,50	0,3197	0,2797	0,2197	0,1097	0,1053
0,55	0,3612	0,3112	0,2512	0,1312	0,1260
0,60	0,4103	0,3503	0,2703	0,1503	0,1443
0,65	0,4711	0,4111	0,3111	0,1811	0,1739
0,70	0,5189	0,4589	0,3389	0,2089	0,2005
0,75	0,5701	0,5101	0,3801	0,2401	0,2305
0,80	0,6079	0,5479	0,4079	0,2679	0,2572
0,85	0,6378	0,5778	0,4378	0,2878	0,2763
0,90	0,6596	0,5996	0,4596	0,3096	0,2972
0,95	0,6701	0,6101	0,4701	0,3201	0,3073
1,00	0,6701	0,6101	0,4701	0,3201	0,3073

Таблица 3.7 – Результаты расчёта $Q_{потерь}$ для сценария Б

a	$Q_{потерь}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,0040	0,0035	0,0025	0,0010	0,0010
0,10	0,0090	0,0080	0,0060	0,0030	0,0028
0,15	0,0152	0,0137	0,0107	0,0062	0,0059
0,20	0,0221	0,0201	0,0161	0,0101	0,0097
0,25	0,0303	0,0278	0,0203	0,0128	0,0123
0,30	0,0451	0,0391	0,0301	0,0169	0,0162
0,35	0,0663	0,0593	0,0453	0,0243	0,0234
0,40	0,0879	0,0759	0,0570	0,0295	0,0283
0,45	0,1215	0,1080	0,0810	0,0405	0,0389
0,50	0,1599	0,1399	0,1099	0,0549	0,0527
0,55	0,1987	0,1712	0,1382	0,0722	0,0693
0,60	0,2462	0,2102	0,1622	0,0902	0,0866
0,65	0,3062	0,2672	0,2022	0,1177	0,1130
0,70	0,3632	0,3212	0,2372	0,1462	0,1404
0,75	0,4276	0,3826	0,2851	0,1801	0,1729
0,80	0,4863	0,4383	0,3263	0,2143	0,2057
0,85	0,5421	0,4911	0,3721	0,2446	0,2348
0,90	0,5936	0,5396	0,4136	0,2786	0,2675
0,95	0,6366	0,5796	0,4466	0,3041	0,2919
1,00	0,6701	0,6101	0,4701	0,3201	0,3073

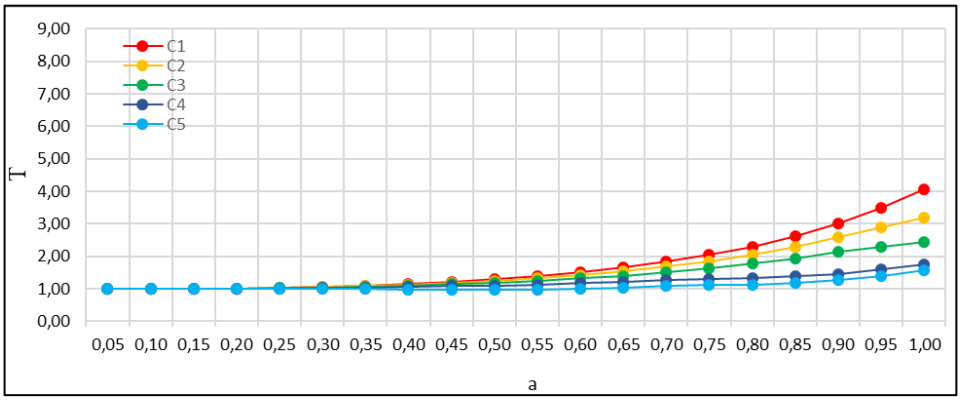


Рисунок 3.13 – Зависимость среднего времени пребывания заявки в системе (T) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий Б)

Результаты расчётов представлены в таблице 3.8.

Таблица 3.8 – Результаты расчёта T для сценария Б

a	***T***				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	1,00	1,00	1,00	0,99	0,99
0,10	1,00	1,00	1,00	0,99	0,99
0,15	1,00	1,00	1,00	0,99	0,99
0,20	1,01	1,01	1,01	1,00	0,99
0,25	1,03	1,03	1,03	1,01	0,99
0,30	1,06	1,05	1,04	1,02	0,99
0,35	1,10	1,08	1,07	1,03	0,99
0,40	1,15	1,12	1,10	1,05	0,98
0,45	1,22	1,18	1,14	1,08	0,98
0,50	1,30	1,24	1,18	1,10	0,96
0,55	1,40	1,32	1,24	1,13	0,98
0,60	1,52	1,42	1,32	1,17	1,01
0,65	1,66	1,53	1,40	1,20	1,02
0,70	1,84	1,68	1,52	1,26	1,08
0,75	2,04	1,83	1,63	1,30	1,12
0,80	2,30	2,04	1,78	1,34	1,13
0,85	2,62	2,29	1,94	1,39	1,20
0,90	3,02	2,59	2,14	1,46	1,26
0,95	3,50	2,90	2,30	1,60	1,40
1,00	4,05	3,20	2,45	1,76	1,56

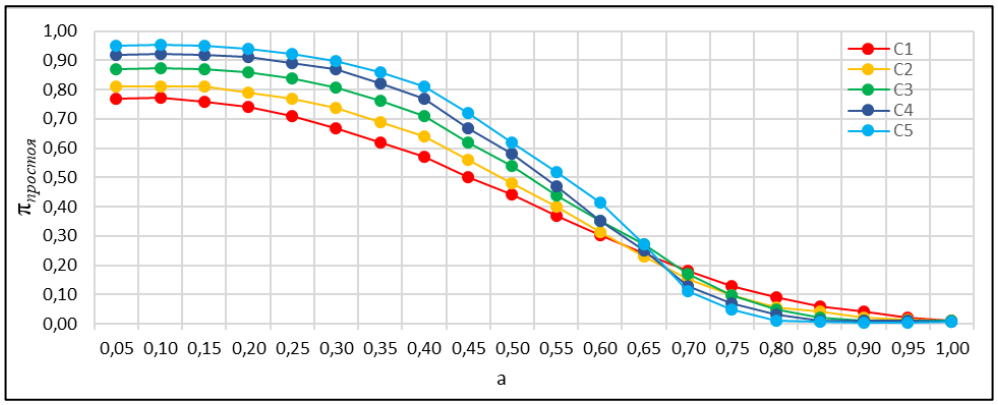


Рисунок 3.14 – Зависимость вероятности простоя системы ($\pi_{простоя}$) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий Б)

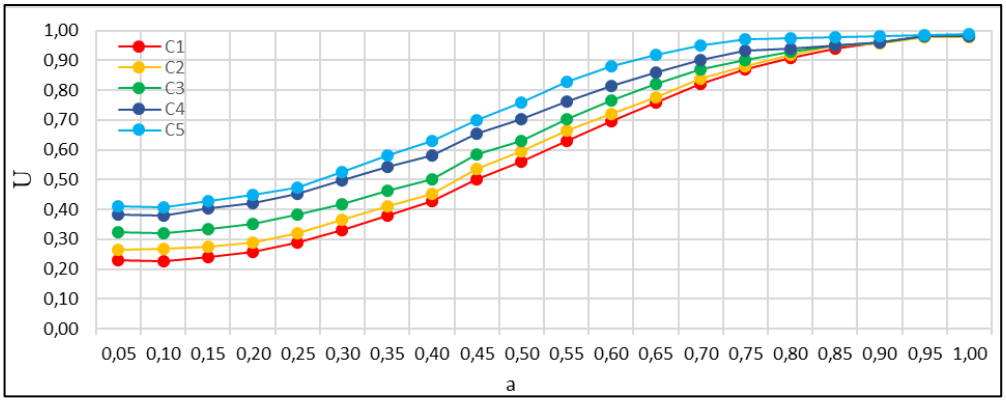


Рисунок 3.15 – Зависимость коэффициента использования системы (U) от вероятности a поступления заявки на СМО для вариантов организации мультиоблачной архитектуры ИСПДн (сценарий Б)

Результаты расчётов представлены в таблицах 3.9 – 3.10.

Таблица 3.9 – Результаты расчёта $\pi_{простоя}$ для сценария Б

a	$\pi_{простоя}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,7701	0,8101	0,8701	0,9201	0,9501
0,10	0,7719	0,8119	0,8719	0,9219	0,9519
0,15	0,7605	0,8105	0,8705	0,9205	0,9505
0,20	0,7408	0,7908	0,8597	0,9108	0,9408
0,25	0,7107	0,7707	0,8397	0,8907	0,9207
0,30	0,6688	0,7388	0,8088	0,8688	0,8988

Продолжение таблицы 3.9

a	$\pi_{простоя}$				
	C1	**C2**	**C3**	**C4**	**C5**
0,35	0,6206	0,6906	0,7606	0,8206	0,8606
0,40	0,5704	0,6404	0,7104	0,7704	0,8104
0,45	0,4997	0,5597	0,6197	0,6697	0,7197
0,50	0,4407	0,4807	0,5407	0,5807	0,6207
0,55	0,3702	0,4002	0,4402	0,4702	0,5202
0,60	0,3034	0,3134	0,3506	0,3534	0,4134
0,65	0,2403	0,2303	0,2703	0,2503	0,2703
0,70	0,1801	0,1529	0,1701	0,1301	0,1101
0,75	0,1289	0,0989	0,0989	0,0699	0,0489
0,80	0,0907	0,0576	0,0507	0,0319	0,0107
0,85	0,0602	0,0406	0,0202	0,0114	0,0065
0,90	0,0404	0,0216	0,0104	0,0104	0,0055
0,95	0,0201	0,0156	0,0098	0,0092	0,0025
1,00	0,0105	0,0099	0,0095	0,0089	0,0075

Таблица 3.10 – Результаты расчёта *U* для сценария Б

a	***U***				
	C1	**C2**	**C3**	**C4**	**C5**
0,05	0,2299	0,2664	0,3241	0,3844	0,4098
0,10	0,2281	0,2675	0,3205	0,3808	0,4063
0,15	0,2395	0,2760	0,3333	0,4036	0,4268
0,20	0,2592	0,2906	0,3526	0,4229	0,4484
0,25	0,2893	0,3211	0,3826	0,4530	0,4724
0,30	0,3312	0,3653	0,4162	0,4966	0,5255
0,35	0,3794	0,4122	0,4623	0,5427	0,5811
0,40	0,4296	0,4532	0,5024	0,5828	0,6309
0,45	0,5003	0,5352	0,5835	0,6539	0,7014
0,50	0,5593	0,5938	0,6312	0,7015	0,7586
0,55	0,6298	0,6655	0,7018	0,7621	0,8287
0,60	0,6966	0,7199	0,7651	0,8153	0,8816
0,65	0,7597	0,7768	0,8209	0,8611	0,9173
0,70	0,8199	0,8378	0,8710	0,9011	0,9512
0,75	0,8711	0,8808	0,9030	0,9332	0,9712
0,80	0,9093	0,9176	0,9292	0,9392	0,9729
0,85	0,9398	0,9489	0,9500	0,9500	0,9793
0,90	0,9596	0,9588	0,9594	0,9594	0,9799
0,95	0,9799	0,9796	0,9799	0,9799	0,9832
1,00	0,9799	0,9796	0,9799	0,9799	0,9899

Полученные результаты показывают, что сценарий Б более адекватно отражает поведение информационной системы с мультиоблачной архитектурой при обслуживании запросов к персональным данным. На графиках прослеживается тенденция снижения вероятности потерь в системе, рисунок 3.11, и доли потерянных заявок за такт, рисунок 3.12, при увеличении количества облаков в мультиоблачной архитектуре. Время пребывания заявки в системе также уменьшается с увеличением количества облаков, рисунок 3.13. При этом вероятность простоя при малой величине a выше у вариантов с большим количеством облаков. Коэффициент использования увеличивается с ростом a, рисунок 3.15. Отметим, что на всех графиках прослеживается, что система при вариантах С4 и С5 ведёт себя практически идентично, при этом коэффициент использования системы от вероятности a поступления заявки на СМО для варианта С5 отличается от аналогичного коэффициента для С4 не более чем на 2 процента. Следовательно, подключение в состав ИСПДн более двух внешних облаков нежелательно, поскольку это может привести к усложнению сценариев обработки запросов, увеличению времени обслуживания заявки (в том числе из-за увеличения количества межоблачных взаимодействий) и снижению коэффициента использования системы.

Выводы по третьей главе

1. Представление процесса обработки запроса к персональным данным в виде графа переходов между макросостояниями даёт возможность использовать в качестве модели рассматриваемого процесса однолинейную СМО конечной ёмкости в дискретном времени с ординарным неоднородным поступающим потоком заявок, распределённым по геометрическому закону.

2. Для построения аналитической модели функционирования ИСПДн предложено под заявкой рассматривать запрос на осуществление действий с персональными данными; в качестве прибора – ИСПДн как совокупность мультиоблаков; в качестве этапов обработки заявки рассматривать отдельные

облака из H облаков ИСПДн; буферный накопитель – сервер буферизации запросов и управления доступом к сервисам. Входящий поток характеризуется случайными моментами поступления заявок в систему и типами поступающих в эти моменты заявок. Такая декомпозиция системы и информационных процессов позволяют рассматривать ИСПДн как СМО класса $Geom_N \left| PHD_N \right| 1 \left| r < \infty \right| f_0$.

3. Построенная аналитическая модель функционирования информационной системы обработки запросов к персональным данным позволяет найти СУР. Это делает возможным расчёт основных ВВХ функционирования ИСПДн для оценки эффективности использования ресурсов ИСПДн при обслуживании заявок на обработку персональных данных, а именно: способность системы справляться с нагрузкой, время обработки заявок, эффективность загрузки системы.

4. Предложенный в диссертации алгоритм позволяет снизить трудоёмкость решения СУР и расчёта основных ВВХ путём преобразования СУР в вид, ориентированный на использование вычислительной техники, не менее, чем на 17%.

5. Проведённые расчёты ВВХ показали, что уже на этапе проектирования ИСПДн с мультиоблачной архитектурой не рекомендуется использовать более двух внешних облаков, поскольку это может привести к усложнению сценариев обработки запросов, увеличению времени обслуживания запроса (в том числе из-за увеличения количества межоблачных взаимодействий) и снижению коэффициента использования системы. При этом, при низкой загруженности ИСПДн будет наблюдаться простой системы и низкая её загрузка (избыточная архитектура). Кроме того, из-за усложнения процессов управления процессами обработки запросов в ИСПДн возрастают риски нарушения качества персональных данных.

6. Разработанные модель и алгоритм оценки эффективности ресурсов рекомендуется применять на этапе проектирования для обоснования выбора мультиоблачной архитектуры.

Глава 4. Разработка модели и алгоритма оценки рисков нарушения качества персональных данных при их обработке в информационной системе с мультиоблачной архитектурой

4.1. Декомпозиция ресурсов информационной системы при обработке запросов к персональным данным

Исследование современных тенденций развития архитектуры сложных территориально распределённых информационных систем, которые начинают применяться для обработки больших объёмов персональных данных, показало, что в данных системах начинается широкое применение технологий «больших данных» и методов машинного обучения, которые используются в качестве помощников при обработке персональных данных [48,55,60,117,125]. Кроме того, изменения в законодательных актах РФ [70,131,132,135,136], регламентирующих вопросы обработки персональных данных, сделали ещё более актуальным необходимость точного учёта категорий персональных данных, которые подлежат автоматизированной обработке. В частности, особое внимание уделяется такой категории, как биометрические ПДн [136], процесс обработки которых включает в себя их хранение и обработку в государственной информационной системе, к которой предъявляются свои особые требования [99,134]. Таким образом появляется новый класс облака в сложной мультиоблачной архитектуре ИСПДн – государственное облако. Это ведёт к появлению новых потенциальных рисков.

Перечисленное выше делает крайне актуальной рассмотренную далее в настоящей диссертации задачу оценки рисков нарушения качества ПДн при их обработке в ИСПДн с мультиоблачной архитектурой.

Рассмотрим подход к исследованию ИСПДн, позволяющий идентифицировать и снизить информационные риски, влияющие на её системную целостность. Автором предлагается в [67] декомпозиция архитектуры ИСПДн на уровни. Каждый уровень отвечает за обеспечение снижения рисков на отдельном этапе процесса обработки ПДн. На каждом уровне можно выделить актуальные

угрозы и определить соответствующие способы противодействия им. Автором предложены требования, «в соответствии с которыми производится построение многоуровневой модели ИСПДн, позволяющей осуществлять классификацию угроз по ее уровням:

- при декомпозиции ИСПДн на уровни должны рассматриваться не отдельные элементы ИСПДн, а ее функциональные типовые объекты, на которые может быть оказано воздействие;
- необходимо рассматривать не только ИСПДн, но и внешнюю по отношению к ней среду из-за наличия потенциальных воздействий за пределами ИСПДн» [67];
- требуется выделение и особый контроль потенциально ненадежных элементов, так как часть ИСПДн может быть построена на импортных средствах.

Для каждого уровня предлагаемой модели следует определить перечень собственных и редуцированных угроз персональным данным.

Будем рассматривать следующие три основных уровня модели ИСПДн [67]:

- аналитический;
- технологический;
- технический.

Технический уровень модели ИСПДн можно представить в виде совокупности следующих основных подуровней: внешняя среда (1), линии (каналы) связи (2), элементы ИСПДн (3), сетевое взаимодействие (4), вычислительные (5), программные (6) и информационные (7) ресурсы.

Совокупность подсистем ИСПДн и сегментов этих подсистем представлена на рисунке 4.1.

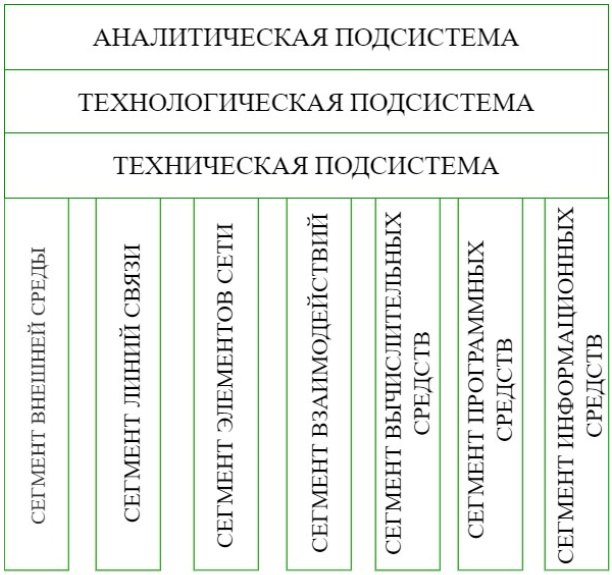


Рисунок 4.1 – Совокупность подсистем и сегментов ИСПДн

На аналитическом уровне решаются вопросы управления процессами ИСПДн и обеспечения их качественного функционирования.

На технологическом уровне решаются вопросы организации процессов функционирования ИСПДн для достижения целей её создания.

На техническом уровне решаются вопросы обеспечения эффективного функционирования линий связи, узлов сетевой инфраструктуры, вычислительных и программных ресурсов, а также вопросы надёжного информационного взаимодействия элементов сети и эффективной циркуляции информации.

Сегментами (подуровнями) технической подсистемы являются:

- сегмент внешней среды технической подсистемы (1);
- сегмент линий связи технической подсистемы (2);
- сегмент элементов сети технической подсистемы (3);
- сегмент, отвечающий за взаимодействие – как сетевое, так и межсетевое – технической подсистемы (4);
- сегмент вычислительных средств технической подсистемы (5);
- сегмент программных средств технической подсистемы (6);
- сегмент информационных средств технической подсистемы (7).

Сегмент (1) - рассматриваются проблемы обеспечения качественного функционирования элементов в пределах определённых физических пространств. ИСПДн.

Сегмент (2) - рассматриваются проблемы обеспечения функционирования линий связи и каналов передачи персональных данных, а также потенциальными негативными воздействиями на них. Отметим, что линии и каналы связи, по которым передаются персональные данные, могут проходить по неконтролируемой организацией территории.

Сегмент (3) - рассматриваются проблемы функционирования сетевой инфраструктуры ИСПДн с мультиоблачной архитектурой.

Сегмент (4) – рассматриваются задачи обеспечения надежного информационного взаимодействия элементов ИСПДн (в т.ч. техническая защита).

Сегмент (5) – рассматриваются задачи эффективного функционирования аппаратных ресурсов ИСПДн.

Сегмент (6) – рассматриваются задачи эффективного функционирования прикладного и специального ПО ИСПДн.

Сегмент (7) - рассматриваются проблемы эффективного обмена персональными данными, на которые и направлено воздействие злоумышленника в корпоративной ИСПДн.

Упомянутые сегменты (подуровни) могут быть подвержены потенциальным угрозам, реализация которых может привести к нарушению параметров качества функционирования элементов и (или) подсистем ИСПДн каждого уровня [170] и, как следствие, к нарушению качества ПДн. Предложенная классификация угроз персональным данным по уровням модели ИСПДн представлена в Приложении В настоящей диссертационной работы. На каждом уровне модели ИСПДн можно задать показатели оценки качества персональных данных - целостности, достоверности, полноты, адекватности, конфиденциальности и т.п.

Предложенная декомпозиция ресурсов ИСПДн позволяет на каждом уровне определить потенциальные риски персональных данных и разработать подход к их оценке и минимизации.

4.2. Разработка семантической модели оценки информационных рисков персональных данных при их автоматизированной обработке

Основная проблема, возникающая при построении математической модели оценки рисков нарушения качества ПДн в ИСПДн с мультиоблачной архитектурой, заключается в описании основных информационных процессов, которые должны наиболее точно описывать существующие бизнес- и технологические процессы и поддерживаться на современных вычислительных ресурсах [50,51,97,138,139,174].

Для формализации процесса оценки информационных рисков ПДн в ИСПДн с мультиоблачной архитектурой используем подход «к построению семантической модели проблемной области оценки рисков» [120-124] при автоматизированной обработке ПДн в ИСПДн с мультиоблачной архитектурой. Её выбор обусловлен тем, что она обеспечивает целостность системы поиска решений, которая даёт возможность сохранять целостность механизмов логических выводов и баз знаний [223].

Одним из преимуществ семантической модели является то, что её можно рассматривать с математической позиции – т.е. можно представить в виде графа со своими вершинами и дугами. Каждая вершина в ней — эквивалент элемента множества, а каждая дуга — предикат таких элементов. Также в таких графах выделяют подграфы − фреймы. Фреймы представляют из себя различные структуры, используемые для определения типов элементов математической модели и определения фрагментов знаний. Фреймы используют для рекурсивного задания типов математической модели, позволяющее предоставлять знания о проблемной области в виде естественной и структурной формы.

К основным недостаткам семантической модели можно отнести: слабое представление о структуре проблемной области; высокая сложность создания и модификации проблемной области и поиска решений; потребность в использовании специального аппарата формального вывода.

Преимущества семантической модели, к которым относятся универсальность применения, наглядность полученных результатов и близость к естественным

языкам, перекрывают её недостатки, указанные выше.

На рисунке 4.2 представлена предлагаемая семантическая модель для описания проблемной области оценки информационных рисков ПДн при их автоматизированной обработке в ИСПДн с мультиоблачной архитектурой. В основе данной модели использована разработанная автором в главе 1 настоящей диссертационной работы обобщенная схема воздействия на персональные данные.

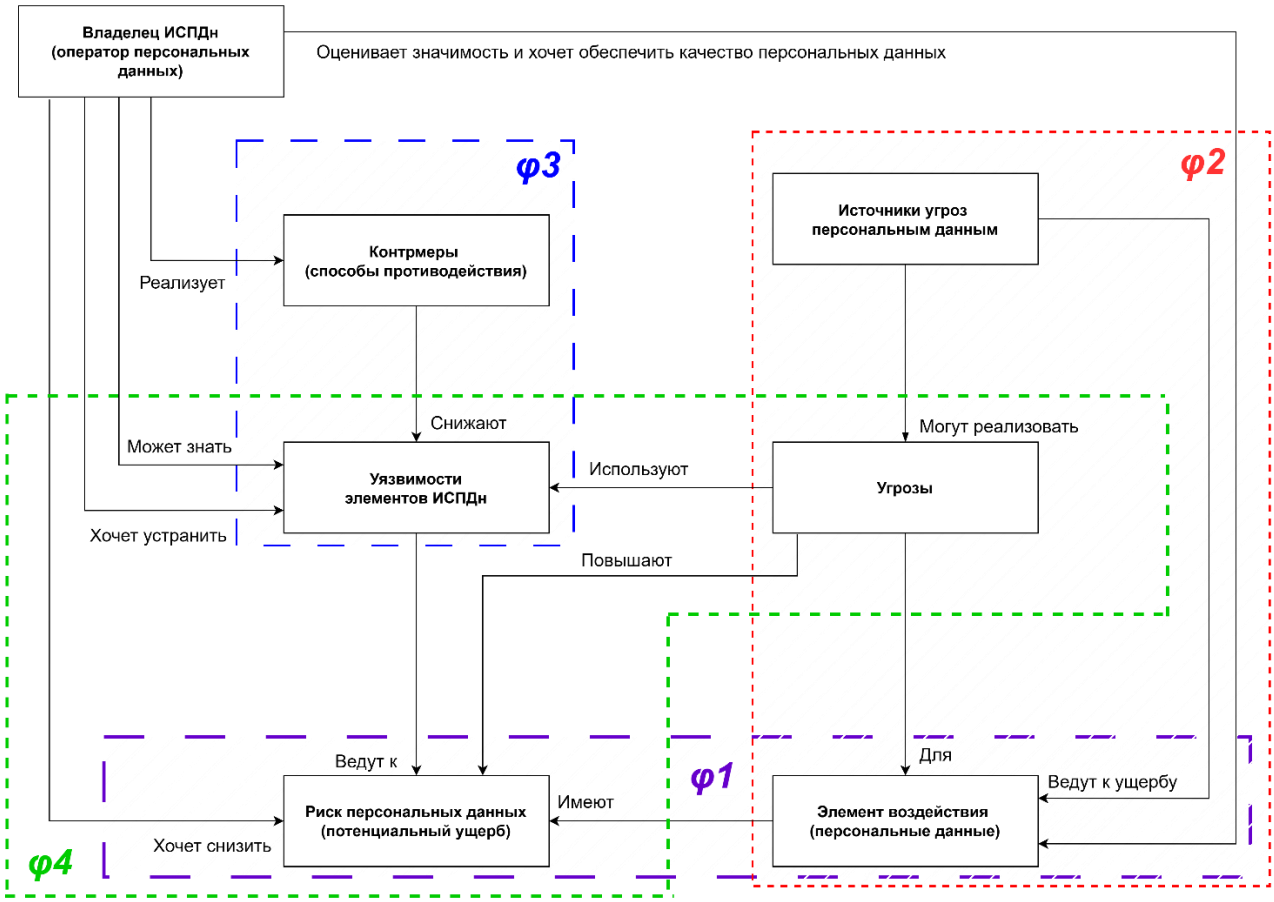


Рисунок 4.2 – Семантическая модель проблемной области оценки информационных рисков персональных данных при их автоматизированной обработке

При этом сделаны следующие допущения:

– данная модель отображает процесс оценки рисков персональных данных при их обработке в пределах одного облака мультиоблачной среды ИСПДн;

– в каждом из облаков рассматриваемой ИСПДн могут храниться различные персональные данные, относящиеся к одному субъекту ПДн.

Определим проблемные подобласти, которые необходимо учитывать при разработке математической модели оценки рисков ПДн в ИСПДн с мультиоблачной архитектурой [50,92,97,174].

- *Подобласть значимости элемента ИСПДн (персональных данных)* ($\varphi 1$). Показывает связь между ПДн в ИСПДн и последствиями нарушения качества ПДн.
- *Подобласть значимости угроз для элементов ИСПДн* ($\varphi 2$). Показывает уровень критичности тех или иных воздействий на качество персональных данных, обрабатываемых в ИСПДн.
- *Подобласть эффективности мер противодействия угрозам*, которые используются для снижения различных уязвимостей ИСПДн ($\varphi 3$). Используемые для этого меры могут быть связаны как с самой ИСПДн, так и с внешней средой, в которой она функционирует.
- *Подобласть критичности уязвимостей* ИСПДн ($\varphi 4$). Отражает возможность реализации определённого события информационного риска за счёт уязвимостей элементов ИСПДн при реализации конкретного воздействия на ПДн. Критичность определяется в момент наступления угрозы для определённого риска.

Выделим список определённых множеств [174] для одного облака *h* в ИСПДн с мультиоблачной архитектурой, где $h = \overline{1,H}$:

$T = \{T_i \mid i = 1,...,I\}$ – множество угроз ПДн;

$R = \{\langle E_j, Q_j \rangle \mid j = 1,...,J\}$ – множество информационных рисков ПДн,

где E_j – событие риска ПДн; Q_j – величина ущерба риска нарушения качества ПДн;

$V = \{V_d \mid d = 1,...,D\}$ – множество уязвимостей облака *h*;

$S = \{S_x \mid x = 1,...,X\}$ – множество источников угроз ПДн в облаке *h*;

$O = \{O_b \mid b = 1,..., B\}$ − множество элементов воздействия в облаке *h*;

$Z = \{\langle F_n, C_n \rangle \mid n = 1,..., N\}$ − множество способов (мер) противодействия в облаке *h*,

где F_n − реализуемая функция; C_n − стоимость реализации.

При оценке рисков нарушения качества персональных данных должны учитываться «требования к потенциальной возможности наступления определённых событий риска, максимально допустимый для ИСПДн ущерб и приемлемую стоимость мер по противодействию» [51,67].

Величина ущерба риска ПДн складывается из величин следующих типов ущербов: финансовые, репутационные потери, стоимость восстановления (включая человеческий капитал), штрафы, компенсация морального ущерба субъектам персональных данных и т.д. [51,67,79,91,97,130].

Определим для каждого приведённого выше множества «соответствующее отображение с учётом подобластей семантической модели» [174]:

- $O \times R \xrightarrow{\varphi 1} A$, где $A = \{a \mid a \geq 0, a \leq 1\}$ - определяет степень критичности информационных рисков существующим множеством элементов облака *h* мультиоблачной архитектуры;
- $S \times T \times O \xrightarrow{\varphi 2} U$, где $U = \{u \mid u \geq 0, u \leq 1\}$ - определяет степень значимости угроз множеству элементов облака *h* мультиоблачной архитектуры;
- $Z \times V \xrightarrow{\varphi 3} M$, где $M = \{m \mid m \geq 0, m \leq 1\}$ - определяет степень доступности уязвимостей ИСПДн при использовании множества способов противодействия;
- $T \times V \times R \xrightarrow{\varphi 4} P$, где $P = \{\langle \mathcal{M}^E, \mathcal{T}^Q \rangle \mid \mathcal{M}^E \geq 0,\ \mathcal{M}^E \leq 1,\ \mathcal{T}^Q \geq 0\}$ - определяет потенциал рисков ПДн при наличии множества угроз и уязвимостей облака *h* мультиоблачной архитектуры.

Одной из задач разработки модели оценки рисков нарушения качества ПДн является задача по снижению рисков с помощью оптимизации мер по противодействию уязвимостям ИСПДн с мультиоблачной архитектурой относительно множества потенциальных угроз. В этом случае необходимость и степень использования таких мер определяется важностью используемых

процессов работы с ПДн, по отношению к которым меры применяются. С учётом принятых выше в работе допущений в математической модели нужно рассматривать облака как отдельные независимые объекты, поэтому множество угроз нужно учитывать для каждого облака, которое входит в состав мультиоблачной архитектуры. Моделирование процесса консолидации/декомпозиции угроз в виде деревьев угроз рассмотрено в [122].

В соответствии с принципом системной целостности, приведённом в настоящей работе, применяемые способы и средства противодействия должны быть адекватными возможным угрозам процессам обработки персональных данных как в отдельном облаке, так и в мультиоблачной среде в целом и соответствовать нормативным правовым документам, регулирующим эти процессы.

Таким образом, задача оценки рисков нарушения качества персональных данных в ИСПДн с мультиоблачной архитектурой сводится к решению задачи (1.3) для множества облаков в мультиоблаке $H = \{H_h \mid h = 1,..., H\}$, где $P_\Sigma = \left\langle \mathcal{M}_\Sigma^E, \mathcal{П}_\Sigma^Q \right\rangle$ – консолидированный риск ПДн в ИСПДн, определяемый по всем источникам угроз; $\mathcal{M}_\Sigma^E$ – степень реализуемости события информационного риска; $\mathcal{П}_\Sigma^Q$ – консолидированный ущерб от нарушения качества ПДн.

При решении данной оптимизационной задачи необходимо учитывать требования по приемлемому ущербу для каждого облака и мультиоблачной среды в целом и допустимым затратам на использование мер противодействия риску. Ущерб при этом может быть выражен в условных единицах, определяющих уровень отрицательных последствий, а затраты – в денежных значениях или трудоёмкости процессов по снижению уровня риска [51,67,78,91,97,130,174].

4.3. Разработка модели оценки рисков нарушения качества персональных данных

Представим математическую модель оценки рисков нарушения качества персональных данных в виде системы показателей и способов их расчёта для проблемных областей, выделенных на ранее предложенной семантической модели [174]. Данные показатели должны отражать критичность угроз процессу обработки ПДн, способы их реализации, информационные риски ПДн, эффективность контрмер, позволяя выделить основные особенности, увеличивающие вероятность возникновения рисков. Оценка рисков производится на основе статистических данных и аналитических расчётов, а также на основе экспертных оценок, на основе которых можно оценить угрозы и уязвимости ИСПДн [95,118], и зачастую носит эвристический, экспертный характер. Поэтому необходимо определить показатели оценки рисков и способы их расчёта.

Для определения *φ1* введём показатель *индикатор критичности элемента риска*, определяющий степень связи риска с воздействиями на элемент ИСПДн:

$$A = \left\{ A_{bj} \middle| b = 1,...,B,\ j = 1,...,J \right\}, \tag{4.1}$$

где A_{bj} – индикатор критичности элемента *b* относительно риска *j*.

$$A_{bj} = \begin{cases} f(t_\tau), \text{ где } 0 \le f(t) \le 1,\ t_H \le t_\tau \le t_K; \\ L^*, \text{ где } L^* \in \left\{ L_W \middle| w = 1,...,W^* \right\},\ 0 \le L_W \le 1; \\ P(A), \end{cases} \tag{4.2}$$

где L_W - весовой коэффициент риска в зависимости от величины ущерба $L_w(Q_j)$, в т.ч. числовой аналог лингвистической переменной (зависит, не зависит и т.п.);

P - вероятность возникновения события *j*-го риска в отношении элемента *b*;

t_H - точка отсчёта оценки рисков;

t_K - точка окончания оценки рисков;

t_τ - текущий момент времени.

Параметры t_H и t_K определяют интервал времени оценки рисков нарушения качества персональных данных, уровень которых зависит от момента времени (риски могут изменять уровень в процессе эксплуатации ИСПДн. Например, поток заявок на обслуживание запросов на обработку персональных данных в дневное и ночное время может значительно отличаться и по объёму, и по типам запросов, и набору задействованных вычислительных ресурсов). А функция актуальности информации о персональных данных может быть использована как *f(t)* для оценки связи элемента ИСПДн с риском. Субъективную вероятность того, что несанкционированно полученная информация о ПДн может привести к негативным последствиям можно задать на основании экспертной оценки.

Для определения *φ2* вводятся показатель степени значимости угрозы и показатели, определяющие степень значимости источника угрозы по отношению к элементу ИСПДн:

– *уровень доступности элемента ИСПДн*, на который воздействует источник угрозы:

$$X^1 = \{X^1_{xb} \mid x = 1,...,X,\ b = 1,...,B\}, \tag{4.3}$$

где X^1_{xb} – уровень доступности элемента *b* со стороны источника *x*;

– *уровень готовности источника угрозы* к её реализации:

$$X^2 = \{X^2_{ix} \mid i = 1,...,I, x = 1,...,X\}, \tag{4.4}$$

где X^2_{ix} – уровень готовности источника *x* к осуществлению угрозы *i*;

– *уровень привлекательности осуществления угрозы* для источника по отношению к элементу ИСПДн:

$$X^3 = \{X^3_{ixb} \mid i = 1,...,I,\ x = 1,...,X,\ b = 1,...,B\}, \tag{4.5}$$

где X^3_{ixb} – уровень привлекательности реализации угрозы *i* для источника *x* по отношению к элементу *b* ИСПДн;

– *уровень серьезности последствий реализации угрозы* для элемента ИСПДн:

$$X^4 = \{X^4_{ib} \mid i = 1,...,I,\ b = 1,...,B\}, \tag{4.6}$$

где X_{ib}^4 – уровень серьезности последствий реализации угрозы *i* для элемента *b* ИСПДн.

Для любых *i*, *x*, *b* значения X_{xb}^1, X_{ix}^2, X_{ixb}^3, X_{ib}^4 равны:

$$X = \begin{cases} f(t_\tau), \text{ где } 0 \le f(t) \le 1,\ t_H \le t_\tau \le t_K; \\ L^*, \text{ где } L^* \in \{L_w \mid w = 1,...,W^*\},\ 0 \le L_w \le 1; \\ P, \end{cases} \quad (4.7)$$

где L_w - числовой аналог лингвистической переменной;

P - вероятность наступления события риска;

X - один из показателей X^1, X^2, X^3, X^4;

t_H, t_K, t_τ – аналогичны переменным из (4.2).

На основе данных значений определим значение *степень значимости угрозы U*, вычисляемой по формуле (4.8).

$$U = \{X_{xb}^1 \times X_{ix}^2 \times X_{ixb}^3 \times X_{ib}^4 \times \gamma(T_i) \mid i = 1,...,I,\ x = 1,...,X,\ b = 1,...,B\}, \quad (4.8)$$

где $\gamma(T_i) = \left(\dfrac{t_K - t_\tau}{t_K - t_H} \right)$.

Тогда из (4.8):

U_{ixb} – степень значимости угрозы *i* от источника *x* по отношению к элементу *b*.

Степень значимости источника угрозы по отношению к элементу можно оценить с помощью показателей X^1, X^2, X^3, X^4 с различными шкалами их оценки.

Определим уровни для оценки значений X^1, X^2, X^3, X^4 с использованием лингвистических переменных.

Уровень доступности элемента со стороны источника может зависеть от выполняемых функций по отношению к процессам обработки персональных данных, от удаленности элемента, а также от особенностей среды. Данный параметр можно категорировать следующим образом:

- высокий уровень (полный доступ к элементам ИСПДн);
- средний уровень (ограниченный доступ к элементам ИСПДн);

- низкий уровень (отсутствие доступа к элементам).

Уровень готовности источника к осуществлению угрозы может зависеть от степени квалификации источника (работника), а также от надежности работы технических и программных средств. Данный параметр можно категорировать следующим образом:

- высокий уровень (квалификация определяется всем объёмом возможных действий с ИСПДн от аппаратной до программной составляющей; срок эксплуатации аппаратных средств истек);
- средний уровень (квалификация ограничивается минимальными навыками работы с ИСПДн; срок эксплуатации аппаратных средств подходит к завершению);
- низкий уровень (отсутствие необходимой квалификации источника; надежное функционирование аппаратной части).

Уровень привлекательности реализации угрозы для источника по отношению к элементу может зависеть от заинтересованности источника для совершения воздействия, а также от наличия определенных условий для возможности воздействия. Данный параметр можно категорировать следующим образом:

- высокий уровень (воздействие на элементы может нанести непоправимый урон или составлять выгоду для источника);
- средний уровень (воздействие на элементы может нанести частичный ущерб ИСПДн);
- низкий уровень (элементы полностью или частично не представляют интереса для источника).

Уровень серьезности последствий реализации угрозы для элемента может зависеть от степени нарушения выполнения функций по обработке персональных данных элементом в результате воздействия. Данный параметр можно категорировать следующим образом:

- высокий уровень (полностью или частично неустранимые последствия);
- средний уровень (полностью или частично устранимые последствия);
- низкий уровень (отсутствие последствий).

Полученные результаты позволяют выявить на основе анализа структуры ИСПДн и используемых информационных ресурсов актуальные критичные источники угроз.

Для определения *φ3* нужно ввести следующие понятия.

– *Показатель использования способа противодействия угрозам*, определяющий, применяется ли конкретный способ (значение 1) или нет (значение 0):

$$K_n = \begin{cases} 1, \text{ если способ } n \text{ используется для противодейтсвия воздействиям;} \\ 0, \text{ в противном случае,} \end{cases} \quad (4.9)$$

где K_n – показатель использования способа n для противодействия.

– *Степень эффективности мер противодействия угрозам через воздействие на существующие уязвимости*:

$$Y_{dn} = \begin{cases} f_{dn}(t_\tau), \text{ где } 0 \le f_{dn}(t) \le 1,\ t_H \le t_\tau \le t_K; \\ L_{dn}{}^*, \text{ где } L_{dn}{}^* \in \{L_w \mid w = 1,...,W^*\},\ 0 \le L_w \le 1; \\ P_{dn}, \end{cases} \quad (4.10)$$

где Y_{dn} – степень эффективности n-й меры противодействия угрозам через уязвимость d;

Lw – числовой аналог лингвистической переменной (уязвимость осталась, уязвимости нет и т.п.);

P_{dn} – вероятность успешного воздействия на уязвимость d;

t_H , t_K , t_τ – аналогичны переменным из (4.2).

– *Степень доступности уязвимости*:

$$M_d = \max_{1 \le n \le N}((1 - Y_{dn}) \times K_n) \ , \quad (4.11)$$

где M_d – степень доступности уязвимости d (остаточный риск после реализации мер противодействия воздействиям на ИСПДн).

Введём следующие понятия для определения *φ4*:

– *Показатель уровня критичности уязвимости*:

$$H_{dixb} = U_{ixb} \times M_d \ , \quad (4.12)$$

где H_{dixb} – показатель уровня критичности уязвимости d при реализации угрозы i от источника x к элементу b;

U_{ixb} – степень значимости угрозы i от источника x по отношению к элементу системы b;

M_d – степень доступности уязвимости d.

Далее на основе полученных значений показателей для оценки информационных рисков ПДн рассчитаем для каждого облака единичные и системные риски персональных данных, введя показатели *потенциала единичного риска персональных данных* и *потенциала системного риска ПДн*.

Под *единичным риском ПДн* в облаке будем понимать вероятность наступления события риска ПДн по отношению к элементу ИСПДн при реализации источником отдельной угрозы через использование уязвимости.

– *Потенциал единичного риска ПДн* определяется парой компонент:

$$P_{dixbj} = \left\langle \mathcal{M}^{E}_{dixbj}, \mathcal{П}^{Q}_{dixbj} \right\rangle, \tag{4.13}$$

где P_{dixbj} – потенциал риска j по отношению к элементу b ИСПДн при реализации источником x угрозы i посредством активизации уязвимости d;

$\mathcal{M}^{E}_{dixbj}$ – степень реализуемости единичного события риска j в ИСПДн, вычисляемая по формуле (4.14);

$\mathcal{П}^{Q}_{dixbj}$ – уровень ущерба от единичного события риска j в ИСПДн, вычисляемый по формуле (4.15).

$$\mathcal{M}^{E}_{dixbj} = H_{dixb} \times A_{bj}; \tag{4.14}$$

$$\mathcal{П}^{Q}_{dixbj} = H_{dixb} \times A_{bj} \times Q_{j}, \tag{4.15}$$

где H_{dixb} – показатель уровня критичности уязвимости d при реализации угрозы i от источника x к элементу b ИСПДн;

A_{bj} – индикатор критичности элемента b ИСПДн относительно риска j в ИСПДн;

Q_j – величина ущерба от риска j для владельца ИСПДн (оператора ПДн).

Под *системным риском ПДн* в облаке будем понимать риск, обладающий максимальным потенциалом в отношении элемента ИСПДн по всем его источникам угроз.

– *Потенциал системного риска ПДн в облаке h*:

$$P_j = \left\langle \mathcal{M}_j^E, \Pi_j^Q \right\rangle, \tag{4.16}$$

где P_j – потенциал системного риска *j* в ИСПДн;

$\mathcal{M}_j^E$ – степень реализуемости события риска *j* в ИСПДн:

$$\mathcal{M}_j^E = \max_{d,i,x,b} \mathcal{M}_{dixbj}^E; \tag{4.17}$$

Π_j^Q – уровень ущерба от системного риска *j* в ИСПДн:

$$\Pi_j^Q = \max_{d,i,x,b} \Pi_{dixbj}^Q. \tag{4.18}$$

Таким образом, по каждому отдельному облаку мультиоблачной архитектуры ИСПДн определяют наиболее критичные информационные риски нарушения качества персональных данных, обрабатываемых в данной ИСПДн. Указанные риски далее должны быть ранжированы по мере убывания и по каждому из них должен быть разработан комплекс организационно-технических мер противодействия (в том числе разработка (доработка) нормативных правовых актов, обучение сотрудников и т.д.).

4.4. Алгоритм решения задачи по минимизации информационных рисков

Задача по уменьшению информационных рисков ПДн предполагает совершенствование применяемых мер противодействия воздействиям на ИСПДн с ограничениями на максимально допустимый ущерб события риска *j* нарушения качества ПДн при максимально допустимой возможности наступления данного события.

Для решения оптимизационной задачи (1.3) по минимизации информационных рисков ПДн необходимо определить критерии оценки информационного риска на основе предлагаемого ниже алгоритма.

Шаг 1. Рассчитаем *консолидированный информационный риск ПДн* в ИСПДн (общий уровень риска мультиоблачной ИСПДн в момент времени):

$$P_{\Sigma} = \left\langle \mathcal{M}_{\Sigma}^{E}, \mathcal{П}_{\Sigma}^{Q} \right\rangle, \tag{4.19}$$

где P_{Σ} – консолидированный информационный риск ПДн в ИСПДн;

$\mathcal{M}_{\Sigma}^{E}$ – степень реализуемости события риска:

$$\mathcal{M}_{\Sigma}^{E} = \max_{j} \mathcal{M}_{j}^{E}; \tag{4.20}$$

$\mathcal{П}_{\Sigma}^{Q}$ – уровень консолидированного ущерба ИСПДн - определяется как совокупная сумма потенциальных ущербов соответствующих рисков по всем индексам *j*:

$$\mathcal{П}_{\Sigma}^{Q} = \sum_{j=1}^{J} \mathcal{П}_{j}^{Q}. \tag{4.21}$$

Шаг 2. Сведём поставленную задачу (1.3) к следующему виду:

$$\min_{1 \le n \le N} \max_{1 \le i \le I} P_{\Sigma} \tag{4.22}$$

Поскольку мы предположили, что в ИСПДн применяются меры противодействия, то необходимо найти такие K_n (n=1,…,N), чтобы достигался (4.22) при ограничениях:

$$\begin{cases} \mathcal{M}_{j}^{E} \le \mathcal{M}_{j_{MAX}}^{E}, j = 1,...,J; \\ \mathcal{П}_{\Sigma}^{Q} \le \mathcal{П}_{\Sigma_{MAX}}^{Q}; \\ \sum_{n=1}^{N} K_n \times C_n \le C_{MAX} \end{cases},$$

где $\mathcal{M}_{j_{MAX}}^{E}$ – максимально допустимая степень реализуемости события риска;

$\mathcal{П}_{\Sigma_{MAX}}^{Q}$ – максимально допустимый уровень ущерба от наступления события риска;

C_{MAX} – максимально допустимая стоимость мер противодействия.

Шаг 3. Показатель остаточного риска после реализации мер противодействия воздействиям на ИСПДн M_d будем рассматривать, как вектор по n, т.е.:

$$M_d = ((1 - Y_{dn}) \times K_n) \tag{4.23}$$

Шаг 4. Раскроем показатель консолидированного информационного риска P_Σ, применив (4.20) и (4.21). Получим следующее выражение:

$$\min_{1 \le n \le N} \max_{1 \le i \le I} P_\Sigma = \min_{1 \le n \le N} \max_{1 \le i \le I} \left\langle \max_j \mathcal{M}_j^E, \sum_{j=1}^{J} \mathcal{П}_j^Q \right\rangle. \tag{4.24}$$

Таким образом, раскрывая (4.24), получаем следующие критерии для оценки информационных рисков после применения мер противодействия с точки зрения эффективности этих мер:

1. $\min\limits_{1 \le n \le N} \max\limits_{1 \le i \le I} \max\limits_j \mathcal{M}_j^E$ – критерий оценки риска с точки зрения его допустимости после применения мер противодействия воздействиям на ИСПДн;

2. $\min\limits_{1 \le n \le N} \max\limits_{1 \le i \le I} \sum\limits_{j=1}^{J} \mathcal{П}_j^Q$ – критерий оценки риска с точки зрения допустимого ущерба после применения мер противодействия воздействиям на ИСПДн.

Шаг 5. Продолжим дальнейшие подстановки, применяя (4.11), (4.12), (4.14), (4.17):

$$\begin{aligned}
&\min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \mathcal{M}_j^E = \min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} \mathcal{M}_{dixbj}^E = \\
&= \min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} \left(H_{dixb} \times A_{bj} \right) = \\
&= \min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} \left(U_{ixb} \times M_{dn} \times A_{bj} \right) = \\
&= \min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} \left(U_{ixb} \times \left(\left(1 - Y_{dn}\right) \times K_n \right) \times A_{bj} \right) = \\
&= \left(\min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} U_{ixb} \right) \times \\
&\times \left(\min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} \left(\left(1 - Y_{dn}\right) \times K_n \right) \right) \right) \times \left(\min_{1 \le n \le N} \max_{1 \le i \le I} \max_j \max_{d,i,x,b} A_{bj} \right) = \\
&= \min_{1 \le n \le N} \left[\left(\max_{i,x,b} U_{ixb} \right) \times \left(\max_{b,j} A_{bj} \right) \times \left(\max_d \left(\left(1 - Y_{dn}\right) \times K_n \right) \right) \right]
\end{aligned} \tag{4.25}$$

Получаем первый критерий эффективности мер противодействия – критерий оценки уровня информационного риска (остаточного информационного риска) наиболее критичного после применения *n*-й группы мер противодействия:

$$\min_{1\le n\le N}\left[U^{\max}\times A^{\max}\times\left(\max_{d}\left(\left(1-Y_{dn}\right)\times K_n\right)\right)\right], \tag{4.26}$$

где $U^{\max}=\max_{i,x,b}U_{ixb}$,

$A^{\max}=\max_{b,j}A_{bj}$.

Шаг 6. Продолжим дальнейшие подстановки, применяя (4.11), (4.12), (4.15), (4.18):

$$\begin{aligned}
&\min_{1\le n\le N}\max_{1\le i\le I}\max_{j}\sum_{j=1}^{J}\Pi_j^{Q}=\min_{1\le n\le N}\max_{1\le i\le I}\sum_{j=1}^{J}\max_{d,i,x,b}\Pi_{dixbj}^{Q}=\\
&=\min_{1\le n\le N}\max_{1\le i\le I}\sum_{j=1}^{J}\max_{d,i,x,b}\left(H_{dixb}\times A_{bj}\times Q_j\right)=\\
&=\min_{1\le n\le N}\max_{1\le i\le I}\sum_{j=1}^{J}\max_{d,i,x,b}\left(U_{ixb}\times M_{dn}\times A_{bj}\times Q_j\right)=\\
&=\min_{1\le n\le N}\max_{1\le i\le I}\sum_{j=1}^{J}\max_{d,i,x,b}\left(U_{ixb}\times\left(\left(1-Y_{dn}\right)\times K_n\right)\times A_{bj}\times Q_j\right)=\\
&=\min_{1\le n\le N}\max_{1\le i\le I}\sum_{j=1}^{J}\left(\max_{i,x,b}U_{ixb}\times\max_{d}\left(\left(1-Y_{dn}\right)\times K_n\right)\times\max_{b}A_{bj}\times Q_j\right),
\end{aligned} \tag{4.27}$$

Получаем второй критерий эффективности мер противодействия – критерий оценки информационного риска наиболее критичного с точки зрения возможного ущерба от его реализации после применения *n*-й группы мер противодействия:

$$\min_{1\le n\le N}\left[\sum_{j=1}^{J}\left(U^{\max}\times A_j^{\max}\times Q_j\times\max_{d}\left(\left(1-Y_{dn}\right)\times K_n\right)\right)\right], \tag{4.28}$$

где $U^{\max}=\max_{i,x,b}U_{ixb}$,

$A_j^{\max}=\max_{b}A_{bj}$.

В результате реализации описанных выше шагов исходная задача может быть решена как задача «линейного программирования». Разработанная модель позволяет определить не только значимые риски для каждого облака мультиоблачной среды, но и риски, связанные с взаимосвязанностью облаков. Результаты расчетов приведены в приложении Г.

4.5. Информационный процесс оценки рисков нарушения качества персональных данных при их автоматизированной обработке

Проведённый анализ полученных в разделах 4.1 – 4.4 результатов оценки рисков нарушения качества персональных данных показал, что информационный процесс оценки рисков персональных данных в ИСПДн должен включать шесть основных этапов:

- определение исходных данных;
- построение семантической модели;
- построение формализованной модели;
- расчёт показателей для оценки рисков;
- расчёт рисков;
- решение оптимизационной задачи;
- анализ полученных результатов.

Информационный процесс, включающий основные этапы и операции разработанного метода оценки информационных рисков персональных данных в ИСПДн, представлен в виде схемы на рисунке 4.3.

На этапе «Определение исходных данных» необходимо в зависимости от бизнес- и технологических операций, связанных с обработкой персональных данных, а также категорий обрабатываемых в ИСПДн персональных данных определить: требования к организации их безопасной автоматизированной обработки; потенциальные информационные риски нарушения качества персональных данных, присущие ИСПДн; показатели оценки их качества и

последствия, к которым может привести нарушение этих характеристик по таким показателям (в первую очередь конфиденциальность, целостность, доступности).

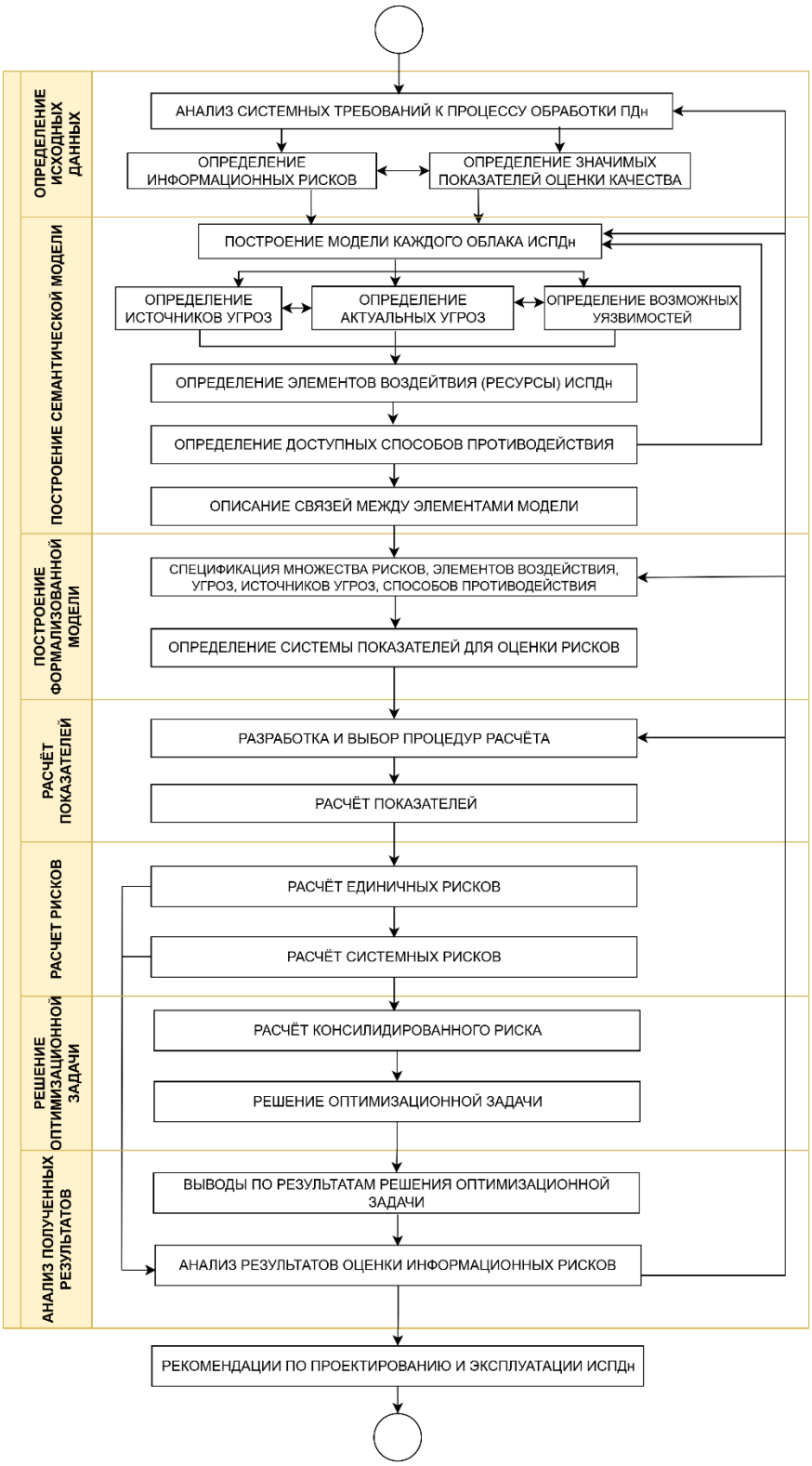


Рисунок 4.3 – Информационный процесс оценки рисков нарушения качества персональных данных в ИСПДн

Далее на этапе «Построение семантической модели» строится семантическая модель проблемной области оценки информационных рисков персональных данных для каждого облака (или одного облака, если не стоит задача оценки консолидированного риска ИСПДн), входящих в состав мультиоблачной архитектуры ИСПДн. На этом этапе определяются: значимость воздействий на ПДн с целью выявления актуальных угроз ПДн; возможность реализации этих угроз посредством использования уязвимостей ресурсов (элементов) ИСПДн; источники угроз; меры противодействия (контрмеры), используемые для снижения уязвимостей; связи между элементами модели. Актуальные угрозы определяются с помощью программного приложения [114]. В результате будет получено описание четырёх подобластей семантической модели, которые необходимо формализовать на следующем этапе для проведения дальнейших расчётов рисков. На этапе «Построение формализованной модели» проводится спецификация полученной семантической модели. Т.е. для каждой подобласти модели определяются системы показателей оценки информационных рисков персональных данных и способов (методов) их расчёта (например, на основе статистических данных или экспертного оценивания).

Далее на этапе «Расчёт показателей» производится расчёт с использованием выбранного способа системы показателей.

На основе полученных значений показателей на этапе «Расчёт рисков» рассчитываются единичные и системные риски персональных данных для каждого облака.

Расчёт консолидированного риска ИСПДн и решение оптимизационной задачи является предпоследним этапом информационного процесса – «Решение оптимизационной задачи».

На завершающем этапе «Анализ полученных результатов» производится анализ результатов оценки информационных рисков в целях выработки предложений по проектированию и эксплуатации ИСПДн.

Если в текущий период времени не стоит задача оптимизировать риски, можно рассчитать отдельные информационные риски и на основе их анализа

оценить эффективность применяемых мер по организации безопасных процессов обработки ПДн в ИСПДн с мультиоблачной архитектурой.

Предложенный информационный процесс может многократно применяться в процессе управления рисками персональных данных, в том числе и после дополнения модели угроз и сценариев воздействий на персональные данные.

Выводы по четвёртой главе

1. Предложенная декомпозиция ресурсов ИСПДн при обработке запросов к ПДн позволяет оператору ПДн провести классификацию угроз ПДн, реализовать декомпозицию информационных рисков на группы по подсистемам и элементам ИСПДн и задать показатели оценки качества ПДн на каждом уровне модели ИСПДн с учётом её мультиоблачной архитьектуры. Это позволяет взаимоувязать элементы ИСПДн, потенциальные угрозы нарушения качества ПДн и информационные риски. Таким образом, процесс воздействия на элементы ИСПДн и процесс оценки рисков персональных данных будут обладать свойствами наблюдаемости и управляемости.

2. Разработанная семантическая модель оценки рисков нарушения качества персональных данных в ИСПДн с мультиоблачной архитектурой позволяет рассматривать облака в данной архитектуре как отдельные объекты и учитывать множество угроз для каждого облака, т.е. оценка рисков представляет собой оптимизационную «минимаксную» задачу.

3. Разработанная система показателей для оценки рисков нарушения качества персональных данных, отражающая критичность воздействий на процесс обработки ПДн, способы их реализации, информационные риски ПДн, эффективность мероприятий по противодействию, позволяет выделить основные особенности, увеличивающие вероятность возникновения рисков, а также разработать модель оценки рисков нарушения качества ПДн с учётом предъявляемых требований к работе ИСПДн с мультиоблачной архитектурой.

4. Предложенная модель оценки рисков нарушения качества ПДн,

учитывает, в отличии от существующих: особенности функционирования корпоративной ИСПДн с мультиоблачной архитектурой, требования к максимально допустимой возможности наступления неопределенных событий риска и максимально допустимого ущерба от нарушения качества ПДн, а также приемлемой стоимости мероприятий по противодействию воздействиям на ИСПДн, и позволяет свести задачу оценки и снижения рисков к решению оптимизационной задачи.

5. Разработанный алгоритм решения оптимизационной задачи позволил свести поставленную многокритериальную оптимизационную минимаксную задачу к задаче линейного программирования.

6. Предложенный информационный процесс оценки рисков нарушения качества персональных данных при их автоматизированной обработке в ИСПДн может многократно применяться в процессе управления рисками персональных данных, в том числе и после дополнения модели угроз и сценариев воздействий на персональные данные.

Заключение

Данная диссертационная работа посвящена актуальной проблеме – разработке моделей и алгоритмов оценки эффективности использования ресурсов корпоративной ИСПДн с мультиоблачной архитектурой при обработке запросов к ПДн и оценки информационных рисков, возникающих при автоматизированной обработке ПДн в подобных ИСПДн, с целью их минимизации.

Для решения данных задач в диссертационной работе были исследованы и проанализированы: существующие требования к организации процессов обработки ПДн в ИСПДн; состав ресурсов ИСПДн; принципы организации и функционирования ИСПДн с мультиоблачной архитектурой при обработке запросов к ПДн; особенности обработки запросов к ПДн в ИСПДн; исследования, модели и алгоритмы по тематике диссертации. Проведённые исследования и анализ позволили получить следующие основные результаты диссертации:

1. Предложен единый системный подход к организации безопасной обработки ПДн в ИСПДн с мультиоблачной архитектурой за счёт унификации информационных процессов, что, в отличии от существующих подходов к реализации данных процессов, позволяет в дальнейшем разработать адекватную подсистему обеспечения качества этих процессов с целью выполнения требований нормативных правовых актов, эффективного использования ресурсов ИСПДн при обработке ПДн и минимизации рисков нарушения их качества.

2. Разработаны сценарии обработки разного типа запросов к ПДн в ИСПДн с мультиоблачной архитектурой, которые позволили выделить участников всех этапов инициации и обработки запросов, для каждого этапа дать краткое описание и указать формирование задержек на этих этапах, что дало возможность использовать графо-матричное моделирование процессов с последующим построением и исследованием модели процесса обработки ПДн в ИСПДн в виде однолинейной СМО конечной ёмкости в дискретном времени с ординарным неоднородным поступающим потоком заявок, распределенным по

геометрическому закону, с распределением длительности обслуживания фазового типа.

3. Разработана модель оценки эффективности использования ресурсов ИСПДн с мультиоблачной архитектурой при автоматизированной обработке ПДн, учитывающая, в отличии от известных моделей, обработку запросов к ПДн на основе сценариев и дискретный характер запросов, и позволяющая на основе рассчитанных ВВХ оценить эффективность использования ресурсов системы и обосновать архитектуру ИСПДн. Разработанный алгоритм решения СУР для расчёта основных ВВХ позволил снизить трудоёмкость вычислительного процесса не менее, чем на 17%.

4. Разработана модель оценки рисков нарушения качества ПДн, учитывающая, в отличии от существующих: особенности и условия функционирования корпоративной ИСПДн с мультиоблачной архитектурой, требования к максимально допустимой возможности наступления события риска, максимально допустимому ущербу, а также приемлемой стоимости мер по противодействию воздействиям на ИСПДн, и позволяющая представить задачу оценки допустимости рисков нарушения качества ПДн как многокритериальную оптимизационную задачу. Разработанный алгоритм решения задачи позволил решить поставленную оптимизационную минимаксную задачу в виде задачи линейного программирования.

Список литературы

1. Автоматизация поддержки принятия решений при подборе специалистов по управлению сложными инфокоммуникационными системами / С. В. Павлов, В. А. Докучаев, В. В. Маклачкова, Д. Д. Гадасин // T-Comm: Телекоммуникации и транспорт. – 2023. – Т. 17, № 12. – С. 36-43. – DOI 10.36724/2072-8735-2023-17-12-36-43. – EDN DWHCMB.

2. Аджемов, А. С. Организация работы с персональными данными [Текст] : [монография] / А. С. Аджемов, Е. Н. Голованова, А. А. Новиков ; Московский технический ун-т связи и информатики. - Москва : ИПК МТУСИ, 2010. - 211 с. : табл.; 21 см.; ISBN 978-5-98880-032-3.

3. Аналитический отчет «Россия: утечки информации ограниченного доступа 2023-2024» [Электронный ресурс] // Экспертно-Аналитический центр InfoWatch: [сайт]. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf (дата обращения: 05.03.2025).

4. Аналитический отчет «Утечки информации в мире 2023-2024 годы» [Электронный ресурс] // Экспертно-Аналитический центр InfoWatch: [сайт]. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-v-mire-2023-2024-gody.pdf (дата обращения: 19.03.2025).

5. Аудит информационных рисков в процессе обработки персональных данных / В. А. Докучаев, К. С. Владимирова, В. В. Маклачкова, В. Ю. Статьев // Технологии информационного общества : Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20–21 марта 2019 года. Том 2. – Москва: ООО "Издательский дом Медиа паблишер", 2019. – С. 34-36. – EDN XNJJOM.

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: методический документ, утверждён ФСТЭК России 15.02.2008 // СПС «КонсультантПлюс». — URL: https://www.consultant.ru/document/cons_doc_LAW_99662/ (дата обращения: 19.02.2023).

7. Башарин Г. П., Ефимушкин В. А. Исследование однолинейной системы с заявками нескольких типов в дискретном времени // Проблемы передачи информации. 1984. Т. 20. Вып. 1. С. 95-104.

8. Башарин Г.П., Бочаров П.П., Коган Я.А. Анализ очередей в вычислительных сетях. Теория и методы расчета. // М.: Наука, 1989. – 336 с.

9. Башарин Г.П., Гайдамака Ю.В., Самуйлов К.Е. Математическая теория телетрафика и ее приложения к анализу мультисервисных сетей связи следующих поколений // Автоматика и вычислительная техника. – 2013. - № 2. - С. 11-21.

10. Башарин Г.П., Ефимушкин В.А. Алгоритмический анализ структурно сложных систем конечной емкости с двумерным пространством состояний // В кн.: Модели теории телетрафика в системах связи и вычислительной технике. М.: Наука, 1985. – С. 28-41.

11. Башарин, Г.П. Графо-матричные модели локальных вычислительных сетей /Г.П. Башарин, В.А. Ефимушкин // М.: Изд-во УДН, 1986. – 40 с.

12. Бочаров П.П., Громов А.И. О пуассоновской двухфазной система ограниченной емкости // В кн.: Методы теории телетрафика в системах распределения информации. М.: Наука, 1975. – С. 15-28.

13. Бочаров П.П., Печинкин В.А. Теория массового обслуживания // М.: Изд-во РУДН, 1995. – 529 с.

14. Бочаров, П. П. Однолинейная система массового обслуживания конечной емкости с марковским потоком и обслуживанием в дискретном времени / П. П. Бочаров, Е. В. Вискова // Автоматика и телемеханика. – 2005. – № 2. – С. 72-91. – EDN NRCQSX.

15. В 2024 году Роскомнадзор зафиксировал 135 утечек данных [Электронный ресурс] // ТАСС: [сайт]. — URL: https://tass.ru/obschestvo/22893187 (дата обращения: 05.03.2025).

16. В.А. Докучаев, С.В. Запольских, В.В. Маклачкова, В.М. Матросов, А.В. Шведов, О.В. Щербина / Под ред. д.т.н., проф. В.А. Докучаева Архитектура цифровых платформ для защищённых ЦОД. Ч. 1. Общие подходы и используемые технологии: учебное пособие / МТУСИ. – М., 2021. – 90 с.

17. Вискова Е.В. Двухфазная система массового обслуживания с марковскими потоком и обслуживанием в дискретном времени // Информационные процессы. – 2005. – Том 5. – № 3. – С. 247-257.

18. Вишневский В.М. Теоретические основы проектирования компьютерных сетей // М.: Техносфера, 2003. – 512 с.

19. Волкова, Л. В. Использование метода CRAMM для оценки информационных рисков / Л. В. Волкова, Д. В. Макарова, В. А. Докучаев // Телекоммуникации и информационные технологии. – 2021. – Т. 8. – № 1. – С. 103-109. – EDN BVQQXM.

20. Гадасин В.А. Надежность сложных информационно-управляющих систем / В.А. Гадасин, И.А. Ушаков. — Москва : Сов. радио, 1975. — 191 с. схем.; 20. — (Библиотека инженера по надежности).

21. Гарайшина И.Р., Моисеева С.П., Назаров А.А. Методы исследования коррелированных потоков и специальных систем массового обслуживания // Томск: Изд-во научно-технической литературы, 2010. – 202 с.

22. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания // М.: Наука, ГРФМЛ, 1987. – 336 с.

23. Голованова, Е. Н. Особенности нормативно-правового обеспечения защиты персональных данных с использованием инфокоммуникационных технологий / Е. Н. Голованова, В. А. Докучаев, В. В. Маклачкова // II научный форум телекоммуникации: теория и технологии ТТТ-2017. Проблемы техники и технологий телекоммуникаций ПТИТТ-2017 : материалы XVIII Международной научно-технической конференции, Казань, 20–24 ноября 2017 года. Том 2. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2017. – С. 316-320. – EDN YUXPRT.

24. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов // СПб.: БХВ-Петербург, 2010. – 400 с.

25. Горбунова, А. В. Обзор систем параллельной обработки заявок. Часть II / А. В. Горбунова, И. С. Зарядов, К. Е. Самуйлов // Вестник Российского университета дружбы народов. Серия: Математика, информатика, физика. – 2018. – Т. 26, № 1. – С. 13-27. – DOI 10.22363/2312-9735-2018-26-1-13-27. – EDN YPNLJK.

26. ГОСТ Р 51275-2006 Объект информатизации. Факторы, воздействующие на информацию. Общие положения. - М.: Стандартинформ, 2018. - 8с.

27. ГОСТ Р 51901.12-2007 (МЭК 60812:2006) Метод анализа видов и последствий отказов. - М.: Стандартинформ, 2008. - 36с.

28. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска. - М.: Стандартинформ, 2020. - 86с.

29. ГОСТ Р 59407-2021 Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных. - М.: Стандартинформ, 2021. - 41с.

30. ГОСТ Р ИСО 31000-2019 Менеджмент риска. Принципы и руководство. - М.: Стандартинформ, 2020. - 14с.

31. ГОСТ Р ИСО 8000 Качество данных. - М.: Стандартинформ, 2019. - 15с.

32. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. - М.: Стандартинформ, 2007. - 18с.

33. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. - М.: Стандартинформ, 2014. - 50с.

34. ГОСТ Р ИСО/МЭК 27001:2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. - М.: Стандартинформ, 2008. - 26с.

35. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. - М.: Стандартинформ, 2014. - 198с.

36. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. - М.: Стандартинформ, 2011. - 47с.

37. Гражданский кодекс Российской Федерации (ГК РФ) [Электронный ресурс]: федеральный закон: принят Гос. Думой 21 окт. 1994г. // СПС «КонсультантПлюс»: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_5142/?ysclid=m9hl5j7fxj897053486 (дата обращения: 21.05.2023).

38. Гребешков А.Ю. Управление и технический учёт ресурсов в телекоммуникациях.– ИРИАС.–М., 2008 г.–268с. (рецензент – д.т.н., проф. Докучаев В.А.).

39. Далингер, Я. М. Модель узла обработки с поглощением данных / Я. М. Далингер, Ю. Л. Леохин, Е. А. Саксонов // Системы синхронизации, формирования и обработки сигналов. – 2018. – Т. 9, № 3. – С. 75-78. – EDN VMWCEZ.

40. Докучаев В.А. Механизмы обеспечения защищенности данных в распределенных информационных системах / В. А. Докучаев, А. В. Нетребко, В. В. Маклачкова, С. С. Мытенков // Экономика и качество систем связи. – 2025. – № 2(36). – С. 125-134. – EDN INMCRQ.

41. Докучаев В.А. Подходы к защите персональных данных на просторе «Больших данных» / В. А. Докучаев, В. В. Маклачкова, В. О. Сундатов [и др.] // Теория и практика экономики и предпринимательства : Труды XX Международной научно-практической конференции, Симферополь - Гурзуф, 20–22 апреля 2023 года / Под редакцией Н.В. Апатовой. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. – С. 34-36. – EDN BUQVMG.

42. Докучаев В.А., Степанов С.Н. Расчет тандемных соединений обслуживающих устройств с учетом повторения заблокированных вызовов // М.: Радио и связь, 1999 34 С.

43. Докучаев, В. А. Анализ бизнес-процессов при организации автоматизированной обработки персональных данных / В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // Технологии информационного общества : Сборник трудов XII Международной отраслевой научно-технической конференции, Москва, 14–15 марта 2018 года. Том 2. – Москва: ООО "Издательский дом Медиа паблишер", 2018. – С. 106-109. – EDN XUPRPN.

44. Докучаев, В. А. Анализ рисков при работе с персональными данными в информационной системе предприятия / В. А. Докучаев, В. В. Маклачкова // Актуальные проблемы и перспективы развития экономики : Труды XVI Международной научно-практической конференции, Симферополь - Гурзуф, 19–21 октября 2017 года / Министерство образования и науки Российской Федерации, Крымский федеральный университет имени В. И. Вернадского, Институт экономики и управления, Кафедра бизнес-информатики и математического моделирования. – Симферополь - Гурзуф: ИП Боровко А.А., 2017. – С. 35-36. – EDN YTPAJK.

45. Докучаев, В. А. Архитектура центров обработки данных / В. А. Докучаев, А. А. Кальфа, В. В. Маклачкова. – Москва : Научно-техническое издательство "Горячая линия-Телеком", 2020. – 240 с. – ISBN 978-5-9912-0849-9. – EDN BHARSE.

46. Докучаев, В. А. Аудит и управление рисками в корпоративных инфокоммуникационных системах / В. А. Докучаев, С. С. Мытенков // Актуальные проблемы и перспективы развития экономики : Труды XVI Международной научно-практической конференции, Симферополь - Гурзуф, 19–21 октября 2017 года / Министерство образования и науки Российской Федерации, Крымский федеральный университет имени В. И. Вернадского, Институт экономики и управления, Кафедра бизнес-информатики и математического моделирования. – Симферополь - Гурзуф: ИП Боровко А.А., 2017. – С. 37-38. – EDN YTQDCT.

47. Докучаев, В. А. Идентификация субъекта – ключевой момент в процессе обработки персональных данных / В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // Технологии информационного общества : Сборник трудов XIV Международной отраслевой научно-технической конференции, Москва, 18–19 марта 2020 года. – Москва: ООО "Издательский дом Медиа паблишер", 2020. – С. 273-274. – EDN ADBXFS.

48. Докучаев, В. А. Исследование моделей машинного обучения по их применению в зависимости от вида экономической деятельности / В. А. Докучаев, В. В. Маклачкова, Д. О. Богданов // Тенденции развития интернет и цифровой

экономики : Труды VII Международной научно-практической конференции, Симферополь-Сатера (Алушта), 30 мая – 01 2024 года. – Симферополь: ИП Зуева, 2024. – С. 18-23. – EDN GRNHUC.

49. Докучаев, В. А. Классификация персональных данных, подлежащих автоматизированной обработке / В. А. Докучаев, К. С. Владимирова, В. В. Маклачкова // Теория и практика экономики и предпринимательства : Труды Юбилейной XV Международной научно-практической конференции, Симферополь-Гурзуф, 19–21 апреля 2018 года / Крымский федеральный университет им. В.И. Вернадского, Институт экономики и управления, Кафедра бизнес-информатики и математического моделирования. – Симферополь-Гурзуф: ИП Зуева Т.В., 2018. – С. 170-172. – EDN YVZOHJ.

50. Докучаев, В. А. Модель для оценки эффективности автоматизированной работы с персональными данными в мультиоблачной информационной системе / В. А. Докучаев, В. В. Маклачкова // Цифровая трансформация. Связь будущего : Материалы XXVIII Международного Форума МАС' 2024, Москва, 26 апреля 2024 года. – Москва: Государственный университет просвещения, 2024. – С. 83-91. – EDN DJIRZE.

51. Докучаев, В. А. Постановка задачи оценки качества информации при обработке персональных данных в информационных системах мультиоблачной архитектуры / В. А. Докучаев, В. В. Маклачкова, В. В. Шемякин // Теория и практика экономики и предпринимательства : Труды XX Международной научно-практической конференции, Симферополь - Гурзуф, 20–22 апреля 2023 года / Под редакцией Н.В. Апатовой. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. – С. 37-39. – EDN JACYHT.

52. Докучаев, В. А. Применение Entity Component System при создании игр / В. А. Докучаев, В. В. Маклачкова, И. Д. Удалов // Экономика и качество систем связи. – 2025. – № 1(35). – С. 57-66. – EDN JFOTMC.

53. Докучаев, В. А. Проблема актуализации данных в CRM-системах / В. А. Докучаев, В. В. Маклачкова, А. А. Бойко // Экономика и качество систем связи. – 2025. – № 1(35). – С. 45-57. – EDN UGUIWG.

54. Докучаев, В. А. Требования к информационным системам при работе с «цифровым образом» субъекта / В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // III Научный форум телекоммуникации: теория и технологии ТТТ-2019 : Материалы XXI Международной научно-технической конференции, Казань, 18–22 ноября 2019 года. Том 1. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. – С. 296-297. – EDN HRNDBS.

55. Докучаев, В. А. Цифровизация субъекта персональных данных / В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14, № 6. – С. 27-32. – DOI 10.36724/2072-8735-2020-14-6-27-32. – EDN XVWYJP.

56. Дюфур С. Л. Расчет числа каналов сети дальней автоматической телефонной связи с учетом повторных вызовов // Автоматика, телемеханика, связь №8, 1969.- С. 16-19.

57. Емельяненко М.В. [Электронный ресурс] // Рецепты безопасности от Емельянникова: [сайт]. — URL: https://emeliyannikov.blogspot.com (дата обращения: 15.12.2023).

58. Ефимушкин В.А. Анализ системы конечной емкости с обслуживанием общего вида и неоднородными заявками в дискретном времени // В кн.: Модели информационных сетей. М.: Наука, 1984. – С. 76-83.

59. Ефимушкин, В. А. Анализ геометрической системы массового обслуживания с конечным накопителем изменяемой емкости / В. А. Ефимушкин, Т. В. Ледовских // Вестник Российского университета дружбы народов. Серия: Прикладная и компьютерная математика. – 2005. – Т. 4, № 1. – С. 19-30. – EDN LABIXB.

60. Ефимушкин, В. А. Мой цифровой двойник / В. А. Ефимушкин // Электросвязь. – 2020. – № 12. – С. 35-45. – DOI 10.34832/ELSV.2020.13.12.005. – EDN XOAVCE.

61. Забелин, О. А. Подсистема оценки и обеспечения качества данных интегрированной информационной системы / О. А. Забелин, Е. А. Саксонов // Качество. Инновации. Образование. – 2008. – № 8(39). – С. 56-59. – EDN JTKGRD.

62. Завгородний В. И. Методика выбора механизмов управления информационными рисками [Электронный ресурс] // Финансы: теория и практика. 2006. №3. - URL: https://cyberleninka.ru/article/n/metodika-vybora-mehanizmov-upravleniya-informatsionnymi-riskami (дата обращения: 22.01.2024).

63. Закон о защите персональной информации Китайской Народной Республики / Personal Information Protection Law of the People’s Republic of China (PIPL) [Электронный ресурс]. - URL: https://chinahelp.me/information/zakon-o-zashhite-personalnoj-informaczii-kitajskoj-narodnoj-respubliki (дата обращения: 15.04.2023).

64. Ионин Г. Л., Седол Я. Я. Исследование полнодоступной схемы с повторными вызовами и предварительным обслуживанием // В кн.: Методы теории телетрафика в системах распределения информации. М.: Наука, 1975. - С. 75-84.

65. Ионин Г. Л., Седол Я. Я. Исследование телефонных систем при повторных вызовах // Латв. мат. ежегодник. - 1970. Вып. 7. - С. 71-83.

66. Ионин Г. Л., Седол Я. Я. Таблицы вероятностных характеристик полнодоступного пучка при повторных вызовах/ М.: Наука.-1970.-155 с.

67. Классификация угроз информации по уровням типовой модели корпоративной инфокоммуникационной системы / В. А. Докучаев, В. В. Маклачкова, С. С. Мытенков, О. А. Сидорова // Технологии информационного общества : Материалы XIII Международной отраслевой научно-технической конференции, Москва, 20–21 марта 2019 года. Том 1. – Москва: ООО "Издательский дом Медиа паблишер", 2019. – С. 433-435. – EDN ZTRJXF.

68. Клейнрок Л. Вычислительные системы с очередями // М.: Мир, 1979. – 600 с.

69. Клейнрок Л. Теория массового обслуживания // М.: Машиностроение, 1979. – 432 с.

70. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ [Электронный ресурс]: федер. закон: принят Гос. Думой 20 дек. 2001г.: по состоянию на 01.03.2025г. // СПС «КонсультантПлюс»: законодательство РФ. – URL: https://www.consultant.ru/document/cons_doc_LAW_34661/?ysclid=m9hky2rv18889753322 (дата обращения: 21.03.2023).

71. Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108, Страсбург, 28.01.1981 г.) [Электронный ресурс]. - URL: https://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 21.03.2023).

72. Кучерявый А.Е. Методы оценки качества обслуживания вызовов АТС// Труды Международной Академии Связи.-1998, №4(8).-С.17-20.

73. Кучерявый А.Е., Цуприков А.Л. Сети связи следующего поколения // М.: ЦНИИС, 2006. – 278 с.

74. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет // СПб.: Наука и техника, 2004. – 336 с.

75. Лазарев Ю.В., Долгов К.А. Метод анализа качества обслуживания поступивших вызовов при адаптивном управлении ресурсами цифровой линии связи. Международный семинар “Информационные сети, системы и технологии”. Часть 1. Телекоммуникационные сети и системы. М.-Ярославль, 1997.-С.13-15.

76. Ледовских Т.В. Дискретная система массового обслуживания с групповым потоком фазового типа и пороговым управлением / / Вестник РУДН. Сер . "Прикладная математика информатика ", 2002 , № 1 . С.107-118.

77. Лившиц Б.С., Пшеничников А.П., Харкевич А.Д. Теория телетрафика // М.: Связь, 1979. – 224 с.

78. Лукацкий А. Цена инцидента на реальном примере утечки персданных из одной финансовой организации [Электронный ресурс] // Алексей Лукацкий "Бизнес без опасности". 2022: [сайт]. – URL: https://lukatsky.ru/business/tsena-intsidenta-na-realnom-primere-utechki-persdannyh-iz-odnoy-finansovoy-organizatsii.html (дата обращения: 05.03.2025).

79. Маклачкова, В.В. Основные риски персональных данных в мультиоблачных информационных средах // Экономика и качество систем связи. – 2025. – № 3(37). – С. 58-61 (Перечень рецензируемых научных изданий № 1729 от 05.02.2025).

80. Мейкшан В. И. Расчет потерь вызовов для неполнодоступных и звеньевых включений с учетом неработоспособных состояний оборудования // Надежность и

техническое обслуживание АМТС с программным управлением / под ред. В. Г. Дедоборща и Н. Б. Суторихина. М.: Радио и связь, 1989. С. 213-226.

81. Методический документ. Методика оценки угроз безопасности информации [Электронный ресурс]: утверждён Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г. // ФСТЭК России. 2021. — URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=m9hjvh8n3a159926334 (дата обращения 15.03.2023).

82. Моисеев Н.Н. Математические задачи системного анализа. - М.: Наука, Гл.редакция физ.- мат. Литературы, 1981. – 488с.

83. Мокров, Е. В. Модель облачных вычислений в виде системы массового обслуживания / Е. В. Мокров, К. Е. Самуйлов // Современные информационные технологии и ИТ-образование. – 2012. – № 8. – С. 685-689. – EDN TJTRFZ.

84. Мокров, Е. В. Модель системы облачных вычислений в виде системы массового обслуживания с несколькими очередями и с групповым поступлением заявок / Е. В. Мокров, К. Е. Самуйлов // T-Comm: Телекоммуникации и транспорт. – 2013. – Т. 7, № 11. – С. 139-141. – EDN RXNODJ.

85. Мунтян, А.В. Комплексная защита персональных данных [Электронный ресурс] / А.В. Мунтян: [сайт]. – URL: https://www.advgazeta.ru/ag-expert/advices/kompleksnaya-zashchita-personalnykh-dannykh/ (дата обращения: 15.01.2025).

86. Назаров А.Н., Сычев К.И. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения // Красноярск: Изд-во ООО «Поликом», 2010. – 389 с.

87. Наумов В.А. О независимой работе подсистем сложной системы. // В кн. «Труды 3-й Всесоюзной школы-совещания по теории массового обслуживания». М.: Изд-во МГУ, 1976. – Т. 2. – С. 169-177.

88. Национальный проект «Экономика данных и цифровая трансформация государства» [Электронный ресурс]. // Официальный сайт Правительства

Российской Федерации: [сайт]. – URL: http://government.ru/rugovclassifier/923/events/ (дата обращения 23.01.2025).

89. Нейман В.И. Телетрафик и теория массового обслуживания // Автоматика и телемеханика. – 2009. – № 12. – С. 29-38.

90. Никитин, Е. В. Управление потоками данных в многосерверных системах обработки информации / Е. В. Никитин, Е. А. Саксонов // Информатика и системы управления / Федеральное агентство по образованию; Амурский государственный университет. - Благовещенск.- 2010.- С. 3-9.- №3(25).- (Организация баз данных).- ISSN 1814-2400.

91. Определение экономической эффективности затрат предприятия на защиту персональных данных / В. И. Неманова, И. С. Вакурин, В. В. Маклачкова, Д. В. Гадасин // DSPA: Вопросы применения цифровой обработки сигналов. – 2024. – Т. 14, № 3. – С. 37-45. – EDN UIELEK.

92. Оценка качества обработки больших объёмов данных в высоконагруженных инфокоммуникационных системах / Е. В. Горбань, В. А. Докучаев, В. В. Маклачкова, В. Ю. Статьев // Телекоммуникационные и вычислительные системы - 2018 : Международный форум информатизации (МФМ-2018); Международный конгресс (CTN-2018) "Коммуникационные технологии сети", Москва, 21 ноября 2018 года. – Москва: Научно-техническое издательство "Горячая линия-Телеком", 2018. – С. 25-28. – EDN VWQCCQ.

93. Першаков, Н.В. Системы M|G|1 с групповым обслуживанием и их применение к анализу модели протокола управления потоковой передачей. Часть I / Н.В. Першаков, К.Е. Самуйлов // Вестник Российского университета дружбы народов. Серия: Математика, информатика, физика. – 2009. – № 1. – С. 34-44. – EDN JYBFJL.

94. Першаков, Н.В. Системы M|G|1 с групповым обслуживанием и их применение к анализу модели протокола управления потоковой передачей. Часть II / Н. В. Першаков, К. Е. Самуйлов // Вестник Российского университета дружбы народов. Серия: Математика, информатика, физика. – 2009. – № 2. – С. 43-53. – EDN KKXTUH.

95. Петухов, Д. А. Анализ показателей качества облачных услуг на мировом рынке / Д. А. Петухов, В. А. Докучаев // REDS: Телекоммуникационные устройства и системы. – 2021. – Т. 11, № 1. – С. 30-35. – EDN ZIWAUQ.

96. Печинкин А.В., Разумчик Р.В. Системы массового обслуживания в дискретном времени. – М.: ФИЗМАТЛИТ, 2018. – 432 с. – ISBN 978-5-9221-1791-3.

97. Постановка задачи оценки рисков при работе с большими объемами информации в высоконагруженных инфокоммуникационных системах / В. А. Докучаев, Е. В. Горбань, В. В. Маклачкова, С. С. Мытенков // Актуальные проблемы и перспективы развития экономики : Труды XVII Международной научно-практической конференции, Симферополь - Гурзуф, 18–20 октября 2018 года / Под редакцией Н.В. Апатовой. – Симферополь - Гурзуф: ИП Зуева Т.В., 2018. – С. 30-31. – EDN YPHZZB.

98. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]: постановление Правительства Российской Федерации: утвержд. 01.11.2012 // СПС «КонсультантПлюс»: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/ (дата обращения: 21.05.2024).

99. Постановление Правительства РФ от 06.07.2015 N 676 (ред. от 18.03.2025) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [Электронный ресурс]: постановление Правительства Российской Федерации: утвержд. 06.07.2015.: по состоянию на 18.03.2025г. // СПС КонсультантПлюс: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_182413/ (дата обращения: 21.03.2025).

100. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных с использованием средств…» [Электронный ресурс]. // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_167862/3faa8723e46ecc4973f2bc794c221b88debfcaa9/ (дата обращения 21.03.2025).

101. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_146520/ (дата обращения 25.03.2025).

102. Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/EC (Общий Регламент о защите персональных данных / General Data Protection Regulation)» (Принят в г. Брюсселе 27.04.2016) // СПС КонсультантПлюс. – URL: https://www.consultant.ru/law/podborki/obschij_reglament_es_po_zaschite_personalnyh_dannyh/ (дата обращения 21.02.2023).

103. Ресурсные системы массового обслуживания с произвольным обслуживанием / А. В. Горбунова, В. А. Наумов, Ю. В. Гайдамака, К. Е. Самуйлов // Информатика и ее применения. – 2019. – Т. 13, № 1. – С. 99-107. – DOI 10.14357/19922264190114. – EDN ZASZJJ.

104. Росляков, А. В. СЕТЬ 2030: архитектура, технологии, услуги / А. В. Росляков. – Москва : Общество с ограниченной ответственностью "Издательско-книготорговый центр "Колос-с", 2022. – 278 с. – ISBN 978-5-00129-251-7. – EDN YSGSAY.

105. Рыкова Т. Алгоритм расчета стационарного распределения для многофазной системы конечной емкости в дискретном времени с распределяемым между фазами множеством приборов // Труды XI Международной отраслевой научно-

технической конференции «Технологии информационного общества». Москва, 15-16.03.2017 г. – М.: Медиа Паблишер, 2017. – С. 416- 418.

106. С. Н. Степанов, И. И. Цитович, “Эквивалентные определения вероятностных характеристик моделей с повторными вызовами и их применение”, Пробл. передачи информ., 25:2 (1989), 79–90 mathnet mathscinet zmath; S. N. Stepanov, I. I. Tsytovich, “Equivalent Definitions of the Probabilistic Characteristics of Models with Repeated Calls and Their Application”, Problems Inform. Transmission, 25:2 (1989), 145–153.

107. Саати Т.Л. Элементы теории массового обслуживания и ее приложения // М.: Советское Радио, 191. – 520 с.

108. Саксонов Е.А., «Метод вычисления вероятностей состояний для однолинейной системы массового обслуживания с «прогулками» обслуживающего прибора», Автомат. и телемех., 1995, № 1, 101–106; Autom. Remote Control, 56:1 (1995), 83–87.

109. Саксонов, Е. А. Процедура обезличивания персональных данных / Е. А. Саксонов, Р. В. Шередин // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2011. – № 3. – С. 1. – EDN NECYGF.

110. Саксонов, Е.А. Модель информационной системы как марковской многолинейной системы с повторными вызовами/ Е.А. Саксонов, А.В. Шубин // Материалы междунар. науч. конф. «Математические методы повышения эффективности информационно-телекоммуникационных сетей». - Вып. 19. - Гродно, 2007. -С. 222-223.

111. Саксонов, Е.А. Модель узла обработки с тиражированием данных / Е. А. Саксонов, Ю. Л. Леохин, Я. М. Далингер // Системы синхронизации, формирования и обработки сигналов. – 2018. – Т. 9, № 1. – С. 137-140. – EDN VMJPFZ.

112. Самуйлов, К. Е. О методе расчета времени отклика системы облачных вычислений с несколькими поставщиками услуг / К. Е. Самуйлов, Е. В. Мокров // Информационно-телекоммуникационные технологии и математическое моделирование высокотехнологичных систем : материалы Всероссийской конференции с международным участием, Москва, 22–25 апреля 2014 года. –

Москва: Российский университет дружбы народов, 2014. – С. 48-49. – EDN UTBSUB.

113. Самуйлов, К.Е. К анализу системы M[X]|G|1|r с прогулками прибора / К.Е. Самуйлов, Э.С. Сопин // Вестник Российского университета дружбы народов. Серия: Математика, информатика, физика. – 2011. – № 1. – С. 91-97. – EDN NBPWXZ.

114. Свидетельство о государственной регистрации программы для ЭВМ № 2023615007 Российская Федерация. Программное приложение «Анализатор актуальности угрозы» («Threat Relevance Analyzer» – на английском языке) для определения актуальности угроз персональных данных при их обработке в информационных системах персональных данных : № 2023613955 : заявл. 27.02.2023 : опубл. 09.03.2023 / В. А. Докучаев, В. В. Маклачкова, Д. В. Гадасин [и др.] ; заявитель Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ». – EDN AOOMDG.

115. Свидетельство о государственной регистрации программы для ЭВМ № 2025660244 Российская Федерация. Программное приложение для оценки эффективности использования ресурсов информационной системы при обработке персональных данных «ИРИС ПД» («ISRU PD» - на английском языке) для расчета аналитических моделей функционирования информационных систем при обработке персональных данных : заявл. 18.04.2025 : опубл. 22.04.2025 / В. В. Маклачкова, В. А. Докучаев, Д. В. Гадасин [et al.] ; заявитель Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики». – EDN GQAKGI.

116. Севастьянов Б.А. Курс теории вероятностей и математической статистики // М.: Изд-во ИКИ, 2004. – 272 с.

117. Сети 2030: перспективы и проблемы / С. В. Павлов, Е. В. Леонович, В. В. Маклачкова, В. А. Докучаев // REDS: Телекоммуникационные устройства и системы. – 2022. – Т. 12, № 2. – С. 17-23. – EDN UZNLKQ.

118. Симонов, А. П. Анализ рисков облачных вычислений / А. П. Симонов, В. А. Докучаев // Перспективные технологии в средствах передачи информации : материалы 14-ой международной научно-технической конференции, Владимир, 06–07 октября 2021 года. – Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2021. – С. 344-347. – EDN PJPHHM.

119. Соколов Н.А. Задачи планирования сетей электросвязи // СПб.: Техника связи, 2012.— 428 с.

120. Статьев В.Ю. и др. Моделирование процессов интеллектуальной поддержки и защиты систем управления органов государственной власти в условиях информационного противодействия // Отчет лаборатории «Математического моделирования и анализа НОРИАС», - М., Академия криптографии РФ, 2001.

121. Статьев В.Ю. Некоторые подходы к организации ложных информационных объектов в информационной системе // Сборник материалов 9-ой научно-техническая конференции по криптографии, - М., Академия Криптографии РФ, 2001. - С. 143-147.

122. Статьев В.Ю. Оценка информационных рисков в системах обработки служебной информации : дис. … канд. техн. наук 05.13.01 / Статьев В.Ю. – Москва, 2004. – 148 с.

123. Статьев В.Ю. Характеристики качества функционирования ИКС // Сборник материалов Юбилейной научно-практической конференции ФАПСИ, 2002. - С.85-88.

124. Статьев В.Ю., Левятов И.Д. Имитационное моделирование как средство оценки эффективности функционирования ИАС // Информатика и вычислительная техника, №1, 1997. - С.87-90.

125. Статьев, В. Ю. Информационная безопасность на пространстве "Больших данных" / В. Ю. Статьев, В. А. Докучаев, В. В. Маклачкова // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 4. – С. 21-28. – DOI 10.36724/2072-8735-2022-16-4-21-28. – EDN IXUYWS.

126. Степанов С.Н. Оптимизация численного расчета характеристик многопотоковых моделей с повторными вызовами // Проблемы передачи информации. - 1989. Т.25. Вып.2. - С.67-78.

127. Степанов С.Н. Численные методы расчета систем с повторными вызовами / - М.: Наука. 1983. - 230 с.

128. Степанов, С. Н. Теория телетрафика: концепции, модели, приложения / С. Н. Степанов. – Москва : Научно-техническое издательство "Горячая линия-Телеком", 2015. – 868 с. – (Теория и практика инфокоммуникаций). – ISBN 978-5-9912-0543-6. – EDN UBWYWF.

129. Суторихин Н. Б. Оценка надежности элементов коммутируемых телефонных сетей. М., «Связь», 1974.

130. Таксономия видов ущерба от инцидента ИБ [Электронный ресурс] // Алексей Лукацкий "Бизнес без опасности". 2022: [сайт]. – URL: https://lukatsky.ru/business/taksonomiya-vidov-uscherba-ot-intsidenta-ib.html (дата обращения: 05.03.2025).

131. Трудовой кодекс Российской Федерации (ТК РФ) от 30.12.2001 N 197-ФЗ (ред. от 07.04.2025) [Электронный ресурс]: [федер. закон: принят Гос. Думой 21 дек. 2001г.: по состоянию на 07.04.2025г.] // СПС КонсультантПлюс: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 21.05.2025).

132. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025): [федер. закон: принят Гос. Думой 24 мая 1996г.: по состоянию на 02.05.2025г.] // СПС КонсультантПлюс: законодательство РФ. - URL: https://www.consultant.ru/document/ cons_doc_LAW_10699/ (дата обращения: 12.05.2025).

133. Ушаков И.А. Задачи расчета надежности. — М.: Знание, 1981

134. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ [федер. закон: принят Гос. Думой 08 июля 2006г.: по состоянию на 02.05.2025г] // СПС КонсультантПлюс:

законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 16.05.2025).

135. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных [федер. закон: принят Гос. Думой 08 июля 2006г.: по состоянию на 02.05.2025г.] // СПС КонсультантПлюс: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 21.05.2025).

136. Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [федер. закон: принят Гос. Думой 21 декабря 2022г.: по состоянию на 02.05.2025г.] // СПС КонсультантПлюс: законодательство РФ. - URL: https://www.consultant.ru/document/cons_doc_LAW_436110/ (дата обращения: 21.05.2025).

137. Филин Б.П. Методы анализа структурной надежности сетей связи. — М.: Радио и связь, 1988. - 208 с.

138. Цаленко М.Ш. Семантические и математические модели баз данных // ВИНИТИ, Серия «Информатика», том 9, - М., 1985.

139. Цикритзис Д., Лоховски Ф. Модели данных // «Финансы и статистика»,-М., 1985.

140. Шередин, Р. В. Защита персональных данных в информационных системах методом обезличивания : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени кандидата технических наук / Шередин Роман Валериевич. – Москва, 2011. – 138 с. – EDN QFRDOJ.

141. Шинаков К.Е. Анализ рисков безопасности информационных систем персональных данных [Текст]+[Электронный ресурс]: монография / К.Е.Шинаков, М.Ю.Рытов, О.М.Голембиовская– Брянск: БГТУ, 2017. – 220 с.

142. Шинаков, К.Е. Оценка риска безопасности информационных систем, обрабатывающих конфиденциальную информацию [Текст] + [Электронный ресурс] / Шинаков К.Е., Рытов М.Ю., Голембиовская О.М., Чиркова К.Ю. // Вестник БГТУ.-Брянск, 2016.-№1(48).-С.193-200.

143. Шинаков, К.Е. Формализация подходов к обеспечению защиты персональных данных [Текст]+[Электронный ресурс]: монография/О.М.Голембиовская, М.Ю.Рытов, К.Е.Шинаков – Брянск: БГТУ, 2014. – 182 с.

144. Шнепс-Шнеппе М.А. Системы распределения информации. Методы расчета // М.: Связь, 1979. – 342 с.

145. Шубин А.В. Модели обслуживания клиентов информационных систем / Е. А. Саксонов, А. В. Шубин // Современные информационные компьютерные технологии: сб. науч. ст.: Информационные системы и их приложения в производстве и управлении, 2009.

146. Шубинский И.Б. Надежные отказоустойчивые информационные системы. Методы синтеза /И.Б. Шубинский. – М.: «Журнал Надежность», 2016, – 546 с., ил.

147. Agosthazi M., Gosztony G. Traffic engineering method for a typical small telegraph station // Budavox Telecomm. Rev. - 1980. N 2.-P.13-18.

148. Alex Cârciu. Multicloud database management: Architectures, use cases, and best practices [Электронный ресурс] // Cloud Architecture Center. - URL: https://cloud.google.com/architecture/multi-cloud-database-management#contributors (дата обращения 17.05.2024).

149. Analysis of Data Risk Management Methods for Personal Data Information Systems / V. A. Dokuchaev, V. V. Maklachkova, D. V. Makarova, L. V. Volkova // 2020 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 19–20 марта 2020 года. – Moscow: Institute of Electrical and Electronics

Engineers Inc., 2020. – P. 9078547. – DOI 10.1109/IEEECONF48371.2020.9078547. – EDN XXGAVW.

150. Basharin G.P., Gaidamaka Yu.V., Samouylov K.E. Mathematical Theory of Teletraffic and Its Application to the Analysis of Multiservice Communication of Next Generation Networks // Automatic Control and Computer Sciences Journal. – 2013. – V. 47. – No. 2. – Pp. 62-69.

151. Berger I., Neal S. R. A sensitivity study of traffic parameter estimation procedures used for engineering trunk groups // In Proc. of the 7th International Teletrafic Congress. - Stockholm. - 1973. Prepr. book. Repr. N 542. - P. 1-7.

152. Biot J., Massant J. On the observation and augmentation of subscriber lines with high probability of being busy // In Proc. of the 9th International Teletrafic Congress. - Torremolinos. 1979 Prepr. book.

153. Bocharov, P. P. A single-server finite-capacity queueing system with Markov flow and discrete-time service / P. P. Bocharov, E. V. Viskova // Automation and Remote Control. – 2005. – Vol. 66, No. 1. – P. 233-248. – DOI 10.1007/s10513-005-0007-3. – EDN LJBUUX.

154. Bodard H., Guerineau J. P. Observations of the quality of service of International traffic by means of a minicomputer // In Proc. of the 9th International Teletrafic Congress. - Torremolinos. 1979. Prepr. Book.

155. Bohge M., Gross J., Wolisz A., Meyer M. Dynamic Resource Allocation in OFDM Systems: an Overview of Cross-Layer Optimization Principles and Techniques // IEEE Networks. – 2007. – V. 21. – No. 1. – Pp. 53-59.

156. Breier, Jakub, and Ladislav Hudec. "Risk analysis supported by information security metrics." In Proceedings of the 12th International Conference on Computer Systems and Technologies (CompSysTech '11). Association for Computing Machinery, New York, NY, USA, 393–398. https://doi.org/10.1145/2023607.2023673.

157. Bruneel H. Performance of discrete-time queueing systems // Computers and Operations Research. – 1993. – V. 20. – No.3. – Pp. 303-320.

158. C. b. Manjunath Reddy, U. k. reddy, E. Brumancia, R. M. Gomathi and K. Indira, "Integrative Approach Of Big Data And Network Attacks Analysis In Cloud

Environment," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 314-317, doi: 10.1109/ICOEI48184.2020.9142913.

159. Capozzi F., Piro G., Grieco L.A., Boggia G., Camarda P. Downlink Packet Scheduling in LTE Cellular Networks: Key Design Issues and a Survey // IEEE Communications Surveys & Tutorials. – 2013. – V. 15. – No. 2. – Pp. 678-700.

160. Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey, Risk management in data protection, International Data Privacy Law, Volume 5, Issue 2, May 2015, Pages 95–98, https://doi.org/10.1093/idpl/ipv005.

161. CobiT, Framework: Introduction and Methodology from ISACA [Электронный ресурс]. - URL: https://www.isaca.org/ (дата обращения 15.05.2024).

162. Cohen J. W. Basic problems of telephone traffic theory and the influence of repeated calls // Philips Telecomm. Rev. - 1957. 18. N 2. - P. 49-100.

163. Collaboration in Multicloud Computing Environments: Framework and Security Issues / Mukesh Singhal, Santosh Chandrasekhar, Merced Tingjian Ge, Lowell Ravi Sandhu, Ram Krishnan, Gail-Joon Ahn, Elisa Bertino. // IEEE Computer Society, 2013.- 76-84 с.

164. CORAS, Framework for Risk Analysis of Security Critical Systems [Электронный ресурс]. - URL: https://www.coras.com/ (дата обращения 28.05.2024).

165. CRAMM, the UK Goverment Risk Analysis and Management Method [Электронный ресурс]. - URL: http://www.cramm.com (дата обращения 15.05.2024).

166. D. B. Rawat, R. Doku and M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security," in IEEE Transactions on Services Computing, vol. 14, no. 6, pp. 2055-2072, 1 Nov.-Dec. 2021, doi: 10.1109/TSC.2019.2907247.

167. Daffy F. P., Mercer R. A. A study of network performance and customer behaviour during direct-distance-dialling call attempts in the USA // Bell Sys. Techn. J. - 1978. 57. N 1.- P.l-33.

168. Discrete time Markov chain model for analyzing characteristics of RACH procedure under massive machine Type Communications / E. Medvedeva, E. Zaripova,

O. Semenova, Y. Gaidamaka [et al.] // ACM International Conference Proceeding Series : 2, Amman, 26–27 июня 2018 года. – Amman, 2018. – P. 59. – DOI 10.1145/3231053.3231126. – EDN SIKNDY.

169. Dokuchaev, V. A. Architecture of the regional transport navigation and information systems / V. A. Dokuchaev, E. V. Gorban, V. V. Maklachkova // 2018 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, 14–15 марта 2018 года. – Moscow: Institute of Electrical and Electronics Engineers Inc., 2018. – P. 8350588-3. – DOI 10.1109/SOSG.2018.8350588. – EDN VCFXXK.

170. Dokuchaev, V. A. Classification of personal data security threats in information systems / V. A. Dokuchaev, V. V. Maklachkova, V. Yu. Statev // T-Comm. – 2020. – Vol. 14, No. 1. – P. 56-60. – DOI 10.36724/2072-8735-2020-14-1-56-60. – EDN QOGYHH.

171. Dokuchaev, V. A. Cybersecurity Impact on the Transport Security / V. A. Dokuchaev, V. V. Maklachkova // 2023 International Conference on Engineering Management of Communication and Technology, EMCTECH 2023 : Proceedings, Vienna, Austria, 16–18 октября 2023 года. – New York: Institute of Electrical and Electronics Engineers Inc., 2023. – P. 10297009. – DOI 10.1109/EMCTECH58502.2023.10297009. – EDN OETMVX.

172. Dokuchaev, V. A. Data subject as augmented reality / V. A. Dokuchaev, V. V. Maklachkova, V. Yu. Statyev // Synchroinfo Journal. – 2020. – Vol. 6, No. 1. – P. 11-15. – DOI 10.36724/2664-066X-2020-6-1-11-15. – EDN ULPVZC.

173. Dokuchaev, V. A. Digital transformation: New drivers and new risks / V. A. Dokuchaev // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings, Vienna, 20–22 октября 2020 года. – Vienna, 2020. – P. 9261544. – DOI 10.1109/EMCTECH49634.2020.9261544. – EDN VWIIZW.

174. Dokuchaev, V. A. The System of Indicators for Risk Assessment in High-Loaded Infocommunication Systems / V. A. Dokuchaev, E. V. Gorban, V. V. Maklachkova // 2019 Systems of Signals Generating and Processing in the Field of on Board

Communications, SOSG 2019, Moscow, 20–21 марта 2019 года. – Moscow, 2019. – P. 8706726. – DOI 10.1109/SOSG.2019.8706726. – EDN WFULUV.

175. ENISA (2021), Interoperable EU Risk Management Framework [Электронный ресурс]. - URL: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework (дата обращения 15.05.2024).

176. ETSI TS 102 165-1, Threat vulnerability and risk analysis (TVRA) [Электронный ресурс]. – URL: https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ ts_10216501v050203p.pdf, ETSI Technical Committee Cyber Security (дата обращения 15.01.2024).

177. Evers R. A survey of subscriber behaviour including repeated call attempts results of measurements in two PABX's // In Proc of the 6th Intern. Symp. on Hum. Factors in Telecomm. - Stockholm. 1972. Prepr. book. IV. 4. - P. 1-12.

178. Evers R. Analysis of traffic flows on subscriber-lines dependent of time and Subscriber-class // In Proc. of the 8th International Teletrafic Congress. – Melbourne. 1976. Prepr. book. Repr. N 345. - P. 1-8.

179. Evers R. Measurement of subscriber reaction to unsuccessful call attempts and the influence of reasons of failure // In Proc. of the 7th International Teletrafic Congress. - Stockholm. 1973. Prepr. book. Repr. N 544. - P. 1-8.

180. Evers R. The structure of traffic offered by different groups of users // In roc of the 7th Intern. Symp. on Hum. Factors in Telecomm. -Montreal. 1974.

181. Evers R., Мам К. Influencing the efficiency rate of the international network by different inodes of handling ineffective call attempts // In Proc. of the Intern. Switching Symp. - Munich. 1974.

182. F. Kunz and Z. Á. Mann, "Finding Risk Patterns in Cloud System Models," 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), Milan, Italy, 2019, pp. 251-255, doi: 10.1109/CLOUD.2019.00051.

183. Features of supporting decision making in modern enterprise infocommunication systems / S. V. Pavlov, V. A. Dokuchaev, V. V. Maklachkova, S. S. Mytenkov // T-Comm. – 2019. – Vol. 13, No. 3. – P. 71-74. – DOI 10.24411/2072-8735-2018-10252. – EDN VZZCPY.

184. Gellert, Raphaël. / Data protection - a risk regulation : Between the risk management of everything and the precautionary alternative. In: International Data Privacy Law. 2015 ; Vol. 5, No. 1. pp. 3-19.…

185. Gosztony G. Repeated call attempts and their effect on traffic engineering // Budavox Telecomm. Rev. - 1976. N 2.-P. 16-26.

186. H. Ye, X. Cheng, M. Yuan, L. Xu, J. Gao and C. Cheng, "A survey of security and privacy in big data," 2016 16th International Symposium on Communications and Information Technologies (ISCIT), Qingdao, China, 2016, pp. 268-272, doi: 10.1109/ISCIT.2016.7751634.

187. Hashida 0., Kawashima K. Buffer behavior with repeated calls // Electron, and Communicat. Jap. - 1979. 62-B. N 3.-P. 27-35.

188. IEC 31010:2019 «Risk management - Risk assessment techniques».

189. ISO/IEC 15408 series - Information technology - Security techniques - Evaluation criteria for IT security [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 15.09.2023).

190. ISO/IEC 23894:2023 Information technology - Artificial intelligence - Guidance on risk management [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 25.09.2023).

191. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 15.09.2023).

192. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 15.09.2023).

193. ISO/IEC 27005:2018 «Information technology - Security techniques - Information security risk management» [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 10.12.2023).

194. ISO/IEC 5140:2024 Information technology - Cloud computing Concepts for multi-cloud and the use of multiple cloud services [Электронный ресурс]. – URL: https://www.iso.org (дата обращения 20.06.2024).

195. Jakub Breier and Ladislav Hudec. 2011. Risk analysis supported by information security metrics. In Proceedings of the 12th International Conference on Computer Systems and Technologies (CompSysTech '11). Association for Computing Machinery, New York, NY, USA, 393–398. https://doi.org/10.1145/2023607.2023673.

196. Jitendra Sayanekar Understanding Multi-Cloud Network Architecture Patterns and Security [Электронный ресурс]. – URL: https://www.calsoftinc.com/blogs/understanding-multi-cloud-network-architecture-patterns-and-security.html (дата обращения 29.09.2024).

197. Kelly F.P. Reversibility and Stochastic Networks // Chichester: John Wiley & Sons, 1979. – 630 p

198. Kennedy A Torkura, Muhammad IH Sukmana, Feng Cheng, and Christoph Meinel. 2021. Continuous auditing and threat detection in multi-cloud infrastructure. Computers & Security 102 (2021), 102124.

199. Klimenok V., Dudin A. Dual tandem queueing system with multiserver stations and retrials // In: Proc. Int. Conf. on Distributed computer and communication networks: control, computation, communications (DCCN-2013), Moscow, Russia, 7-10 October 2013. – Moscow: Technosfera, 2013. – Pp. 394-401.

200. Kobayashi H., Konheim A. Queueing Models for Computer Communications System Analysis // IEEE Trans. Communications. – 1977. – V. 25. – No. 1. – Pp. 2-29.

201. Learn About Multicloud Architecture Framework [Электронный ресурс]. - URL: https://docs.oracle.com/en/solutions/learn-about-multicloud-arch-framework/index.html#GUID-D2C31879-5A92-4101-9246-54420BBC8419 (дата обращения 11.11.2024).

202. Liu K. S. Direct distance dialing: call completion and customer retrial behaviour // Bell Sys. Techn. J. - 1980. 59. N 3.-P. 295-311.

203. Lopatina, K. Data Risks Identification in Healthcare Sensor Networks / K. Lopatina, V. A. Dokuchaev, V. V. Maklachkova // 2021 International Conference on

Engineering Management of Communication and Technology, EMCTECH 2021 - Proceedings, Vienna, 20–22 октября 2021 года. – Vienna, 2021. – DOI 10.1109/EMCTECH53459.2021.9619178. – EDN GAVTTO.

204. Macfadyen N. W. Statistical observation of repeat attempts in the arrival process // In Proc. of the 9th International Teletrafic Congress. Torremolinos. 1979. - Prepr. Book.

205. Majid Mollaeefar, Silvio Ranise Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR, Computers & Security, Volume 129, 2023, 103206, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103206.

206. Maklachkova, V. V. Risks identification in the exploitation of a geographically distributed cloud infrastructure for storing personal data / V. V. Maklachkova, V. A. Dokuchaev, V. Y. Statev // 2020 International Conference on Engineering Management of Communication and Technology, EMCTECH 2020 - Proceedings, Vienna, 20–22 октября 2020 года. – Vienna, 2020. – P. 9261541. – DOI 10.1109/EMCTECH49634.2020.9261541. – EDN EQOLNB.

207. Marwan Al Shawi and other contributors, Build hybrid and multicloud architectures using Google Cloud [Электронный ресурс] // Cloud Architecture Center. - URL: https://cloud.google.com/architecture/hybrid-multicloud-patterns (дата обращения 30.05.2024).

208. Marwan Al Shawi and other contributors, Hybrid and multicloud architecture patterns [Электронный ресурс] // Cloud Architecture Center. - URL: https://cloud.google.com/architecture/hybrid-multicloud-patterns-and-practices (дата обращения: 30.05.2024).

209. Microsoft Threat Modeling Tool threats [Электронный ресурс] // Microsoft: [сайт]. 2022. — URL: https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (дата обращения: 30.05.2024).

210. MITRE, 2015-2021. MITRE ATT&CK. [Электронный ресурс]. - URL: https://attack.mitre.org/ (дата обращения 28.05.2024).

211. Multi-Cloud and Hybrid Cloud Guide [Электронный ресурс] // CSA: [сайт]. 2021. – URL: https://www.cio.gov/assets/resources/MultiCloud%20and%20Hybrid%20Cloud%20Guide_v4_Final.pdf (дата обращения: 30.05.2024).

212. Myskja A., Wallmann 0. 0. An investigation of telephone user habits by means of computer technics// In Proc. of the 6th Intern. Symp. on Hum. Factors in Telecomm. – Stockholm. 1972. Prepr. book. IV. 3. -P. 2-12.

213. Myskja A., Walmann 0. 0. A statistical study of telephone traffic data, with emphasis on subscriber behaviour // In Proc. of the 7th International Teletrafic Congress. - Stockholm. 1973 Prepr. book. Repr. N 132. - P. 1-7.

214. N. Chitransh, C. Mehrotra and A. S. Singh, "Risk for big data in the cloud," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 277-282, doi: 10.1109/CCAA.2017.8229815.

215. NIST SP 800-30 REV.1, Guide for Conducting Risk Assessments (https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, USA).

216. NIST SP 800-37 REV. 2, Risk Management Framework [Электронный ресурс]. - URL: https://www.nist.gov/cyberframework/risk-management-framework, USA (дата обращения 28.05.2024).

217. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View [Электронный ресурс]. - URL: https://csrc.nist.gov/pubs/sp/800/39/final (дата обращения 28.05.2024).

218. OCTAVE, Framework for identifying and managing information security risks [Электронный ресурс]. - URL: https://insights.sei.cmu.edu/documents/2312/2020_004_001_644641.pdf (дата обращения 07.06.2024).

219. OWASP, Risk Assessment Framework [Электронный ресурс]. - URL: https://owasp.org/www-project-risk-assessment-framework/migrated_content (дата обращения 07.06.2024).

220. RiskWatch, Software for managing risk, security, compliance [Электронный ресурс]. - URL: https://www.riskwatch.com/ (дата обращения 07.06.2024).

221. Rory Duncan. 2020. A multi-cloud world requires a multi-cloud security approach. Computer Fraud & Security 2020, 5 (2020), 11–12.

222. SANS, Cyber risk management essentials practical [Электронный ресурс]. - URL: https://www.sans.org/webcasts/cyber-risk-management-essentials-practical-ciso/ (дата обращения 23.12.2023).

223. Semantic Model of Knowledge Bases Representation and Processing /V.V. Golenkov, N.A. Guliakina, I.T. Davydenko, D.V. Shunkevich // ФИЦ ИУ РАН, Москва, Российская Федерация, 2017- 8 с.

224. Stepanov S.N. Asymptotic analysis models with repeated calls in case of extreme load // In Proc. of the 13th International Teletraffic Congress.-1991. Copenhagen.- 7 p. N6, - C.19-26.

225. Stepanov S.N. Optimal calculation of characteristics of models with repeated calls // In Proc. of the 12th International Teletraffic Congress. - 1988. Torino. - P.l-7.

226. T. V. Rykova. Towards the analysis of the performance measures of heterogeneous networks by means of two-phase queueing systems // Discrete and Continuous Models and Applied Computational Science 29 (3) (2021) 242–250. DOI: 10.22363/2658- 4670-2021-29-3-242-250.

227. Takagi H. Queueing Analysis, Vol. III: Discrete-Time Systems. // Amsterdam: North-Holland Publishing, 1993. – 470 p.

228. Titov I., Tsitovich I., Poryazov S. Use of time-scale for analysis of data source traffic // BWWQT 2013. Berlin: Springer-Verlag. Communications in Computer and Information Science. - 2013. - Vol. 356. - P. 187-197.

229. V. S. Bhamidipati and S. De, "A Risk Based Approach for Privacy Compliant Machine Learning Lifecycle," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022, pp. 1-6, doi: 10.1109/CONIT55038.2022.9847739.

230. Vishnevsky V., Larionov A., Semenova O. and Ivanov R. State reduction in analysis of a tandem queueing system with correlated arrivals // 16th International Conference on Information Technologies and Mathematical Modelling. – Vol.800. – 2017. – Pp.215–230.

231. Wilkinson R.I. Theories for toll traffic engineering in the USA // Bell Sys. Techn. J. - 1956. 35. N 2.-P. 421-514.

232. Wilkinson R.I., Radnik R. C. Customer retrials in toll circuit operation // In Proc. of the IEEE Intern. Conf. on Commun. Record.- 1968. Vol. 4. - P. 9-14.

233. Wilkinson R.I., Radnik R. C. The character and effect of customer retrials in intertoll circuit operation // In Proc. of the 5th International Teletrafic Congress. - New York. 1967.

234. Wu D., Ci S., Zhang W., Zhang J. Cross-Layer Rate Adaptation for Video Communications over LTE Networks // In: Proc. IEEE Global Communications Conference. Anaheim, CA, 2012. – Pp. 5056-5061.

Приложение А. Основные сценарии воздействий на процесс обработки персональных данных

Одним из важных аспектов анализа рисков нарушения качества персональных данных при их автоматизированной обработке является возможность прогноза технологий реализации вероятных (актуальных) угроз с использованием сценариев информационного воздействия.

В таблице А.1 представлены возможные варианты моделей воздействия на ИСПДн и в качестве источников угроз, которые способны оказать влияние на процесс обработки персональных данных, рассматриваются нижеперечисленные типы субъектов:

- пользователь внешней информационной системы;
- локальный пользователь, имеющий легитимное право доступа к ИСПДн;
- удалённый пользователь, имеющий легитимное право доступа к ИСПДн;
- работник, не обладающим правом доступа к ИСПДн, но имеющий доступ на территорию объекта;
- администратор ИСПДн;
- администратор безопасности ИСПДн;
- разработчик ИСПДн.

Таблица А.1 – Возможные сценарии воздействия на процесс обработки персональных данных в ИСПДн

Источник	**Цель осуществления воздействия**	**Возможные сценарии воздействия**
Пользователь внешней информационной системы	Анализ ИСПДн с целью обнаружения уязвимостей	• осуществление перехвата данных учётных записей; • подбор паролей к учётным записям; • осуществление сбора информации о ИСПДн; • осуществление анализа трафика сети.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• внедрение вредоносного программного обеспечения; • несанкционированная передача пакетов данных; • искажение пакетов данных; • осуществление перехвата пакетов; • нарушение адресности; • вставка ложной информации или вредоносных команд в обычный поток данных; • нарушение регламентированной скорости передачи пакетов персональных данных; • несанкционированное изменение или удаление данных; • нарушение функционирования канала передачи данных; • нарушение регламента взаимодействия с ИС.
	Доступ к персональным данным	• осуществление копирования, модификации, удаления, блокирования, кражи персональных данных;

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
		• подбор пароля; • поиск уязвимостей в механизмах шифрования.
	Непреднамеренные воздействия	• распространение вредоносного программного обеспечения; • превышение регламентированной нагрузки на ИСПДн из-за осуществленных по ошибке действий.
Локальный пользователь, имеющий легитимное право доступа к ИСПДн	Поиск возможности доступа к программным модулям и базам данных ИСПДн, к которым он не имеет права доступа	• осуществление наблюдения за другими сотрудниками, имеющими доступ к персональным данным, чтение данных с их мониторов; • изучение любой корпоративной документации, располагающей важными сведениями; • осуществление установки и запуска системных программ, которые позволяют собрать особо важные сведения, касающиеся архитектуры и системного взаимодействия ИСПДн; • установление технологий и принципов обработки персональных данных; • доступ к базам данных, в которых хранятся данные учётных записей, хищение этих данных.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• ошибки в выполнении своих должностных функций при работе с персональными данными, совершённые преднамеренно; • физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • превышение регламентированной нагрузки на ИСПДн из-за осуществленных по ошибке действий; • превышение регламентированной нагрузки на ИСПДн, операционную систему; • ввод неверных, неполных или неактуальных данных; • неверное изменение или удаление персональных данных.
	Доступ к персональным данным	• осуществление хищения съёмных носителей персональных данных; • осуществление копирования персональных данных, с входом в систему с помощью чужой учётной записью; • осуществления копирования персональных данных с несанкционированным использованием служебных программ или утилит; • передача персональных данных по электронной почте.

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
	Непреднамеренные воздействия	• ошибки в выполнении своих должностных функций при работе с персональными данными; • физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • превышение регламентированной нагрузки на ИСПДн из-за осуществленных по ошибке действий; • превышение регламентированной нагрузки на ИСПДн, операционную систему; • ввод неверных, неполных или неактуальных данных; • неверное изменение или удаление персональных данных; • передача персональных данных по электронной почте.
Удалённый пользователь, имеющий легитимное право доступа к ИСПДн	Поиск возможности доступа к программным модулям и базам данных ИСПДн, к которым он не имеет права доступа	• осуществление наблюдения за другими сотрудниками, имеющими доступ к персональным данным, чтение данных с их устройств; • изучение любой корпоративной документации, располагающей важными сведениями; • осуществление установки и запуска системных программ, которые позволяют собрать особо важные сведения, касающиеся архитектуры и системного взаимодействия ИСПДн; • выявление технологий и принципов обработки персональных данных; • доступ к базам данных, в которых хранятся данные учётных записей, хищение этих данных; • осуществление сбора информации о ИСПДн с помощью общедоступных данных и приложений.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• ошибки в выполнении своих должностных функций при работе с персональными данными, совершённые преднамеренно; • физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • превышение регламентированной нагрузки на ИСПДн, операционную систему; • ввод неверных, неполных или неактуальных данных; • неверное изменение или удаление персональных данных.
	Доступ к персональным данным	• вывод данных на съёмные носители персональных данных;

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
		• осуществление пересылки персональных данных по корпоративной и внешней электронной почте; • осуществление копирования персональных данных, с входом в систему с помощью чужой учётной записью.
	Непреднамеренные воздействия	• ошибки в выполнении своих должностных функций при работе с персональными данными; • физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • превышение регламентированной нагрузки на ИСПДн, операционную систему; • ввод неверных, неполных или неактуальных данных; • неверное изменение или удаление персональных данных; • доступ к данным посторонних лиц (например, членов семьи).
Работник, не обладающим правом доступа к ИСПДн, но имеющий доступ на территорию объекта	Доступ к автоматизированному рабочему месту (АРМ) работника, уполномоченного/ ответственного в организации за работу с персональными данными, серверам корпоративной ИСПДн, базам данных и хранилищам персональных данных	• установление мест нахождения АРМов, серверов, баз данных и хранилища данных; • выявление информационных систем обработки персональных данных и СУБД; • изучение режима и правил допуска в помещения, а также к ресурсам ИСПДн; • хищение данных учётных записей легитимных пользователей; • взлом и хищение криптографических ключей легитимных пользователей.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения, имеющее катастрофические последствия.
	Доступ к персональным данным	• установка электронного устройства перехвата данных; • внедрение вредоносного программного обеспечения, в том числе использующее уязвимости ИСПДн; • хищение носителей персональных данных; • копирование данных под видом легитимного пользователя ИСПДн.

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
	Непреднамеренные воздействия	• физическое нарушение функционирования программных и/или технических средств; • непреднамеренное получение сведений об действующих системах доступа и категориях персональных данных.
Администратор ИСПДн	Проведение анализа способов хранения, распространения и иных действий, направленных на персональные данные, а также проведение анализа средств разграничения доступа к данным, не входящих в круг его компетенций в организации	• осуществление прослушки разговоров других администраторов и персонала подразделения управления информационной безопасности; • получение доступа к любой корпоративной документации, из которой можно получить любые сведения о ИСПДн; • осуществление неправомерной установки и запуска системных программ и утилит, которые дают возможность осуществлять копирование данных из оперативной памяти системы, а также с любого вида съёмных носителей; • неправомерное получение (хищение или вскрытие) идентификаторов, ключей, паролей учётных записей.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• физическое нарушение функционирования программных и/или технических средств; • преднамеренное блокирование сервисов или информационных ресурсов ИСПДн; • внедрение вредоносного программного обеспечения; • умышленные ошибки при исполнении своих должностных обязанностей и функций при описании полномочий пользователей для предоставления доступа к ИСПДн; • несанкционированное удаление или изменение системных файлов.
	Доступ к персональным данным	• осуществление копирования баз данных и иных файлов, содержащих персональные данные, с использованием низкоуровневого программного обеспечения и иных системных утилит; • осуществление копирования персональных данных с использованием чужой учётной записи; • создание временной учётной записи «несуществующего» пользователя для осуществления доступа к персональным данным и их копированию; • распространение информации о средствах защиты и разграничения доступа; • осуществление пересылки персональных данных по корпоративной и внешней электронной почте; • осуществление хищения носителей персональных данных.

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
	Непреднамеренные воздействия	• физическое нарушение функционирования программных и/или технических средств; • осуществление блокировки информационных ресурсов и иных сервисов ИСПДн; • случайные ошибки при исполнении своих должностных обязанностей и функций при описании полномочий пользователей для предоставления доступа к ИСПДн; • непреднамеренные изменения или удаление системных утилит и файлов.
Администратор безопасности ИСПДн	Не требуется проведение анализа	• получение любой информации о ИСПДн санкционированным способом.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • умышленные ошибки при исполнении своих должностных обязанностей и функций; • установка и запуск утилит или программ, нарушающих работоспособность системы; • получение доступа к ресурсам, которые вызывают увеличение нагрузки в сети; • умышленное нарушение политик установленных средств защиты.
	Доступ к персональным данным	• осуществление копирования баз данных и иных файлов, содержащих персональные данные, с использованием низкоуровневого программного обеспечения и иных системных утилит; • осуществление копирования персональных данных с использованием чужой учётной записи; • распространение информации о средствах защиты и разграничения доступа; • осуществление хищения носителей персональных данных.
	Непреднамеренные воздействия	• физическое нарушение функционирования программных и/или технических средств; • случайное внедрение вредоносного программного обеспечения; • случайные ошибки при исполнении своих должностных обязанностей и функций; • неумышленное нарушение политик установленных средств защиты.

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
Разработчик ИСПДн	Анализ ИСПДн, баз данных и хранилищ персональных данных	• осуществление наблюдения за другими сотрудниками, имеющими доступ к персональным данным; • получение доступа к корпоративной документации, из которой можно получить любые сведения о ИСПДн; • осуществление неправомерной установки и запуска системных программ и утилит, которые дают возможность осуществлять сбор информации о программном и информационном обеспечениях ИСПДн; • применение инструментальных средств разработки программного обеспечения для получения критически важной информации о ИСПДн и системе защиты; • неправомерное получение (хищение или вскрытие) идентификаторов, ключей, паролей учётных записей.
	Нарушение функционирования программных, технических средств, технологических процессов ИСПДн	• физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • включение при разработке в обеспечивающие подсистемы ИСПДн вредоносных недекларированных функций; • использование инструментальных средств разработки для несанкционированного изменения рабочих обеспечивающих подсистем ИСПДн; • умышленные ошибки при установке, настройке или модификации ИСПДн.
	Доступ к персональным данным	• осуществление копирования персональных данных с использованием чужой учётной записи; • хищение носителей персональных данных; • несанкционированное использование инструментальных средств разработки и системных утилит для копирование персональных данных; • передача персональных данных по электронной почте.
	Непреднамеренные воздействия	• физическое нарушение функционирования программных и/или технических средств; • внедрение вредоносного программного обеспечения; • непреднамеренные ошибки в процессе установки, модификации или настройки ИСПДн и утилит; • ошибки в коде программ;

Источник	Цель осуществления воздействия	Возможные сценарии воздействия
		• осуществление передачи персональных данных по электронной почте.

Для разработки таких сценариев целесообразно расширить классификацию угроз персональным данным, обрабатываемым в ИСПДн. В [170] автором дополнительно предлагается классификация таких угроз по следующим критериям:

- по видам возможных источников угроз безопасности персональных данных, вызванного умышленными или непреднамеренными действиями пользователей ИСПДн: с доступом или без доступа к ней. Следует отметить, что источники угроз по отношению к ИСПДн могут быть как внешними, так и внутренними;
- по типу несанкционированных действий, совершенных с персональными данными:
  - угрозы, ведущие к нарушению конфиденциальности персональных данных (копирование или несанкционированное распространение), реализация которых напрямую не влияет на содержание информации;
  - угрозы, ведущие к несанкционированному, в том числе случайному, влиянию на содержание информации, в результате которого персональные данные изменяются или уничтожаются;
  - угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные и/или аппаратные элементы информационной системы, в результате чего персональные данные блокируются;
- по методам реализации угрозы безопасности персональных данных:
  - угрозы, реализуемые в ИСПДн при их подключении к сетям связи общего пользования;
  - угрозы, реализуемые в ИСПДн при их подключении к международным сетям обмена информацией;
  - угрозы, реализованные в ИСПДн, не имеющих подключения к сетям связи общего пользования и интернету;
- по типу каналов реализации угрозы безопасности персональных данных:
  - угрозы, реализуемые по каналам, возникающим в результате использования технических средств перехвата персональных данных, обрабатываемых в ИСПДн;
  - угрозы, реализуемые в результате несанкционированного доступа к персональным данным в ИСПДн с использованием стандартного программного обеспечения или специально разработанного или прикладного программного обеспечения.

Для поддержания взаимодействия элементов территориально распределённой ИСПДн с облачной архитектурой необходимо применять коммуникационные ресурсы внешних по отношению к ИСПДн информационных систем. В таких условиях использование корпоративных ИСПДн с возможностью накопления больших объёмов данных ведёт к увеличению угроз нарушения качества обрабатываемых данных или эффективности использования ресурсов как отдельных элементов ИСПДн, так и всей ИСПДн в целом. Поэтому предлагается дополнить классификацию угроз по уровням типовой модели разделением угроз на внутренние и внешние.

К внешним угрозам относятся несанкционированный доступ пользователей внешних систем либо ошибки или технические сбои со стороны внешних информационных систем, которые влияют на отдельные элементы ИСПДн (сетевое оборудование, рабочие станции,

сервера, базы данных и т.д.), её работоспособность, нарушают процессы взаимодействия с ней или её взаимодействие с другими внешними системами. Внутренние угрозы представляют собой несанкционированный доступ или ошибки пользователей или администраторов/разработчиков ИСПДн, которые могут привести к сбоям отдельных её элементов или нарушению работоспособности в целом, а также технические сбои, влияющие на процессы обработки персональных данных.

Кроме того, для создания сценариев воздействия необходимо определить и классифицировать потенциальные факторы воздействия на саму систему, а также на процессы обработки персональных данных в ней для последующей параметризации этих факторов.

Основные факторы воздействия на информацию (в том числе персональные данные) в процессе её обработки, которые могут влиять на безопасность защищаемой информации и способствовать нанесению ущерба организации (оператору персональных данных), определены в ГОСТ Р 51275-2006 «Объект информатизации. Факторы, воздействующие на информацию. Общие положения» [26]. Этот стандарт также устанавливает требования по защите информации при создании и эксплуатации объектов информатизации.

Согласно [31] под безопасностью персональных данных понимается состояние защищённости персональных данных, которое характеризуется способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в ИСПДн. Таким образом под факторами, воздействующими на процесс обработки персональных данных и которые могут приводить к реализации определенных информационных рисков на защищаемую информацию, будем понимать процессы, явления, действия или события, которые:

- могут повлечь нарушение характеристик качества персональных данных, а именно конфиденциальности, доступности и целостности;
- могут создать условия для реализации рисков утечки, хищения или модификации обрабатываемых персональных данных.

Для того, чтобы провести классификацию возможных воздействий на персональные данные в процессе их автоматизированной обработки, следует привести все возможные признаки этих воздействий. Признаками могут являться как цели воздействия, так и характер используемой уязвимости. У каждого признака воздействия есть свой параметр воздействия, то есть именно тот элемент ИСПДн, на который и осуществляется воздействие. Применительно к ИСПДн с облачной структурой эту систему классификации факторов воздействия, которые могут приводить к реализации определённых информационных рисков, можно представить в виде таблицы А.2. Для классификации были использованы источники, рассмотренные в разделе 1.1, документы ФСТЭК [6,81], ГОСТ Р 51275-2006 [26].

Таблица А.2 – Система классификации факторов воздействия на ИСПДн с облачной структурой

№	Признак классификации	Значение параметра
1	Цель воздействия на ИСПДн	• Нарушение конфиденциальности • Нарушение доступности • Нарушение целостности
2	Принцип воздействия на ИСПДн	• Применение текущих штатных каналов воздействия • Применение текущих специальных каналов воздействия • Создание новых каналов воздействия

№	Признак классификации	Значение параметра
3	Элемент воздействия ИСПДн	• Информационное обеспечение • Программное обеспечение • Техническое обеспечение • Физическо-инженерное обеспечение • Кадровое обеспечение • Организационно-нормативное обеспечение • Облачное хранилище
4	Характер возникновения (воздействие)	• Преднамеренное воздействие • Непреднамеренное воздействие
5	Модель воздействия на ИСПДн	• Внешний субъект по отношению к ИСПДн • Внутренний субъект по отношению к ИСПДн • Локальный легитимный пользователь ИСПДн • Удалённый легитимный пользователь ИСПДн • Администратор ИСПДн • Администратор безопасности ИСПДн • Разработчик ИСПДн • Локальный нелегитимный пользователь ИСПДн • Удалённый нелегитимный пользователь ИСПДн
6	Характер воздействия на процесс обработки персональных данных	• Активное – нарушение, разрушение, искажение процесса • Пассивное внутреннее – сбор и анализ внутренних факторов процесса • Пассивное внешнее – сбор и анализ внешних факторов процесса
7	Этапы жизненного цикла ИСПДн	• Проектирование • Разработка • Внедрение • Эксплуатация • Модернизация • Вывод из эксплуатации
8	Причины информационных рисков	• Применение технических средств • Использование программного обеспечения • Человеческий фактор • Использование сети передачи данных • Естественные и природные факторы • Применение специальных средств защиты информации • Применение облачных технологий для хранения и обработки персональных данных
9	Тип потенциального ущерба	• Минимальный: последствиями можно пренебречь • Низкий: последствия легко устранимы, затраты на ликвидацию минимальны, воздействие на процесс обмена информацией невелико • Средний: ликвидация последствий не слишком затратно, воздействие на процесс обмена информацией невелико и не затрагивает критических фрагментов

№	Признак классификации	Значение параметра
		• Высокий: ликвидация последствий требует больших затрат, воздействие на процесс обмена информацией высокое и затрагивает критические фрагменты • Катастрофический: ликвидация последствий невозможна, процесс обмена информацией находится в деструктивном состоянии
10	Характер используемой уязвимости	• Объективная уязвимость • Субъективная уязвимость • Случайная уязвимость
11	Место возникновения	• Внешние • Внутренние
12	Причина возникновения	• Неполнота технического обеспечения • Неполнота организационных действий

Путём объединения указанных классификаторов можно определить комплекс неблагоприятных внешних и внутренних факторов, их влияние на ИСПДн, а также выявить потенциальные угрозы нарушения свойств качества персональных данных в процессе их обработки. Под угрозой будем понимать совокупность условий или факторов, представляющих потенциальную опасность для элементов ИСПДн и процессов работы с персональными данными.

Реализация любой из угроз становится возможной при наличии в ИСПДн уязвимостей. Определим уязвимость, как недостаток аппаратного, программного или аппаратно-программного элемента или всей информационной системы в целом, который может быть использован для реализации угроз процессу обработки персональных данных.

В таблице А.2 определено, что уязвимости ИСПДн бывают трех видов: объективные, субъективные и случайные.

К *объективным уязвимостям* относятся те, которые зависят от способа построения ИСПДн, а также от её технических характеристик. Для подобного типа уязвимостей полное устранение является невозможным, но использование отдельных способов противодействия угрозам минимизирует вероятность использования этих уязвимостей. К подобному типу уязвимостей в ИСПДн предлагается отнести:

1. Излучение, которое сопутствует техническим средствам:
   - электромагнитные;
   - электрические;
   - звуковые.
2. Активизируемые:
   - аппаратные устройства, которые устанавливаются в телефонных линиях, в сети электропитания, в технических средствах, а также в помещениях;
   - программные средства, к примеру, вредоносное программное обеспечение или его нелегальные копии.
3. Устанавливаемые особенностями структурных элементов:
   - элементы, которые обладают способностью к электроакустическому преобразованию (телефон, громкоговоритель, катушка индуктивности, микрофон, дроссель, трансформатор и т.д.);

- элементы, которые подвергаются воздействию электромагнитного поля.

4. Определяемые особенностями объекта информатизации:
   - расположением объекта (отсутствие или наличие зоны под контролем; наличием доступных в прямой видимости объектов, далеко расположенных и легко перемещаемых элементов объекта; вибрирующих поверхностей, способных отражать сигнал);
   - способностью создания каналов обмена данными (радиоканалы, глобальные сети, арендуемые каналы).

Субъективные уязвимости являются напрямую зависимыми от действий персонала и в большинстве случаев их можно устранить с помощью организационных и программно-аппаратных методов. К таким уязвимостям могут относиться:

1. Ошибки в процессе подготовки и при эксплуатации прикладного программного обеспечения (разработка алгоритмов; разработка, установка, загрузка и эксплуатация программного обеспечения; ввод информации);
2. Нарушения:
   - нарушение доступа к техническим средствам, нарушение режима доступа на объект;
   - нарушение процесса использования технических средств;
   - нарушение правил использования данных (нарушение правил обработки или обмена данными, правил хранения и/или уничтожение физических или виртуальных носителей данных);
   - нарушение правил конфиденциальности (несанкционированный доступ персонала в нерабочее время или уволенных работников).

Случайные уязвимости являются зависимыми от происходящих событий в окружающей среде объекта информатизации, а также от случайных обстоятельств, которые невозможно предвидеть. Данные факторы являются непредсказуемыми, а их минимизация или полное устранение возможно только в случае проведения комплекса мер, направленных на противодействие угрозам безопасности персональных данных. Комплекс мер должен быть как организационным, так и инженерно-техническим. Ниже приведен список возможных случайных уязвимостей:

1. Сбои и отказы:
   - неисправности или отказы средств, которые обрабатывают информацию о персональных данных, обеспечивают надлежащую работы средств обработки персональных данных, а также средств, которые обеспечивают контроль доступа и охрану объекта;
   - возможное размагничивание физических носителей информации или структурных элементов системы (съёмные носители, жёсткий диск, элементы микросхемы, кабели, соединительные линии);
   - сбой программного обеспечения, СУБД, прикладного программного обеспечения, средств защиты;
   - сбой в электропитании систем, которые обрабатывают данные, а также вспомогательного оборудования.
2. Повреждения:
   - коммуникаций, обеспечивающих жизнедеятельность (электричество, водоснабжение, газоснабжение, отопление, канализация, вентиляция, кондиционирование);

- конструкций, ограждающих территорию, а также стен и перекрытий корпусов, в которых располагается технологическое оборудование.

Кроме того, следует выделить классы и типы уязвимостей по следующим признакам:

- Область происхождения:
  - программная уязвимость (ошибки в программном коде);
  - конфигурационная уязвимость (ошибки при конфигурации системы или отдельных её элементов);
  - архитектурная уязвимость (ошибки при проектировании системы, неправильный выбор архитектуры или её недостатки);
  - организационная уязвимость (ошибки в регламентах по работе с системой или их несоблюдение);
  - многофакторная уязвимость (совокупность нескольких типов уязвимостей).
- Тип недостатка ИСПДн:
  - неверная настройка параметров программного обеспечения, отсутствие необходимых параметров, наличие избыточных или неопределённых параметров;
  - отсутствие, неполнота или избыточность проверки входных данных;
  - возможность прослеживания доступа к месту хранения данных;
  - возможность неконтролируемого выполнения команд операционной системы;
  - возможность внедрения произвольного кода и скриптов через веб-страницы;
  - используемые языки и средства программирования;
  - различные ошибки в программном обеспечении;
  - отсутствие политики разграничения доступа или ошибки при её реализации.
- Место проявления уязвимости:
  - общесистемное программное обеспечение (операционная система, система управления базами данных и т.д.);
  - прикладное программное обеспечение (офисные пакеты и т.д.);
  - специальное программное обеспечение для решения задач ИСПДн;
  - технические средства (процессоры, запоминающие устройства, контроллеры, портативные устройства и т.д.);
  - сетевое оборудование (маршрутизаторы, коммутаторы, сетевые протоколы и т.д.);
  - средства защиты информации (межсетевые экраны, антивирусные средства и т.д.).

Приложение Б. Сравнительный анализ обработки данных в ИСПДн с различной архитектурой

Таблица Б.1 – Сравнительный анализ обработки данных в ИСПДн разных архитектур

Критерий	**Централизованная архитектура**	**Распределенная архитектура**	**Мультиоблачная архитектура**
Задержки	Для локальных клиентов - 1-10 мс. Для удалённых пользователей - до 100 мс.	В пределах одного региона 2-5 мс, между регионами до 100 мс.	Межоблачные задержки от 50 до 200 мс в зависимости от расстояния и параметров сети.
Согласованность данных	Высокая (используется ACID). Все клиенты получают актуальные данные.	Может быть как модель ACID, так и модель BASE.	Обычно модель BASE для минимизации задержек между облаками.
Доступность	Уязвима к отказам. При сбое в ЦОД сервисы недоступны.	Высокая. Один узел может выйти из строя, не влияя на работу всей системы.	Очень высокая. Использование нескольких облаков минимизирует влияние отказов одного из них.
Безопасность	Легче контролировать за счет централизованного управления доступом.	Более сложная из-за распределённости данных по узлам.	Сложная из-за необходимости управления безопасностью в нескольких облаках.
Затраты на инфраструктуру	Высокие начальные вложения в программно-аппаратное обеспечение и поддержку.	Гибкие, с возможностью масштабирования по горизонтали (добавление узлов).	Затраты могут быть выше из-за использования нескольких поставщиков облачных услуг, но возможна оптимизация за счет выбора лучших предложений.
Пропускная способность	Высокая для локальных задач, ограничена мощностью одного ЦОД.	Масштабируется за счёт увеличения числа узлов.	Масштабируется за счёт использования ресурсов разных облаков.
Статистика по времени обработки	Для локальных пользователей — 1-10 мс. Для удаленных может достигать 100 мс.	В одном регионе — 2-5 мс. Межрегиональные запросы — до 100 мс.	Задержка между облаками 100-200 мс, но высокая доступность (до 99.999%).
Применение	Для критически важных приложений с высокой согласованностью и локальной доступностью.	Для глобально распределенных систем, где важна отказоустойчивость и гибкость.	Для обеспечения высокой доступности и минимизации зависимости от одного поставщика облачных услуг.

Приложение В. Классификация угроз персональным данным по уровням модели ИСПДн

В [5,170] показано, что для того, чтобы создать модель защиты персональных данных, необходимо выявить и классифицировать потенциальные угрозы персональным данным в ИСПДн. Там же [5,170] автором предлагается такая классификация угроз.

В частности, показано, что существует два класса угроз персональным данным в информационных системах:

- угрозы, которые нельзя соотнести с атаками;
- угрозы, которые могут быть соотнесены с атаками.

Несовместимые с атаками угрозы включают:

- угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (землетрясения, наводнения, ураганы и др.);
- угрозы социально-политического характера: забастовки, саботаж, локальные конфликты, сопровождающиеся нападением на объект, на котором размещены ресурсы ИСПДн и др.;
- ошибочные действия и (или) нарушение персоналом и пользователями ИСПДн требований к соответствующей эксплуатационной, организационной, технической или иной документации;
- угрозы антропогенного характера, например: аварии, различные неисправности, помехи, приводящие к нарушениям и сбоям в аппаратных компонентах ИСПДн.

Защита от таких угроз регулируется инструкциями, разработанными и утвержденными уполномоченными службами оператора персональных данных с учётом конкретных условий функционирования ИСПДн, а также действующей нормативной базы.

Защита от угроз, которые могут быть связаны с атаками, должна обеспечиваться с помощью защитных мер и средств, используемых ИСПДн и предназначенных в основном для противодействия атакам.

Состав и содержание угроз безопасности персональных данных определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным. Данная совокупность формируется с учётом характеристик ИСПДн, свойств среды распространения информационных сигналов, содержащих защищённую информацию, а также возможностей источников угроз.

Следующие характеристики информационной системы могут вызвать угрозы нарушения качества персональных данных:

- структура, категория и объём персональных данных, обрабатываемых в информационной системе;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сети интернет;
- характеристики подсистемы безопасности и режимы обработки персональных данных;
- режимы разграничения прав доступа пользователей информационной системы;
- расположение и условия размещения технических средств информационной системы.

Угроза нарушения качества персональных данных реализуется в результате формирования каналов реализации данной угрозы между источником угрозы и носителем

персональных данных, создает необходимые условия для нарушения безопасности персональных данных.

Основными элементами канала реализации угрозы нарушения качества персональных данных являются:

- источник угрозы – субъект, материальный объект или физическое явление, создающее угрозу безопасности персональных данных, например, нарушитель безопасности персональных данных, возможности которого в отношении системы определены в модели нарушителя;
- окружающая среда для распространения персональных данных или воздействий, в котором физическое поле, сигнал, данные или программы могут быть распределены и влияют на характеристики защищённых персональных данных. Эти характеристики включают: конфиденциальность, целостность, доступность;
- носитель персональных данных – физический или материальный объект, в том числе физическое поле, в котором персональные данные отражаются в виде символов, изображений, сигналов.

Также возможны другие характеристики качества персональных данных, которые важны для оператора, например, подлинность данных.

Носители персональных данных могут содержать информацию, представленную в следующих формах: акустическая (речевая) информация; текстовая и визуальная информация; обрабатываемая (циркулирующая в информационной системе) информация.

Для наиболее полной идентификации угроз персональным данным и связанных с ними информационных рисков следует рассмотреть угрозы и риски как для каждого уровня модели ИСПДн, так и для каждого сегмента технической подсистемы ИСПДн.

Для аналитического уровня характерны следующие основные угрозы:

- неверное категорирование (или нарушение категорирования) персональных данных;
- нарушение распределения прав доступа для каждого пользователя системы, имеющих согласно должностной инструкции право работы с персональными данными;
- неверное определение совокупности информации (в том числе персональных данных) для конкретных пользователей;
- отсутствие нормативной базы, регламентирующей процесс обработки персональных данных;
- недостаточная квалификация работника для работы с персональными данными, обрабатываемых в информационной системе.

Технологический уровень характеризуется следующими угрозами:

- нарушение адресности информации, содержащей персональные данные, дающее возможность доступа к такого рода информации не только легитимного пользователя, участвующего в технологическом процессе обработки персональных данных, но и нелигитимного;
- неверная степень консолидации персональных данных, дающая возможность недопустимого объединения данных и вывода недоступной пользователю информации;
- увеличение вычислительной сложности различных технологических процедур, что в результате влияет на уровень доступности результатов процесса;
- нарушения регламента технологических процессов.

На техническом уровне можно выделить следующие основные угрозы:

- воздействие на процесс хранения и обработки персональных данных, не предусмотренное регламентом;
- сбои и аварии систем жизнеобеспечения, элементов сети и линий связи;
- использование в аппаратных и программных компонентах элементов, реализующих функции, не предусмотренные документацией на эти компоненты;
- распространение программ-вирусов, нарушающих нормальное функционирование общесистемной среды.
- утечка акустической (речевой) информации – при наличии функций голосового ввода или функций воспроизведения персональных данных акустическими средствами информационной системы;
- утечка конкретных персональных данных—– при просмотре информации оптическими (оптоэлектронными) средствами с экранов дисплеев;
- утечка персональных данных из-за наличия электромагнитного излучения, в основном мониторы и системные блоки персональных компьютеров и серверов из информационной системы.

Техническая подсистема, как было описано в разделе 4.1 настоящей работы, состоит из семи сегментов. Для правильной идентификации рисков необходимо определить основные угрозы для каждого такого сегмента.

Сегмент внешней среды подвержен следующим угрозам:

- различные факторы окружающей среды, к примеру пожар, наводнение, ураган и т.п., оказывающие воздействие на центр обработки данных, в котором осуществляются облачные вычисления по запросам на обработку персональных данных;
- нарушение условий эксплуатации серверов, что может привести к поломке или затруднению работы оборудования системы;
- неправильное использование охранных средств организации, следствием чего может явиться проникновение третьих лиц в непредназначенные для общего доступа помещения;
- отказ оператора облачных услуг от выполнения запросов на обработку персональных данных.

Сегмент линий связи может подвергаться угрозам:

- обрыв волоконно-оптической и других физических компонентов линий связи;
- воздействие различных факторов окружающей среды, к примеру пожар, наводнение, ураган и т.п.;
- нарушение качества персональных данных, в частности – целостности;
- физическое антропогенное воздействие как для уничтожения линии связи, так и для подключения нелегитимного пользователя системы – прослушивание информации, а также её изменение;
- несанкционированное подключение пользователя.

Сегмент элементов корпоративной сети может быть подвержен следующим угрозам:

- нарушение правильного функционирования оборудования системы;
- внешнее воздействие на отдельные элементы сети;
- нарушение параметров информационной безопасности, в частности – доступности.

Сегмент взаимодействий – сетевого и межсетевого – подвергается следующим угрозам:

- сбой программного обеспечения;

- физическое или программное нарушение правильного функционирования взаимодействия между подсистемами или системами;
- атаки на сегмент;
- нарушение качества персональных данных, в частности – конфиденциальности;
- перехват управления межсетевым экранированием;
- несанкционированные доступ по локальной сети.

Для *сегмента вычислительных средств* устанавливаются такие угрозы, как:

- задержка в использовании любого типа вычислительных устройств;
- неконтролируемое использование средств вычисления;
- перегрузка устройств;
- загрузка в вычислительные устройства неправомерного программного обеспечения (вирусного программного обеспечения);
- использование вычислительных средств не по их прямому функциональному назначению;
- несанкционированный доступ к вычислительным ресурсам системы, которые представляют особую важность.

Сегмент программных средств может быть подвержен следующим угрозам:

- сброс установок программного обеспечения;
- сбой в работе программного обеспечения;
- уязвимости одного дня в программном обеспечении или утилитах системы;
- неправильная настройка политики доступа к программным и вычислительным средствам;
- несанкционированные и неправомерные действия со стороны системного администратора.

Для *сегмента информационных средств* могут быть установлены угрозы:

- нарушение качества персональных данных (целостности, конфиденциальности и доступности);
- несанкционированный доступ неавторизованных пользователей к информационным средствам системы;
- нарушение прав доступа к информационным средствам;
- искажение информации;
- удаление информации;
- недостаточная изоляция баз данных системы, а также средств управления ими.

Процесс ранжирования угроз и рисков по подсистемам и сегментам корпоративной ИСПДн позволяет наиболее точно идентифицировать все возможные воздействия на систему. При правильной идентификации воздействий процесс оценки и управления рисками проводится с гарантированной точностью и надёжностью.

В рамках рассмотренной модели все три уровня неразрывно связаны между собой совокупностью угроз. Угрозы нижних уровней модели редуцируются на верхние уровни и проявляются в виде консолидированных угроз. При этом может быть получен одинаковый результат от реализации угроз, специфицированных на различных уровнях модели.

Этот перечень угроз лежит в основе модели угроз конкретной информационной системы персональных данных и необходим для определения потенциальных информационных рисков в процессе автоматизированной обработки персональных данных в информационной системе.

Приложение Г. Вариант расчёта данных для оценки рисков по разработанной модели

В приложении приводится пример получения данных для проведения оценки рисков нарушения качества персональных данных в ИСПДн транспортной компании. Источник исходных данных – экспертный опрос.

Таблица Г.1 – Активы ИСПДн

№	Наименование элемента воздействия (актива)
O1	Сервер хранение справочной информации
O2	Распределенное хранилище информации
O3	Сервер приложений
O4	Сервер мониторинга
O5	Облачный кластер системы

Таблица Г.2 – Источники воздействий

№	Наименование источника угрозы
S1	Пользователи ИСПДн
S2	Администраторы и разработчики ИСПДн
S3	Внешние информационные ИСПДн
S4	Аппаратные средства ИСПДн

Таблица Г.3 – Актуальные угрозы нарушения качества персональных данных

№	U*	Наименование угрозы
T1	0,75	Недостаточная квалификация пользователей для работы с ИСПДн
T2	0,35	Увеличение времени обработки или доступа информации в результате увеличения вычислительной сложности процедур
T3	0,5	Превышение регламентированной нагрузки на ИСПДн со стороны пользователей
T4	0,5	Превышение регламентированной нагрузки на ИСПДн со стороны внешних систем
T5	0,5	Нарушение регламента работы с ИСПДн со стороны пользователей
T6	0,5	Нарушение регламента работы с ИСПДн со стороны внешних систем
T7	0,5	Нарушение регламентированной скорости передачи информации со стороны внешних систем
T8	0,35	Распространение внешними системами некачественной информации (ложной, отфильтрованной, зашумленной, избыточной, неактуальной, искаженной, усеченной или задержанной)
T9	0,35	Ввод пользователями некачественной информации (ложной, отфильтрованной, зашумленной, избыточной, неактуальной, искаженной, усеченной или задержанной)
T10	0,35	Уничтожение информации со стороны пользователей
T11	0,25	Уничтожение информации со стороны администратора ИСПДн
T12	0,5	Игнорирование или неправильная интерпретация поступающих уведомлений мониторинга администратором ИСПДн
T13	0,25	Ошибки при установке, разработке, настройке или модификации ИСПДн администратором ИСПДн

№	U*	Наименование угрозы
T14	0,25	Воздействие на процесс хранения и обработки информации, не предусмотренное регламентом со стороны администратора ИСПДн
T15	0,35	Сбои и аварии элементов сети и линий связи

*U - степень критичности угрозы

Таблица Г.4 – Уязвимости ИСПДн

№	Наименование уязвимости
V1	Ошибки в сопровождающих документах по функционированию ИСПДн или их отсутствие
V2	Ошибки в регламентах, описывающих процессы взаимодействия с внешними системами, или отсутствие подобной документации
V3	Ошибки в руководствах пользователя, либо отсутствие подобной документации
V4	Недостатки в процессах управления релизами или отсутствие подобных процессов
V5	Недостаточная квалификация сотрудников, занимающихся проектированием, разработкой и/или сопровождением ИСПДн
V6	Недостаточная квалификация пользователей
V7	Неправильная настройка отдельных параметров программного обеспечения, или ошибочная конфигурация ИСПДн
V8	Неправильно настроенная система мониторинга, или ее отсутствие
V9	Недостаточное резервирование оборудования и каналов связи или его отсутствие
V10	Недостатки процессов резервного копирования информации, или их отсутствие
V11	Отсутствие или недостаточность процесса приемо-сдаточных испытаний
V12	Техническое и/или программное несоответствие тестовой среды ИСПДн относительно промышленной
V13	Недостатки политики доступа к инфраструктуре ИСПДн
V14	Возможность ошибочного получения доступа к ресурсам с ограниченным доступом
V15	Возможность несанкционированного внедрения стороннего программного кода
V16	Ошибки при реализации политики доступа к ресурсам ИСПДн
V17	Недостатки при проверке входных и/или поступающих данных
V18	Ошибки при реализации программного кода ИСПДн
V19	Ошибки в общесистемном или прикладном программном обеспечении
V20	Неисправности аппаратного или программного характера в техническом или сетевом оборудовании

Таблица Г.5 – Исследуемые риски

№	Событие риска	Величина ущерба (усл. ед.)
R1	С ИСПДн работает пользователь, несоответствующий минимальному уровню подготовки и/или не обладающий достаточной квалификацией в рамках своих компетенций	5
R2	Были добавлены/удалены/изменены программные процедуры, что привело к снижению эффективности работы ИСПДн либо полностью остановило ее работу	10
R3	Действия пользователей при работе с ИСПДн привели к такому увеличению нагрузки на нее, которое снизило эффективность ее работы, либо полностью остановило ее функционирование	5

R4	Увеличение потока информации от внешних систем привело к такому увеличению нагрузки на ИСПДн, которое снизило эффективность ее работы, либо полностью остановило ее функционирование	5
R5	В результате ошибочных действий пользователей снизилась эффективность работы ИСПДн либо произошел сбой в ее функционировании	10
R6	В результате нарушения регламента взаимодействий со стороны внешних систем снизилась эффективность работы ИСПДн либо произошел сбой в ее функционировании	10
R7	Внешние системы нарушают регламентированную скорость передачи информации	5
R8	От внешних систем поступает некачественная информация	10
R9	Пользователь вводит в ИСПДн некачественную информацию	10
R10	Действия пользователя ИСПДн привели к ошибочному уничтожению информации или ее части	15
R11	Действия администратора ИСПДн привели к ошибочному уничтожению информации или ее части	15
R12	Эффективное функционирование ИСПДн было нарушено в результате игнорирования или не правильной интерпретации уведомлений мониторинга со стороны администратора ИСПДн	10
R13	Эффективное функционирование ИСПДн было нарушено в результате ошибочных действий администратора или разработчика при ее разработке, настройке или модификации	15
R14	Эффективное функционирование ИСПДн было нарушено в результате ошибочных действий во время воздействия на процессы ИСПДн	15
R15	Эффективное функционирование было полностью или частично нарушено в результате сбоев элементов инфраструктуры ИСПДн или аварий на линях связи	15

Таблица Г.6 – Функции противодействия угрозам

№	Наименование функции противодействия	Стоимость реализации (усл. ед.)
Z1	Создание спецификаций, описывающих задачи, функции, режимы функционирования ИСПДн, также обрабатываемый в ней набор данных и виды предоставляемых сервисов	10
Z2	Создание сопроводительных документов для пользователей и администраторов ИСПДн	15
Z3	Разработка спецификаций по взаимодействию с внешними информационными системами	15
Z4	Организация процесса по управлению релизами	5
Z5	Организация процессов по управлению приемо-сдаточными испытаниями	10
Z6	Обеспечение технического и программного соответствия между тестовой и промышленной средами	15
Z7	Разработка критериев качества обработки информации	5
Z8	Разработка системы учета внешних источников, подключаемых к ИСПДн	5
Z9	Разработка системы адресации	5

Z10	Разработка регламентов архивирования и резервного копирования информации	10
Z11	Создание системы обучения и сертификации пользователей	15
Z12	Создание системы обучения и повышения квалификации сотрудников, сопровождающих инфокоммуникационную систему	15
Z13	Разработка классификации пользователей и регламентирование контроля доступа	10
Z14	Обеспечение резервирования критических элементов, а также создание регламента по использованию резервных ресурсов	20
Z15	Организация контроля доступа к сервисам и ресурсам ИСПДн	10
Z16	Обеспечение процессов мониторинга	15
Z17	Обеспечение защиты от внедрения стороннего программного кода	15
Z18	Обеспечение ограниченного доступа к инфраструктуре ИСПДн	5

Таблица Г.7 – Результат оценки рисков ПДн в ИСПДн (актуальности угроз)

№	Наименование угрозы	Степень реализуемости	Уровень ущерба	Значимость угрозы	Актуальность
Аналитический уровень					
1	Администратор ИСПДн неверно категорировал информацию в части ограничения доступа к ней	0,25	< 0,05	0	Нет
2	Администратор ИСПДн неверно определил список легитимных пользователей для конкретной совокупности данных	0,25	< 0,05	0	Нет
3	Администратор ИСПДн неверно определил совокупность информации для конкретных пользователей	0,25	< 0,05	0	Нет
4	Недостаточная квалификация пользователей для работы с ИСПДн	0,75	0,21	1,0	Да
5	Отсутствие регламента по описанию процессов обработки информации	0,25	0,03	0	Нет
6	Ошибки в регламенте по описанию процессов обработки информации	0,25	0,03	0	Нет
7	Отсутствие регламента работы с ИСПДн пользователей	0,25	0,03	0	Нет
8	Ошибки в описании регламента работы с ИСПДн пользователей	0,25	0,03	0	Нет
9	Отсутствие регламента по подключению внешних систем и взаимодействию с ними	0,25	0,03	0	Нет
10	Ошибки в описании регламента по подключению внешних систем и взаимодействию с ними	0,25	0,03	0	Нет
Технологический уровень					
11	Нарушение адресности информации	0,25	0,05	0	Нет
12	Неверная степень консолидации информации	0,35	0,05	0,2	Нет
13	Увеличение времени обработки или доступа информации в результате увеличения вычислительной сложности процедур	0,35	0,12	0,2	Да
14	Превышение регламентированной нагрузки на ИСПДн со стороны пользователей	0,5	0,09	0,5	Да

№	Наименование угрозы	Степень реализуемости	Уровень ущерба	Значимость угрозы	Актуальность
15	Превышение регламентированной нагрузки на ИСПДн со стороны внешних систем	0,5	0,12	0,5	Да
16	Нарушение регламента работы с ИСПДн со стороны пользователей	0,5	0,09	0,5	Да
17	Нарушение регламента работы с ИСПДн со стороны внешних систем	0,5	0,09	0,5	Да
18	Нарушение регламента работ по взаимодействию с внешними системами со стороны администратора ИСПДн	0,25	< 0,05	0	Нет
19	Нарушение регламентированной скорости передачи информации со стороны внешних систем	0,5	0,09	0,5	Да
20	Распространение внешними системами некачественной информации (ложной, отфильтрованной, зашумленной, избыточной, неактуальной, искаженной, усеченной или задержанной)	0,35	0,07	0,2	Да
21	Ввод пользователями некачественной информации (ложной, отфильтрованной, зашумленной, избыточной, неактуальной, искаженной, усеченной или задержанной)	0,35	0,07	0,2	Да
22	Формирование и передача ИСПДн некачественной информации к потребителю (ложной, несуществующей, отфильтрованной, зашумленной, избыточной, неактуальной, искаженной, усеченной или задержанной)	0,25	0,05	0	Нет
23	Уничтожение информации со стороны пользователей	0,35	0,12	0,2	Да
24	Уничтожение информации со стороны администратора ИСПДн	0,25	0,12	0	Да
25	Вмешательство потребителя в процессы хранения и обработки информации и формирование им некачественной информации (искаженной, порожденной, зашумленной, избыточной, отфильтрованной, неактуальной)	0,25	0,05	0	Нет
26	Несанкционированное прочтение информации со стороны пользователей	0,35	< 0,05	0,2	Нет
27	Несанкционированное прочтение информации со стороны внешних систем	0,35	< 0,05	0,2	Нет
28	Несанкционированная консолидация информации (получение доступа к большому объему консолидированной информации, которая не должна быть доступна)	0,25	< 0,05	0	Нет
29	Несанкционированный вынос информации со стороны пользователей	0,35	< 0,05	0,2	Нет
30	Несанкционированный вынос информации со стороны внешних систем	0,35	< 0,05	0,2	Нет
31	Отказ в предоставлении данных со стороны пользователей	0,25	< 0,05	0	Нет

№	Наименование угрозы	Степень реализуемости	Уровень ущерба	Значимость угрозы	Актуальность
32	Отказ в предоставлении данных со стороны внешних систем	0,25	< 0,05	0	Нет
33	Блокирование входящего потока информации администратором ИСПДн	0,25	< 0,05	0	Нет
34	Игнорирование или неправильная интерпретация поступающих уведомлений мониторинга администратором ИСПДн	0,5	0,10	0,5	Да
35	Ошибочная конфигурация системы и взаимодействий с внешними системами;	0,25	< 0,05	0	Нет
36	Ошибочное блокирование сервисов или информационных ресурсов ИСПДн администратором ИСПДн	0,25	< 0,05	0	Нет
37	Ошибки при установке, разработке, настройке или модификации ИСПДн администратором ИСПДн	0,25	0,10	0	Да
Технический уровень					
38	Воздействие на процесс хранения и обработки информации, не предусмотренное регламентом со стороны администратора ИСПДн	0,25	0,07	0,5	Да
39	Сбои и аварии элементов сети и линий связи	0,35	0,07	0,2	Да
40	Использование в аппаратных и программных элементах ИПДн не предусмотренных в документации функций	0,25	< 0,05	0	Нет
41	Распространение вирусных программ, нарушающих работу ИСПДн	0,25	< 0,05	0	Нет
42	Физическое нарушение функционирования программных или технических средств со стороны пользователей ИСПДн или внешних систем	0,25	< 0,05	0	Нет

Приложение Д. Значения параметров, используемых в эксперименте

Значения параметров, используемых в эксперименте для Сценария А:

Вариант С1

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=1$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(1,0)$	$\mathbf{c}_2^T=(1,0)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=(0,5)$	$\mathbf{B}_2=(0,5)$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,5)$	$\mathbf{d}_2^T=(0,5)$

Вариант С2

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=2$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,5;0,5)$	$\mathbf{c}_2^T=(0,5;0,5)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,33 & 0,33\\ 0,5 & 0,5\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,5 & 0,5\\ 0,33 & 0,33\end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,3;0)$	$\mathbf{d}_2^T=(0;0,34)$

Вариант С3

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=3$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,33;0,33;0,33)$	$\mathbf{c}_2^T=(0,33;0,33;0,33)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,25 & 0,25 & 0,25\\ 0,33 & 0,33 & 0,33\\ 0,33 & 0,33 & 0,33\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,33 & 0,33 & 0,33\\ 0,33 & 0,33 & 0,33\\ 0,25 & 0,25 & 0,25\end{pmatrix}$

вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T = (0,25;0;0)$	$\mathbf{d}_2^T = (0,0,0.25)$

Вариант С4

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=4$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T = (0,25;0,25;0,25;0,25)$	$\mathbf{c}_2^T = (0,25;0,25;0,25;0,25)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1 = \begin{pmatrix} 0,2 & 0,2 & 0,2 & 0,2 \\ 0,25 & 0,25 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0,25 & 0,25 \end{pmatrix}$	$\mathbf{B}_2 = \begin{pmatrix} 0,25 & 0,25 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0,25 & 0,25 \\ 0,25 & 0,25 & 0,25 & 0,25 \\ 0,2 & 0,2 & 0,2 & 0,2 \end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T = (0,2;0;0;0)$	$\mathbf{d}_2^T = (0;0;0;0,2)$

Вариант С5

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=5$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T = (0,2;0,2;0,2;0,2;0.2)$	$\mathbf{c}_2^T = (0,2;0,2;0,2;0,2;0.2)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1 = \begin{pmatrix} 0,16 & 0,16 & 0,16 & 0,16 & 0,16 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \end{pmatrix}$	$\mathbf{B}_2 = \begin{pmatrix} 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,2 & 0,2 & 0,2 & 0,2 & 0,2 \\ 0,16 & 0,16 & 0,16 & 0,16 & 0,16 \end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T = (0,2;0;0;0;0)$	$\mathbf{d}_2^T = (0;0;0,;0;0,2)$

Значения параметров, используемых в эксперименте для Сценария Б:

Вариант С1

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=1$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(1,0)$	$\mathbf{c}_2^T=(1,0)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=(0,5)$	$\mathbf{B}_2=(0,5)$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,5)$	$\mathbf{d}_2^T=(0,5)$

Вариант С2

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=2$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,8;0,2)$	$\mathbf{c}_2^T=(0,2;0,8)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,1 & 0,1\\ 0,9 & 0,1\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,1 & 0,9\\ 0,1 & 0,1\end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,8;0)$	$\mathbf{d}_2^T=(0;0,8)$

Вариант С3

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=3$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,7;0,2;0,1)$	$\mathbf{c}_2^T=(0,1;0.2;0,7)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,1 & 0,1 & 0\\ 0,9 & 0,1 & 0\\ 0,7 & 0,2 & 0,1\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,1 & 0,2 & 0,7\\ 0 & 0,1 & 0,9\\ 0 & 0,1 & 0,1\end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,8;0;0)$	$\mathbf{d}_2^T=(0;0;0,8)$

Вариант С4

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=4$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,6;0,2;0,1;0,1)$	$\mathbf{c}_2^T=(0,1;0,1;0,2;0,6)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,1 & 0,1 & 0 & 0\\ 0,9 & 0,1 & 0 & 0\\ 0,7 & 0,2 & 0,1 & 0\\ 0,6 & 0,2 & 0,1 & 0,1\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,1 & 0,1 & 0,2 & 0,6\\ 0 & 0,1 & 0,2 & 0,7\\ 0 & 0 & 0,1 & 0,9\\ 0 & 0 & 0,1 & 0,1\end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,8;0;0;0)$	$\mathbf{d}_2^T=(0;0;0;0,8)$

Вариант С5

Параметр	**Значение**	
	Заявка $i=1$	**Заявка** $i=2$
количество типов заявки, N	$N=2$	
ёмкость буферного накопителя, r	$r=6$	
количество этапов обработки, K	$K=5$	
вероятность поступления i-заявки, g_i	$g_1=0,5$	$g_2=0,5$
вектор вероятностей постановки на этапы, $\mathbf{c}_i^T$	$\mathbf{c}_1^T=(0,5;0,2;0,15;0,1;0,05)$	$\mathbf{c}_2^T=(0,05;0,1;0,15;0,2;0,5)$
матрица переходов между этапами, $\mathbf{B}_i$	$\mathbf{B}_1=\begin{pmatrix}0,1 & 0,1 & 0 & 0 & 0\\ 0,9 & 0,1 & 0 & 0 & 0\\ 0,7 & 0,2 & 0,1 & 0 & 0\\ 0,6 & 0,2 & 0,1 & 0,1 & 0\\ 0,5 & 0,2 & 0,15 & 0,1 & 0,05\end{pmatrix}$	$\mathbf{B}_2=\begin{pmatrix}0,05 & 0,1 & 0,15 & 0,2 & 0,5\\ 0 & 0,1 & 0,1 & 0,2 & 0,6\\ 0 & 0 & 0,1 & 0,2 & 0,7\\ 0 & 0 & 0 & 0,1 & 0,9\\ 0 & 0 & 0 & 0,1 & 0,1\end{pmatrix}$
вектор вероятностей ухода из системы, $\mathbf{d}_i^T$	$\mathbf{d}_1^T=(0,8;0;0;0;0)$	$\mathbf{d}_2^T=(0;0;0;0;0,8)$

Приложение Е. Свидетельства о государственной регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023615007

Программное приложение «Анализатор актуальности угрозы» ("Threat Relevance Analyzer" - на английском языке) для определения актуальности угроз персональных данных при их обработке в информационных системах персональных данных

Правообладатель: ***Общество с ограниченной ответственностью Фирма «ТЕЛЕСОФТ» (ООО Фирма «ТЕЛЕСОФТ») (RU)***

Авторы: ***Докучаев Владимир Анатольевич (RU), Маклачкова Виктория Валентиновна (RU), Гадасин Денис Вадимович (RU), Шведов Андрей Вячеславович (RU), Кузин Роман Денисович (RU), Редин Павел Олегович (RU)***

Заявка № **2023613955**

Дата поступления **27 февраля 2023 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***09 марта 2023 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2025660244

Программное приложение для оценки эффективности использования ресурсов информационной системы при обработке персональных данных «ИРИС ПД» («ISRU PD» - на английском языке) для расчета аналитических моделей функционирования информационных систем при обработке персональных данных

Правообладатель: ***Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (RU)***

Авторы: ***Маклачкова Виктория Валентиновна (RU), Докучаев Владимир Анатольевич (RU), Гадасин Денис Вадимович (RU), Надёжный Фёдор Дмитриевич (RU), Шишкин Кирилл Сергеевич (RU)***

Заявка № **2025619102**
Дата поступления **18 апреля 2025 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***22 апреля 2025 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0692e7c1a6300bf54f240f670bca2026
Владелец **Зубов Юрий Сергеевич**
Действителен с 10.07.2024 по 03.10.2025

Ю.С. Зубов

Приложение Ж. Акты о внедрении

Ректор ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики» (МТУСИ)

_____

к.т.н., доцент Ерохин С.Д.

« » _____ 2025 г.

АКТ

об использовании результатов диссертационной работы Маклачковой В.В. на тему: «Модели и алгоритмы оценки информационных процессов и ресурсов корпоративных автоматизированных информационных систем персональных данных»
в учебном процессе кафедры «Сетевые информационные технологии и сервисы» МТУСИ

Комиссия в составе: проректора по учебной работе МТУСИ, к.э.н., доцента Аджиковой Алтынай Султахановны, начальника Отдела планирования и организации учебного процесса МТУСИ Кузнецовой Виктории Анатольевны, декана факультета «Информационные технологии» МТУСИ, к.т.н., доцента Городничего Михаила Геннадьевича удостоверяет, что в учебном процессе кафедры «Сетевые информационные технологии и сервисы» при выполнении лабораторных и практических работ по дисциплинам: «Анализ производительности информационной системы», «Архитектура центров обработки данных», «Сетевая безопасность и её планирование», «Управление и администрирование информационных систем» используются результаты диссертации Маклачковой Виктории Валентиновны, такие как: архитектура мультиоблачных информационных систем, модели и алгоритмы оценки эффективности использования информационных систем работы с персональными данными и оценки информационных рисков, позволяющие улучшить производительность информационной системы и минимизировать риски качества персональных данных. Эффективность внедрения заключается в приобретении студентами знаний по перспективным направлениям развития науки и техники.

Проректор по учебной работе, к.э.н., доцент А.С. Аджикова

Начальник Отдела планирования и организации учебного процесса В.А. Кузнецова

Декан факультета ИТ, к.т.н., доцент М.Г. Городничев

Общество с ограниченной ответственностью «ТрастВерс»

115230, Россия, Москва, 1-й Нагатинский проезд, д. 10, стр. 1
Тел.: +7 (495) 280-36-75 Email: info@trustverse.ru https://www.trustverse.ru

исх. № от 3 июля 2025 года

АКТ
о внедрении результатов диссертационной работы Маклачковой Виктории Валентиновны на тему: «Модели и алгоритмы оценки информационных процессов и ресурсов корпоративных автоматизированных информационных систем персональных данных», представленной на соискание ученой степени кандидата технических наук

Настоящим актом подтверждается, что основные результаты диссертационного исследования Маклачковой Виктории Валентиновны «Модели и алгоритмы оценки информационных процессов и ресурсов корпоративных автоматизированных информационных систем персональных данных» в настоящее время используются в режиме опытной эксплуатации в работе сервисной компании ООО «ТрастВерс», оказывающей услуги консалтинга, внедрения и технической поддержки средств защиты информации, а также в компаниях партнёрах, а именно:

- алгоритм вычисления вероятностно-временных характеристик использования ресурсов информационной системы с мультиоблачной архитектурой при обработке персональных данных позволил снизить трудоемкость вычислительного процесса не менее чем на 17%;
- математическая модель и последовательность организации информационных процессов оценки информационных рисков персональных данных при их автоматизированной обработке, которые позволяют выявить наиболее критичные информационные риски с целью дальнейшей разработки мер противодействия им. Проведённые расчёта показали, что к наиболее критичным рискам при использовании ИСПДн с мультиоблачной архитектурой являются: недостаточная квалификация пользователей для работы с ИСПДн (риск 0,75), превышение регламентированной нагрузки на ИСПДн как со стороны работников, так и со стороны внешних систем (риск 0,5), сбой и аварии элементов сети и линий связи (риск 0,35).

Результаты диссертационного исследования позволили осуществить разработку обобщённых сценариев запросов на обработку персональных данных в информационной системе, на основе рассчитанных ВВХ и позволили обосновать структуру ИСПДн с учётом её мультиоблачной архитектуры, а также выявить наиболее критичные риски, влияющие на качество персональных данных.

Генеральный директор,
член Наблюдательного совета
АНО НТЦ «Цифровая криптография» **А.Е. Шарков**

АКТ

о внедрении результатов диссертационной работы
Маклачковой Виктории Валентиновны,
представленной на соискание ученой степени кандидата технических наук

Настоящим актом подтверждается, что основные результаты диссертационного исследования Маклачковой Виктории Валентиновны «Модели и алгоритмы оценки информационных процессов и ресурсов корпоративных автоматизированных информационных систем персональных данных» используются при разработке технических заданий на создание и модернизацию ИСПДн, а именно:

- унификация процессов жизненного цикла обработки персональных данных с целью организации контроля за выполнением требований нормативных правовых актов, регламентирующих работу с персональными данными и идентификации признаков обработки персональных данных в корпоративной информационной системе;
- разработка обобщенных сценариев обработки запросов к персональным данным с целью планирования архитектуры ИСПДн и контроля использования её ресурсов, а также контроля доступа к ресурсам ИСПДн со стороны пользователей из числа сотрудников компании для обеспечения качества обработки запросов к персональным данным и минимизации информационных рисков;
- математическая модель для оценки вероятности нарушения качества персональных данных при их обработке в ИСПДн с мультиоблачной архитектурой с целью выявления актуальных угроз и рисков, соответствующих фактическим условиям функционирования ИСПДн и отражающих модель бизнес-технологических процессов, в которых используются ИСПДн;
- алгоритм для решения оптимизационной задачи минимизации рисков при ограничениях на используемые меры противодействия воздействия на ИСПДн;
- рекомендации по организации информационного процесса оценки информационных рисков персональных данных при их автоматизированной обработке.

Результаты диссертационного исследования также использованы при создании курса «Организация обработки и обеспечение безопасности персональных данных в ОАО «РЖД» в системе дистанционного обучения ОАО «РЖД», при подготовке программы повышения квалификации ответственных за организацию обработки персональных данных в подразделениях ОАО «РЖД» по теме «Организация обработки и обеспечение безопасности персональных данных», в тестировании работников ОАО «РЖД» на знание и оценку потенциальных информационных рисков при работе с персональными данными и действиях по их минимизации, подготовке методических рекомендаций, презентационных материалов и выступлений по вопросам обеспечения безопасности персональных данных в рамках корпоративных мероприятий.

Заместитель начальника Департамента
управления информационной безопасностью
ОАО «РЖД» Шемякин В.В.