

Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, государственного управления и финансов
Базовая кафедра цифровых финансовых технологий Сбербанка России

УТВЕРЖДАЮ
Заведующий кафедрой

_____ Д. В. Солнцев
подпись
« _____ » _____ 2024 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

**ИССЛЕДОВАНИЕ ФАКТОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НАСЕЛЕНИЯ**

38.04.01 «Экономика»
(код и наименование направления)

38.04.01.17 «Финансово-экономическая аналитика и принятие решений в
цифровой среде»
код и наименование магистерской программы

Научный руководитель _____	<u>доцент, к.э.н.</u>	<u>Ю.И. Черкасова</u>
Выпускник _____		<u>К.А. Болдырь</u>
Рецензент _____	<u>доцент, к.э.н.</u>	<u>В.М. Грязнов</u>
Нормоконтролер _____		<u>Э.Ф. Мамедова</u>

Красноярск 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	2
1 Теоретические основы информационной безопасности населения	5
1.1 Теоретические аспекты и роль информационной безопасности населения в условиях формирования информационного общества	5
1.2 Ретроспективный обзор исследований по оценке информационной безопасности: российский и зарубежный опыт	13
2 Анализ факторов, оказывающих влияние на информационную безопасность населения	20
2.1 Методические подходы к расчету показателя информационной безопасности	20
2.2 Обоснование выборки и описание статистики данных для расчетов.....	29
2.3 Построение модели зависимости показателя информационной безопасности населения и независимыми факторами	45
3 Направления повышения уровня информационной безопасности населения.....	61
3.1 Практическая значимость предложенной модели.....	61
3.2. Использование показателя информационной безопасности населения как индикатора в национальном проекте	68
ЗАКЛЮЧЕНИЕ	70
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	72
ПРИЛОЖЕНИЕ А.....	80

ВВЕДЕНИЕ

Актуальность исследование факторов информационной безопасности населения обусловлена периодом становления информационного общества в современной России. В настоящее время наблюдается тенденция повсеместного применения информационных технологий, что является одним из ключевых факторов развития экономики, одновременно формируя новые информационные угрозы.

Целью магистерской диссертации является научное обоснование и разработка рекомендаций по повышению информационной безопасности населения на основе анализа и оценки факторов, оказывающих на него влияние.

Задачи магистерской диссертации:

1. На основе анализа нормативно-правовой базы и теоретических источников выделить подходы к определению информационной безопасности и факторов на нее влияющих.

2. Определить методическую основу расчета показателя, характеризующего информационную безопасность населения, на основе имеющихся статистических данных произвести соответствующие расчеты.

3. Установить наличие статистически значимой зависимости между показателем информационной безопасности населения и независимыми переменными.

4. На основе полученных данных разработать практические рекомендации направленные на совершенствование политики в области информатизации и связи с целью повышения информационной безопасности населения.

Гипотеза 1. Уровень цифровой грамотности населения оказывает статистически значимое влияние на показатель информационной безопасности населения.

Гипотеза 2. Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения оказывает статистически значимое влияние на показатель информационной безопасности населения.

Гипотеза 3. Уровень среднедушевых денежных доходов населения оказывает статистически значимое влияние на показатель информационной безопасности населения.

Гипотеза 4. Затраты на внедрение и использование цифровых технологий оказывают статистически значимое влияние на показатель информационной безопасности населения.

Объект исследования – информационная безопасность населения на территории Российской Федерации.

Предмет исследования – показатель информационной безопасности населения.

Методология исследования: контент анализ, ретроспективный анализ, корреляционно-регрессионный анализ.

Научная новизна заключается в формировании подхода, который будет отражать расчетные значения уровня «цифровой зрелости» регионов с учетом побочных эффектов от цифровизации общества.

Информационной базой исследования послужили Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации, документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, справочно-правовая система «Консультант Плюс» и электронные ресурсы.

Теоретическая значимость диссертационного исследования заключается в разработке методологии расчета показателя информационной безопасности населения.

Разработка и внедрение авторских рекомендаций позволят количественно оценить уровень информационной безопасности населения в регионах РФ, а также рассчитывать «цифровую зрелость» регионов с учетом показателя информационной безопасности населения, что будет способствовать снижению его уровня.

Кроме того, полученные в настоящей работе результаты могут быть учтены органами государственной власти при направлении рекомендаций по формированию системы показателей к новому национальному проекту «Экономика данных и цифровая трансформация государства» разработка которого предусмотрена Перечнем поручений по реализации Послания Президента Федеральному Собранию (утв. Президентом РФ 30.03.2024 № Пр-616).

Основные положения, научные выводы и результаты, сформулированные в процессе исследования, прошли апробацию в форме публикации в трудах IV Международной научной конференции «Цифровая экономика глазами студентов» организованной Казанским национальным исследовательским техническим университетом им. А. Н. Туполева.

Магистерская диссертация состоит из введения, трех глав, заключения, списка использованных источников заключения и приложений.

1 Теоретические основы информационной безопасности населения

1.1 Теоретические аспекты и роль информационной безопасности населения в условиях формирования информационного общества

В связи с развитием информационно-коммуникационных технологий и повышения вероятности возникновения угроз в условиях информационного развития общества приобретает актуальность проблема информационной безопасности населения.

В различных источниках, контекстах термин «информационная безопасность» имеет различные определения.

Так, пунктом 2.19. ГОСТа Р ИСО/МЭК 27000-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» термин «информационная безопасность» определен как сохранение конфиденциальности, целостности и доступности информации [1]. Закон РФ «Об участии в международном информационном обмене» от 04.07.1996 № 85-ФЗ определяет информационную безопасность как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [2]. Близкое по содержанию определение дается в Доктрине информационной безопасности Российской Федерации, где указано, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства [3]. В проекте «Концепции информационной безопасности сетей связи общего пользования Российской Федерации» предусмотрено более детальное определение:

1. Информационная безопасность – это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2. Информационная безопасность – свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов Российской Федерации. Это, в первую очередь, обусловлено насущной потребностью, создания развитой и защищенной информационной среды общества [4].

Национальная программа «Цифровая экономика Российской Федерации» утвержденная президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7 предусматривает три основные цели, направленные на формирование Цифровой экономики в Российской Федерации:

1. Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом.

2. Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств.

3. Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями [5].

Стоит отметить, что развитие цифровой экономики на территории РФ будет способствовать развитию информационного общества.

Формирование информационного общества в целом невозможно без формирования культуры обеспечения безопасности в информационном

пространстве как у пользователей, так и у владельцев информационных систем и ресурсов [6].

В целях предотвращения прогнозируемых негативных тенденций Правительство РФ в декабре 2022 года утвердило концепцию формирования и развития культуры информационной безопасности граждан Российской Федерации [7]. Предполагается, что реализация Концепции будет способствовать непосредственному повышению уровня грамотности широких слоев населения Российской Федерации по вопросам информационной безопасности, сокращению финансового, морально-психологического и репутационного ущерба представителей широких слоев населения Российской Федерации от преступлений с использованием информационно-коммуникационных технологий, сохранности их данных, в том числе персональных, повышению уровня доверия к цифровым сервисам, а также дальнейшей цифровизации экономики Российской Федерации.

Национальными целями развития Российской Федерации на период до 2030 года и на перспективу до 2036 года является:

- технологическое лидерство;
- цифровая трансформация государственного и муниципального управления, экономики и социальной сферы [8].

Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы предусматривает проведение непрерывного мониторинга и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них. Перечень показателей стратегии выражен в:

- оценке развития информационных и коммуникационных технологий в Российской Федерации;
- оценке развития информационного общества в Российской Федерации;

- параметры формирования цифровой экономики, оценку ее влияния на темпы роста валового внутреннего продукта Российской Федерации;

- состоянию перехода к использованию организациями наукоемких технологий.

При этом под информационным обществом понимается общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.

Факторами, которые оказывают влияние на информационную безопасность обозначены:

- компьютерные атаки на информационные ресурсы и системы критической информационной инфраструктуры;

- угрозы, возникающие в связи с внедрением новых информационных технологий;

- нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации;

- баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну;

- обработка данных на российских серверах;

- незаконная обработка и сбор сведений о гражданах, в том числе персональных данных граждан, на территории Российской Федерации неуполномоченными и неустановленными лицами, а также используемым ими техническим средства [9].

Постановлением Правительства РФ от 15.04.2014 № 313 утверждена государственная программа Российской Федерации «Информационное общество» (далее – Программа). Приоритетами Программы обозначены такие направления как: защита личности, общества и государства от внутренних

и внешних информационных угроз; обеспечение государственной защиты интересов российских граждан в информационной сфере.

Одной из первоочередных целей Программы установлено достижение к 2030 году уровня «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления до 100 процентов. Ключевая задача на пути к достижению цели: реализация проектов, направленных на становление информационного общества, в том числе на территориях субъектов Российской Федерации [10]. Также показатель «цифровая зрелость» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления является результатом проведения цифровой трансформации государственного и муниципального управления, экономики и социальной сферы, вектор развития которой определен национальной целью развития РФ.

Система официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере отражена в Доктрине информационной безопасности Российской Федерации.

Так, задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются: обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере, оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления, планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности.

К факторам, влияющим на состояние информационной безопасности, в Доктрине относят:

- наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
- средства оказания информационно-психологического воздействия;
- компьютерную преступность;
- увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;
- компьютерные атаки;
- недостаточность кадрового обеспечения в области информационной безопасности;
- низкую осведомленность граждан в вопросах обеспечения личной информационной безопасности [3].

Проведя анализ подходов к определению информационной безопасности было выявлено, что само понимание понятия является значимой задачей научного анализа.

Рассматривая структуру информационной безопасности имеет смысл рассмотреть уже действующие подходы. Так, российский ученый Баринов С. В. рассматривает такие аспекты информационной безопасности личности как информационно-техническая безопасность, информационно-идеологическая безопасность, информационно-психологическая безопасность личности, а также информационно-правовая безопасность личности [11].

Грачев Г. В. также обращает внимание на многофакторность категории, определяя информационно-психологическую безопасность как «состояние защищенности психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование

и функционирование адекватной информационно-ориентировочной основы социального поведения человека (и в целом жизнедеятельности в обществе), а также адекватной системы его субъективных (личностных, субъективно-личностных) отношений к окружающему миру и самому себе» [12].

Малюк А. А. всесторонне исследовавший информационную безопасность, выделяет три подхода:

- эмпирический – непрерывное слежение за появлением новых угроз информации, разработка средств защиты от новых угроз, выбор средств защиты на основе опыта;

- концептуально-эмпирический – формирование на основе опыта общей концепции защиты, разработка и научное обоснование методов оценки уязвимости информации и синтеза оптимальных механизмов защиты, появление унифицированных и стандартных решений по защите;

- теоретико-концептуальный – разработка основ теории защиты информации, обоснование постановки задачи многоаспектной комплексной защиты, введение понятия стратегии защиты, унификация концепции защиты, разработка методологий анализа и синтеза систем защиты и управления ими в процессе функционирования, широкое развитие унифицированных и стандартных решений [13].

Мазуров В. А., Невинский В. В. предлагают подход к определению информационной безопасности на основе анализа нормативно правовых актов, которые формируют понятийный аппарат, так была предложена формулировка, определяющая информационную безопасность как состояние защищенности жизненно-важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающих ее формирование, использование и развитие [14].

Еркин А. В. выделил два подхода к определению информационной безопасности. Для индустриального общества информационная безопасность – это состояние рассматриваемой системы управления, при котором

обеспечивается сохранность секретной информации под воздействием внешних и внутренних угроз; ее восприятие во внешнем окружении является объективным с точки зрения цели и результатов ее функционирования (указанный аспект обычно не учитывается). Для информационного общества информационная безопасность – это состояние рассматриваемой системы управления, при котором ее информационная инфраструктура не дестабилизируются под воздействием внешних и внутренних угроз; восприятие результата ее деятельности во внешнем окружении является объективным [15].

Шавва А. И., Хаблов Д. Е. охарактеризовали в широком понимании информационную безопасность как определенный процесс управления угрозами и опасностями [16].

Золотар О. А. в подходах к определению информационной безопасности выделяет доктринальные, энциклопедические и нормативно-правовые определения [17].

Несколько более узко трактует информационную безопасность Тер-Акопов А. А. [18], который под информационной безопасностью понимает «состояние защищенности информации, обеспечивающей жизненно важные интересы человека».

Орлова А. А. в научной работе «Систематизация подходов к пониманию информационной безопасности» выделяет два научно-исследовательских направления изучения информационной безопасности:

1. Технологическое, которое содержит организационно-технические мероприятия, программно-аппаратные средства, которые осуществляют надежную защиту информации.

2. Научно-исследовательское направление (политико-правовое), которое отражает характеристики политико-правового смысла, взаимосвязи с обществом и государством, установления правовых пределов ее регулирования [19].

Королев Ю. А. выделив два аспекта изучения информационной безопасности: информационно-технический и социальное политическое можно классифицировав определение на три группы:

1. Информационная безопасность как непосредственное состояние защищённости интересов, личности, общества и государства в информационной сфере.

2. Информационная безопасность как состояние социально-политической среды, при котором обеспечивается защита личности, общества, государства.

3. Информационная безопасность как право, гарантия получения достоверной информации. дал определение информационной безопасности общества [20].

Мороз Н. О. при выявлении подходов к определению термина «информационная безопасность» в контексте международного сотрудничества обозначила два региональных подхода к определению наиболее значимых терминов в рассматриваемой сфере: «западный» (термин «кибербезопасность» является преобладающим), и «восточный» (термин «информационная безопасность» рассматривается как более приемлемый) [21].

Исследовав нормативно-правовую базу, а также теоретические источники подходов к определению информационной безопасности проведем ретроспективный обзор исследований, по оценке информационной безопасности.

1.2 Ретроспективный обзор исследований по оценке информационной безопасности: российский и зарубежный опыт

31 августа 2017 года Секретарем Совета безопасности Российской Федерации Патрушевым Н. П. утверждены «Основные направления научных

исследований в области обеспечения информационной безопасности Российской Федерации», в которых проблема оценки информационной безопасности личности, общества и государства обозначена как общенаучная проблема обеспечения информационной безопасности Российской Федерации [22].

Впервые комплексный анализ факторов информационной и интеллектуальной безопасности регионов был проведен в 2009 году Брумштейном Ю. М., а также Подгорным А. Н. по результатам которого были выделены подходы для количественного измерения уровня информационной безопасности региона. По результатам исследования было отмечено, что расчет уровня информационной безопасности региона затруднен по причине слабого информационного обеспечения расчетов данными, что остается актуальным и на сегодняшний день [23].

По прошествии двух лет Брумштейн Ю. М., Подгорный А. Н. опубликовали научную статью «Информационная безопасность региона: анализ содержания термина, моделей оценки и некоторые вопросы управления». В исследовании были выделены такие виды угроз информационной безопасности как: несанкционированный доступ к информационным ресурсам, утечка информации о деятельности юридических и физических лиц, нарушение прав физических лиц на персональную информацию, вредоносные программы, спам, а также отмечено, что оценка информационной безопасности регионов возможна как качественная, так и количественная, в том числе инвариантная по отношению к размеру региона. Так, к примеру, была предложена основная модель оценки уровня информационной безопасности, представленная в формуле (1).

$$\Psi = \gamma^*(U_z / U_D), \tag{1}$$

где U_z – уровень угроз для информационной безопасности регионов, учитывающий не только интенсивность «атак», но и их диверсифицированность по направлениям и типам;

U_D – уровень защищенности информационного пространства регионов (далее ИПР);

γ – коэффициент, обеспечивающий приведение правой части формулы к безразмерной величине. «Атаки» на ИПР могут иметь место как изнутри, так и извне региона.

Также были рассмотрены другие модели с применением безразмерных весовых коэффициентов для исследуемых компонент [24].

В тот же период Зефиоров С. Л., Алексеев В. М. в научной статье «Способы оценки информационной безопасности организации» предлагают такие способы оценки информационной безопасности как: на основе экономических показателей (прямые и косвенные затраты на внедрение, эксплуатацию и сопровождение системы информационной безопасности), оценка информационной безопасности по эталону (подразумевает выбор эталона и формирование на его основе критериев оценки информационной безопасности) [25].

В 2014 году авторы Козачок В. И., Власова С. А. провели исследование на тему «Факторы определяющие информационную безопасность корпорации» результаты которого были опубликованы в среднерусском вестнике общественных наук [26]. По результатам исследования наиболее значимыми факторами были выделены: знание правил обеспечивающих информационную безопасность и благонадежность, при этом под благонадежностью понималось выполнение всех существующих внутрикорпоративных законов и предписанных правил.

Начиная с 2019 года были проведены следующие исследования:

Миковым Д. А., Булдаковой Т. И., Сюзовым В. В., Смирновой Е. В., Бауманом Ю. И. была предложена модель оценки защищённости данных

в информационно-управляющих системах реального времени, посредством индексного и рейтингового метода. Были рассчитаны индексы оценивающие информационную безопасность и выполнены группировки регионов на основе соответствия значений индексных переменных нормативным. Корреляционный анализ позволил оценить степень взаимосвязи между развитием таких факторов как информационная инфраструктура, информационная открытость организаций и учреждений, защищенность от киберугроз, а также цифровая и финансовая грамотность населения [27].

Так, Шепелевой О. Ю., Шепелевым П. Ю., Газуль С. М. была предложена модель, позволяющая оценить эффективность стратегического управления информационной безопасностью предприятия, с учетом наличия у предприятия больших возможностей количественного измерения показателей информационной безопасности. Основными параметрами модели были определены: физический контроль информационной безопасности, технический контроль информационной безопасности, цифровая грамотность сотрудников, поддержание позитивных настроений среди сотрудников в отношении политики информационной безопасности и пр. Результаты показали недостаточное развитие мер, связанных с оптимизацией использования информационных ресурсов и управления рисками на уровне стратегического управления [28].

Самохвалов Ю. Я. предложил подход к оценке информационной безопасности на основе критерия уверенности в том, что в организации реализуется принятая политика безопасности. Оценка уверенности включает оценку доверия к информационной безопасности организации, качества модели оценки доверия и бекграунда лиц, проводивших такую оценку и оценку знаний относительно угроз. В качестве показателя уверенности используется показатель полезности как значение обобщенной функции желательности Харрингтона [29].

Барыбина А. З. исследовала возможность проведения моделирования и оценки информационной безопасности как совокупного процесса. Факторами, учитываемыми в модели, были предложены: количество ПК с доступом к сети Интернет, количество используемых почтовых клиентов, наличие корпоративной почты, использование съемных носителей, использование облачных технологий, объем инвестиций направленный на приобретение ИКТ оборудования, по итогам исследования был сделан вывод о невозможности построения модели и создания обоснованного сценария развития информационной безопасности в текущее время [30].

Проведя ретроспективный анализ исследований российского опыта в научной и методической литературе достаточно широко представлены публикации, по оценке уровня информационной безопасности объектов, при этом большинство из них сосредотачивают внимание на уровне организации, либо комплексной оценки информационной безопасности в целом.

В свою очередь, по мнению автора, оценка уровня информационной безопасности населения остается в тени, в то время как национальные интересы страны направлены на развитие информационного общества. Данный процесс может привести к увеличению вероятности возникновения перманентных угроз безопасности граждан, что еще раз подтверждает актуальность исследования информационной безопасности населения.

В зарубежной литературе достаточно широко представлены исследования, направленные на изучение осведомленности об информационной безопасности личности, определяя данный фактор первоочередным при оценке проблем информационной безопасности.

В 2016 году Гизем Огютчу ,Озлем Мюге Тестик, Умутом Чусейноглу проанализировано поведение и осведомленность 881 пользователей информационных систем в области безопасности личной информации. В зависимости от данных, собранных с помощью опросов, были разработаны четыре шкалы: шкала рискованного поведения (RBS), шкала консервативного

поведения (CBS), шкала подверженности правонарушениям (EOS) и шкала восприятия риска (RPS). По результатам исследования было определено, что безопасность – это не проблема технологий, а проблема человеческой природы, поведения пользователей, их осведомленность об информационной безопасности [31].

В 2022 Цзюнь Ли, Кай Цзоу, Подкладка Син в исследовательской статье «Распределение внутренних ресурсов для информационной безопасности умных городов с использованием модели эволюционной игры» сосредоточили внимание на распределении информационных ресурсов умных городов, проанализировав взаимосвязь между факторами информационной безопасности, построив направленный граф связей и матрицу смежности, в целях получения диаграммы направленной иерархической структуры путем расчета матрицы достижимости, тем самым разработав объяснительную структурную модель для ресурсов информационной безопасности в умных городах. Влияющими факторами были определены десять классов: технические специалисты, система управления, основное оборудование, IoT-оборудование, сетевое оборудование, прикладные системы, внешняя среда, данные, профилактические меры и защитные меры посредством комплексного анализа. Анализ взаимосвязи данных факторов основывался на мнении экспертов в данной области [32].

В январе 2024 года Венди Ю., Закари А., Коллиер, Текди Ш. разработали методологию для оценки и сравнения политик информационной безопасности в процессе выбора партнеров. Политика информационной безопасности компании была определена основополагающим фактором, влияющим на уровень информационной безопасности при обмене информацией между компаниями. Посредством алгоритмов анализа текстов была проведена оценка политики конфиденциальности данных по отраслям [33].

Обзор исследований российского и зарубежного опыта по оценке информационной безопасности показывает высокий интерес исследователей

в области информационной безопасности как на уровне физических лиц, так и на уровне государства.

Установленная тенденция обусловлена всеобщим пониманием о том, что в процессе стремительной глобальной цифровизации мы сталкиваемся с проблемами информационной безопасности, которые раньше для нас не имели место быть и мы должны успевать на них реагировать. При этом скорость нашей реакции должна превосходить последствия от процессов становления информационного общества.

Так, по мнению М. М. Васильевой «становление информационного общества в России, с одной стороны, – это объективная необходимость развития современного социума на пути к экономическому процветанию и интеграции в глобальное информационное пространство, с другой стороны, – необходимость защиты и отстаивания интересов России в сфере информационной безопасности, прогнозировании угроз размыванию культурных и нравственных национальных ценностей в условиях глобализации мирового информационного пространства» [34].

Е. А. Стукаленко определяет безопасность информационной деятельности населения как самый уязвимый компонент качества жизни населения с точки зрения рисков ее снижения при внедрении цифровой экономики [35]. Серьезными рисками выделены: утечка конфиденциальных данных, коммерческих сведений и информации, составляющей государственную тайну, утечку персональных данных граждан за границу к мощным иностранным игрокам, что может привести к риску возникновения внешнего управления страной рост экономических преступлений.

2 Анализ факторов, оказывающих влияние на информационную безопасность населения

2.1 Методические подходы к расчету показателя информационной безопасности

Показатель информационной безопасности населения определяет информационную безопасность как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан.

Теоретические основы вышестоящего определения закреплены в Законе РФ от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене» [2].

Обобщив факторы, оказывающие влияние на информационную безопасность населения, была разработана методология количественного расчета показателя информационной безопасности населения на основе имеющихся статистических данных.

При расчете показателя информационной безопасности населения использовалась официальная информация Федеральной службы государственной статистики РФ по регионам с 2019 по 2022 год.

Метод сбора данных – опрос населения. Опрос населения проводился по форме федерального статистического наблюдения № 1-ИТ «Анкета выборочного федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей», утверждаемой приказом Росстата. Анкета ИКТ содержит перечень вопросов, характеризующих использование ИКТ частными домашними хозяйствами и населением, с указаниями по ее заполнению.

Объем выборки при проведении обследования ИКТ составляет около 154 тыс. человек в возрасте от 15 лет и старше (приблизительно 64 тыс. домашних хозяйства), что соответствует 0,12% численности населения данного возраста.

Доля населения, столкнувшегося с проблемами информационной безопасности выражена в процентах от общей численности населения в возрасте 15 лет и старше, использовавшего сеть Интернет в течение последних 12 месяцев.

Стоит отметить, что при формировании итогов обследования ИКТ его результаты распространяются на все частные домохозяйства и все население, проживающее в них.

По результатам анкетирования Росстатом была сформирована база данных по 10 направлениям, выраженная в процентах от общего числа опрошенных домохозяйств, которая отражала долю населения, столкнувшегося с проблемами информационной безопасности. Всего было зафиксировано 10 направлений (угроз информационной безопасности населения), данные по которым легли в структуру расчета показателя информационной безопасности населения. Они представлены в Таблице 1.

Таблица 1 – Структура показателя информационной безопасности населения

Условное обозначение	Наименование субпоказателя
(P1)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством заражения вирусами, что привело к потере информации и (или) времени на их удаление
(P2)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством несанкционированного доступа к устройству опрашиваемого, информационным ресурсам, информационным системам
(P3)	Доля населения, столкнувшаяся с проблемами информационной безопасности несанкционированной рассылкой (спамом)

Окончание таблицы 1

(P4)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством посещения детьми нежелательных сайтов, контактами детей с потенциально опасными людьми через сеть Интернет
(P5)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством хищением денежных средств или персональных данных
(P6)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством использования мобильного телефона опрашиваемого неизвестными лицами (например, при краже устройства)
(P7)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством использования электронной почты неизвестными лицами
(P8)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством других проблемам
(P9)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством получения по электронной почте мошеннических писем с просьбой выслать персональные данные (например, логин и пароль для доступа к учетной записи, паспортные данные, реквизиты банковской карты и т.п.)
(P10)	Доля населения, столкнувшегося с проблемами информационной безопасности посредством перенаправления на фальшивые сайты с просьбой указать персональные данные (например, логин и пароль для доступа к учетной записи, паспортные данные, реквизиты банковской карты и т.п.

Рассмотрим результаты анкетирования выраженного в долях населения, сталкивающегося с проблемами информационной безопасности в динамике по годам с 2019 по 2022 гг. на территории Российской Федерации на Рисунке 1.

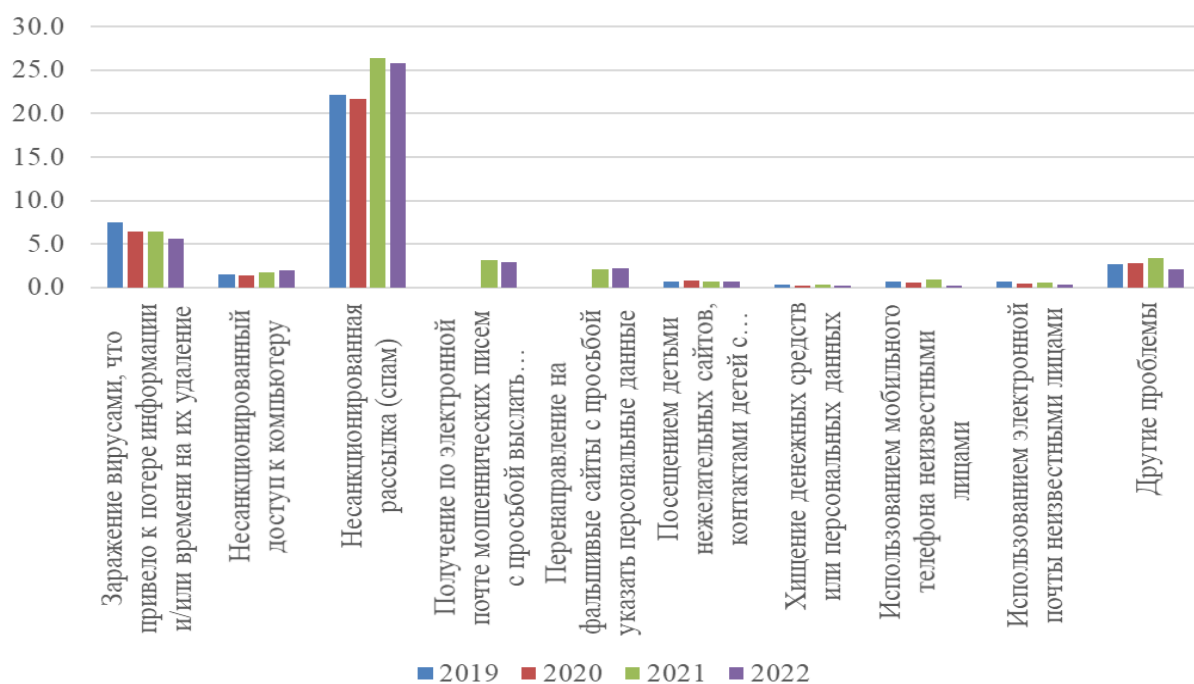


Рисунок 1 – Доля населения столкнувшаяся с проблемами информационной безопасности на территории РФ в период с 2019 по 2022 гг.

Из представленного Рисунка 1 можно сделать вывод, что чаще всего население на территории Российской Федерации сталкивается с такими проблемами информационной безопасности как:

- несанкционированной рассылкой (спамом);
- заражением вирусами, что приводит к потере информации и/или времени на их удаление;
- несанкционированный доступ к устройству опрашиваемого, информационным ресурсам, информационным системам
- хищением денежных средств или персональных данных.

Рассмотрим каждый фактор более подробно.

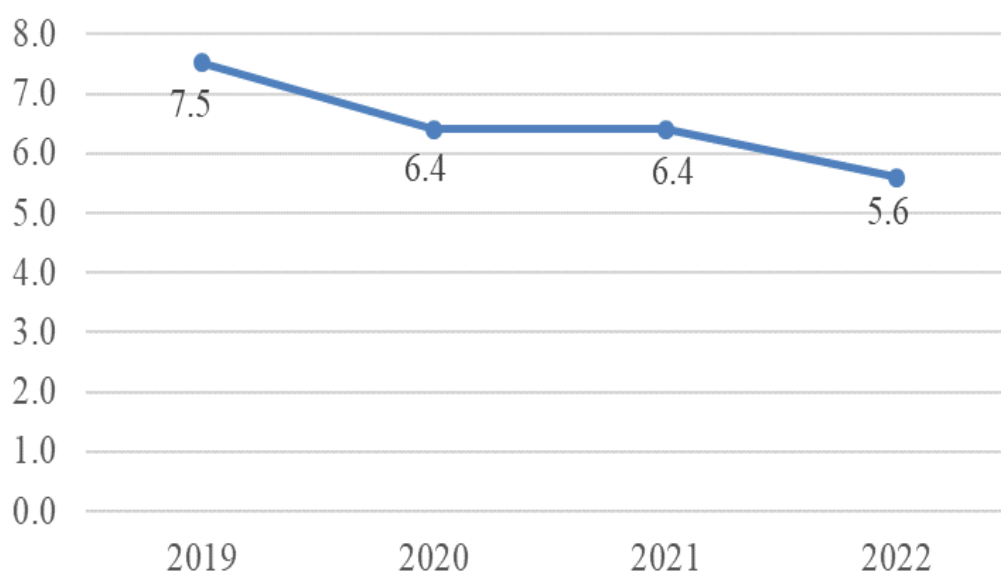


Рисунок 2 – Динамика заражения вирусами, что привело к потере информации и/или времени на их удаление

Как мы видим из Рисунка 2 наблюдается положительная динамика, что говорит о снижении столкновений населения с заражением вирусами, которые приводят к потере информации. Это очень благоприятная тенденция, курсу которой способствует применения средств антивирусного программного обеспечения.

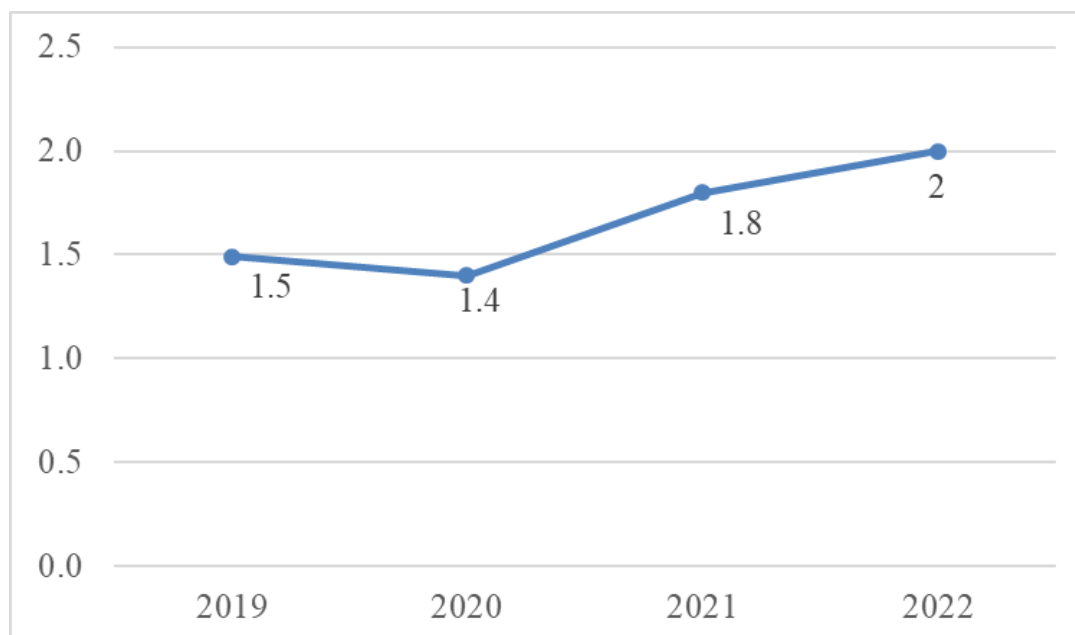


Рисунок 3 – Динамика несанкционированного доступа к устройству опрашиваемого, информационным ресурсам, информационным системам

Динамика несанкционированного доступа к устройству опрашиваемого, информационным ресурсам, информационным системам как мы видим из Рисунка 3 наблюдается отрицательная. По мнению автора, это связано с низким уровнем знаний населения о защите своих социальных сетей, а также организационной техники средствами защиты информации (паролями, двухфакторными системами обеспечения).

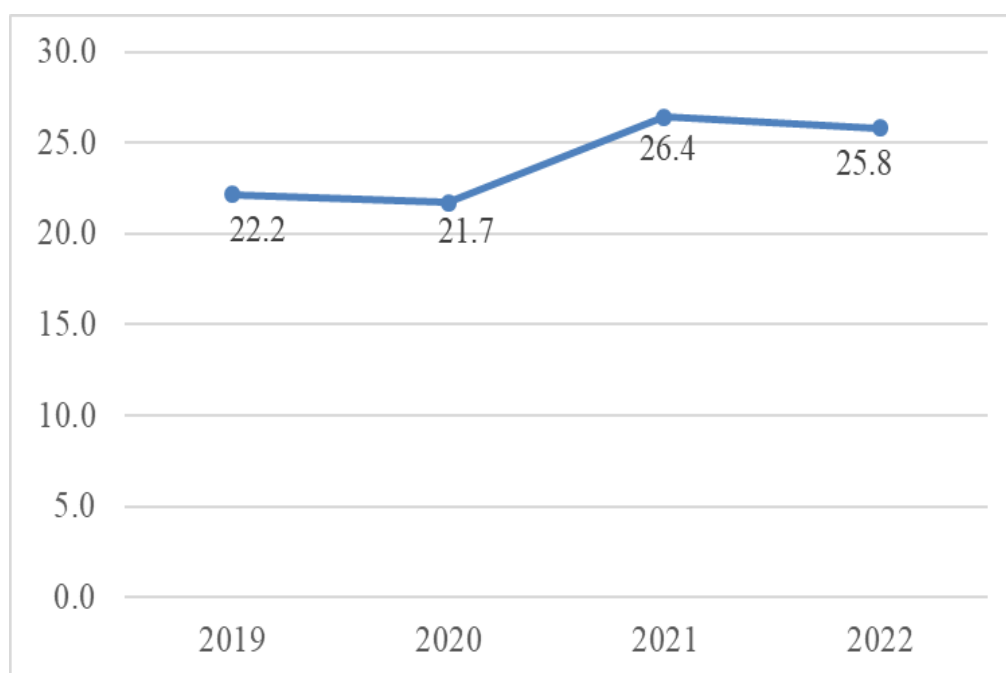


Рисунок 4 – Динамика несанкционированной рассылки (спама)

Из Рисунка 4 можно сделать вывод что в период с 2020 по 2021 год население, сталкивающееся с несанкционированной рассылкой (спамом) составило существенный прирост, в 2022 году результаты опроса показали положительную динамику.

Динамика по показателю хищение денежных средств и персональных данных представленная на Рисунке 5 неоднозначная. В 2021 году произошел резкий скачок (0,3%), который к 2022 году снизился до уровня 2020 года.

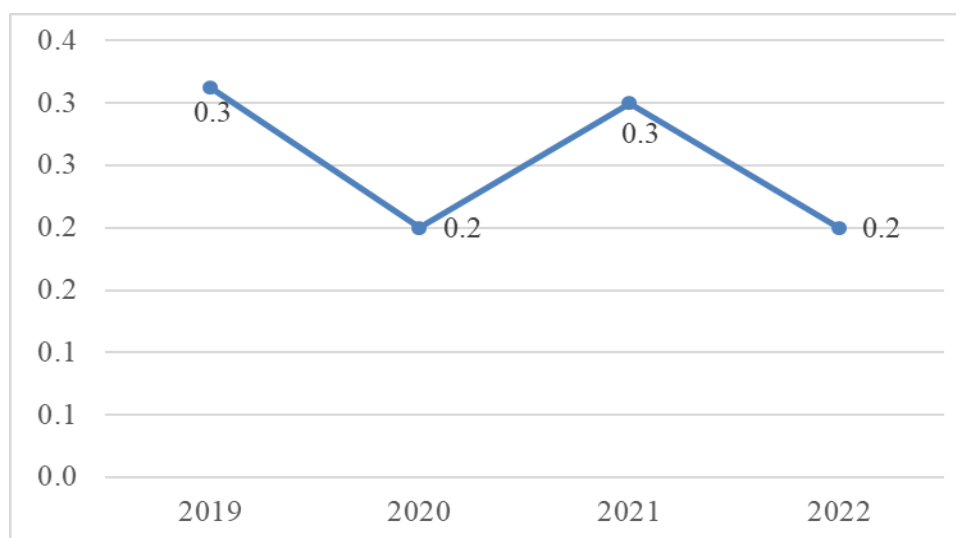


Рисунок 5 – Динамика хищения денежных средств или персональных данных

Прежде всего автор связывает это с условиями пандемии в 2021 году, что привело к переходу на «удаленный» режим работы.

Далее по вышеустановленным субпоказателям произведем расчет показателя информационной безопасности населения расчетным методом по средневзвешенной.

$$\text{Средневзвешенное значение} = \frac{\sum w_i X_i}{\sum w_i}, \quad (2)$$

где w_i = значения веса

X_i = значения данных

В целях определения веса каждого субпоказателя использовалась следующая формула:

$$w_i = (P_i * 100) / \sum X_i, \quad (3)$$

где w_i = значения веса

P_i = значение субпоказателя

Данная методология была определена исходя из теории вероятности и математической статистики, а также имеющихся статистических данных

позволяющих количественно оценить уровень информационной безопасности населения.

Расчет показателя информационной безопасности населения регионов были получены следующие результаты, представленные на Рисунке 6.

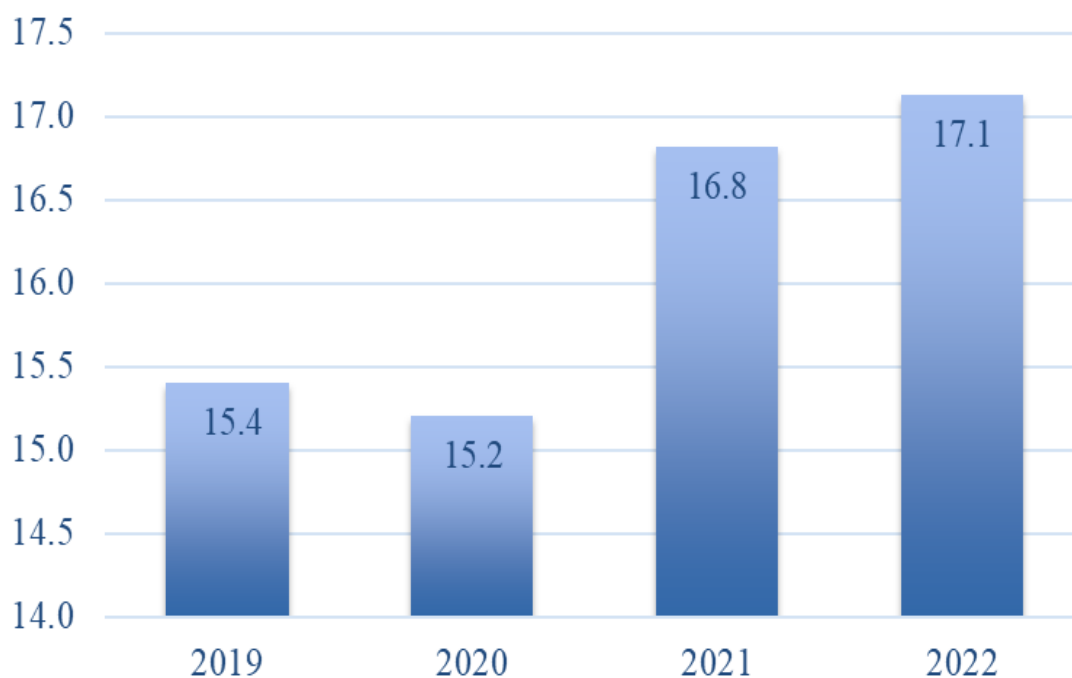


Рисунок 6 – Показатель информационной безопасности населения на территории Российской Федерации

Наибольшие темпы роста показателя информационной безопасности населения наблюдаются в период с 2020 по 2021 год, в целом наблюдается отрицательная тенденция с 2019 года, все чаще население на территории регионов сталкивается с проблемами информационной безопасности, что оказывает негативное влияние на качество жизни граждан нашей страны.

Воспользуемся платформой Kaggle, которая представляет среду для написания кода на языке Python и посредством библиотеки matplotlib визуализируем полученные данные по регионам Российской Федерации.

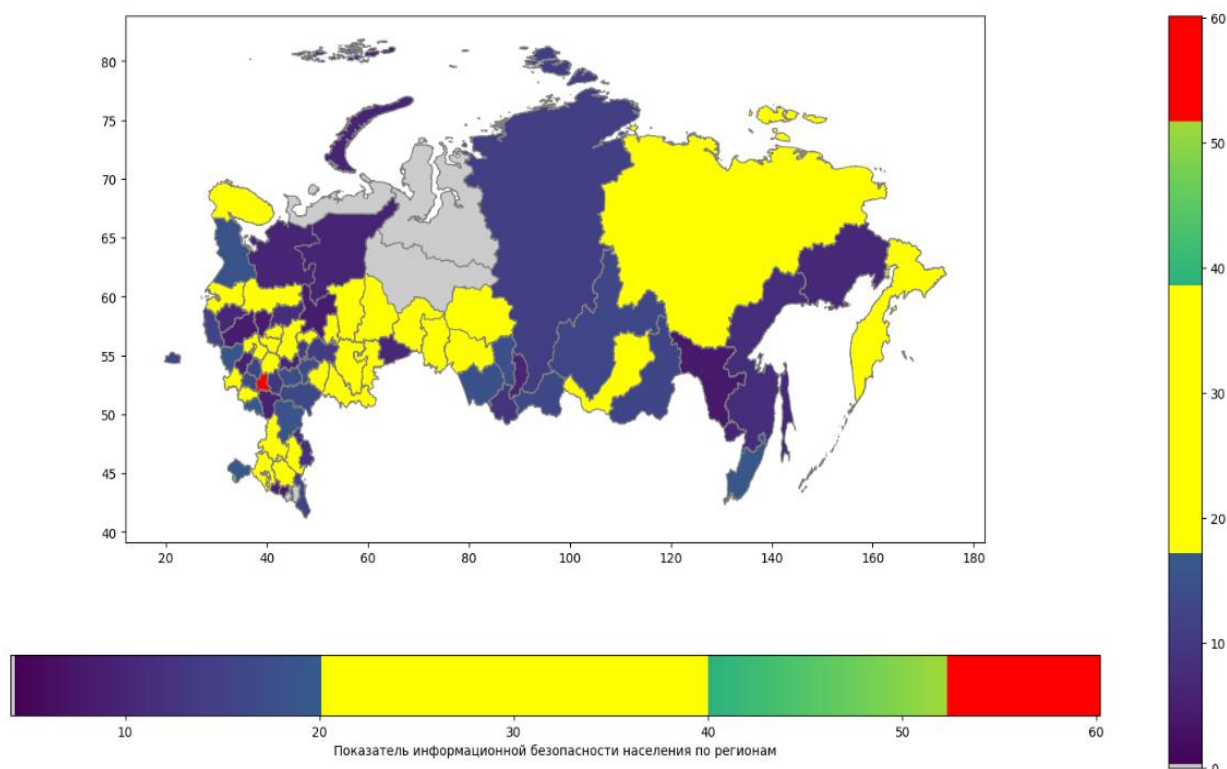


Рисунок 7 – Показатель информационной безопасности населения по субъектам РФ за 2022 год

Карта наглядно отражает показатель информационной безопасности населения по регионам. Так, Республика Саха Якутия, Камчатский край, Республика Бурятия, Мурманская область, Вологодская область, Томская область, Новосибирская область, Омская область, Тюменская область, Челябинская область, Республика Башкортостан, Свердловская область, Пермский край, Удмурдская республика, Московская область и граничащие с ней регионы имеют средний (желтый) уровень информационной безопасности населения, Липецкая область имеет критическое значение и отмечена красным цветом, это означает, что в данном регионе зафиксирован наибольший показатель информационной безопасности. Также высокие показатели информационной безопасности зафиксированы в Амурской области, Кемеровской области, Архангельской области, Республике Коми, Кировской области, Тверской области (фиолетовый цвет).

Рассмотрим показатель информационной безопасности населения по регионам за 2019 год.

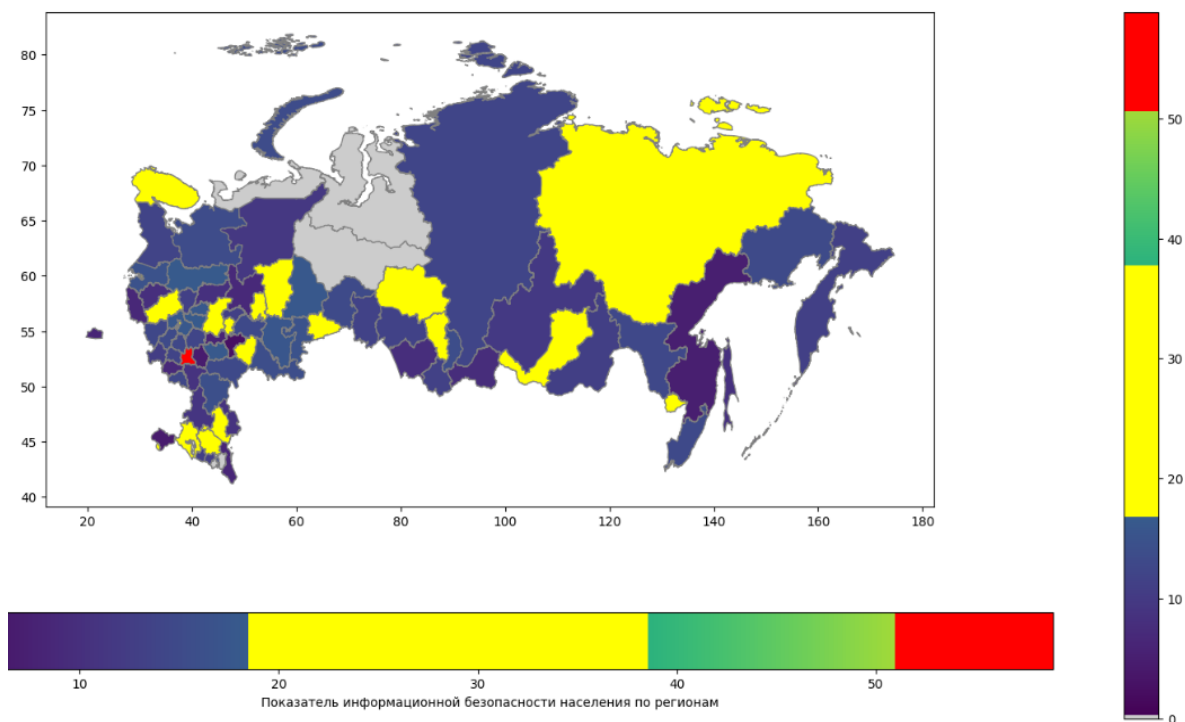


Рисунок 8 – Показатель информационной безопасности населения по субъектам РФ за 2019 год

Из Рисунка 8 мы можем сделать вывод что в ряде регионов за четырехлетний период уровню столкновений населения с проблемами информационной безопасности растет. Интересно отметить что 2019 году Липецкая область по сравнению с иными регионами в большей степени подвержена столкновениям с проблемами информационной безопасности.

Расчет показателя информационной безопасности населения по регионам в количественном выражении представляется возможным определить его зависимой переменной и посредством корреляционно-регрессионного анализа определить влияние независимых переменных.

2.2 Обоснование выборки и описание статистики данных для расчетов

В целях проведения исследования были собраны числовые панельные данные по семи факторам, предположительно оказывающим статистически

значимое влияние на показатель информационной безопасности населения в период с 2019 по 2022 года из официальных источников Федеральной службы государственной статистики [36], а также всероссийской акции, признанной самой масштабной в России проверкой знаний в области цифровой грамотности населения [37].

Факторы были сформированы с учетом возможности их получения из базы данных официальной статистической информации, а также с учетом требований информационной достаточности описания. К исследуемым факторам относятся:

1. Уровень цифровой грамотности населения.
2. Среднедушевые денежные доходы населения.
3. Объем информации, переданной при доступе к сети Интернет, петабайт (фиксированный доступ + мобильный доступ).
4. Затраты на внедрение и использование цифровых технологий (млн. руб.).
5. Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения.
6. Плотность населения на 1 км².
7. Использование сети интернет населением.

Рассмотрим каждый фактор более подробно.

Уровень цифровой грамотности населения определяется по результатам Всероссийской акции «Цифровой Диктант.РФ» (далее – Цифровой диктант). Первый Цифровой диктант был проведен в 2019 году. На тот момент количество участников составило 39 398 человек, среднее значение уровня цифровой грамотности всех участников было зафиксировано на уровне 7,15 из 10. «Отличники» Цифрового Диктанта 304 человека (0,77%) от всех участников, 37% пользователей продемонстрировали высокий уровень знаний в области кибербезопасности.

В 2020 году количество участников Цифрового диктанта составило 330 148 человек, среднее значение уровня цифровой грамотности всех участников было зафиксировано 7,25 из 10, что на 0,1 больше, чем в 2019 году. «Отличники» Цифрового Диктанта уже 11 538 человека (3,5%) от всех участников, что на 2,73 % больше года ранее. Всего 37% пользователей продемонстрировали высокий уровень знаний в области кибербезопасности. Особенностью цифровой безопасности в 2020 году стало то, что 73% взрослых не знают основные правила создания надежного пароля.

В 2021 году количество участников Цифрового диктанта дошло до отметки в 919 317 человек, среднее значение уровня цифровой грамотности – 6,90 из 10. «Отличники» Цифрового Диктанта 13 321 человека (1,4%) от всех участников. В 2021 году численность участников выросла в 2,8 раза в сравнении с 2020 годом. Общее падение уровня цифровой грамотности в 2021 году сопровождалось ростом цифрового потребления, а также снижением уровня цифровых компетенций, к ключевым факторам, повлиявшим на динамику эксперты относят пандемию коронавируса и связанным с ней переход многих повседневных процессов в онлайн-формат.

В 2023 году количество участников акции составило 1 358 643 человек, что больше значений 2019 года на 1 319 245 участников. Среднее значение уровня цифровой грамотности всех участников 6,43 из 10. По сравнению с 2021 годом численность участников выросла в 1,5 раза, что говорит о потребности населения в повышении своих цифровых навыков. Наиболее высокие значения в 2023 году показали аудитории 26-35 и 36-45 лет – 6,96 балла и 6,73 балла, соответственно. К ключевым факторам, повлиявшим на текущий уровень цифровой грамотности организаторы по итогам акции относят:

1. Увеличение количества участников.
2. Увеличение количества новых импортозамещающих сервисов и услуг, с которыми плохо знаком потребитель.

3. Изменение рекламного ландшафта, с которым плохо знаком потребитель.

4. Увеличение количества внешних угроз в разрезе цифровой безопасности.

Интересно отметить, что наилучшие результаты анкетирования по цифровой грамотности населения были зафиксированы в 2020 году – 3,5% от всех участников. В 2023 году данный показатель составил всего 0,6 % от всех участников.

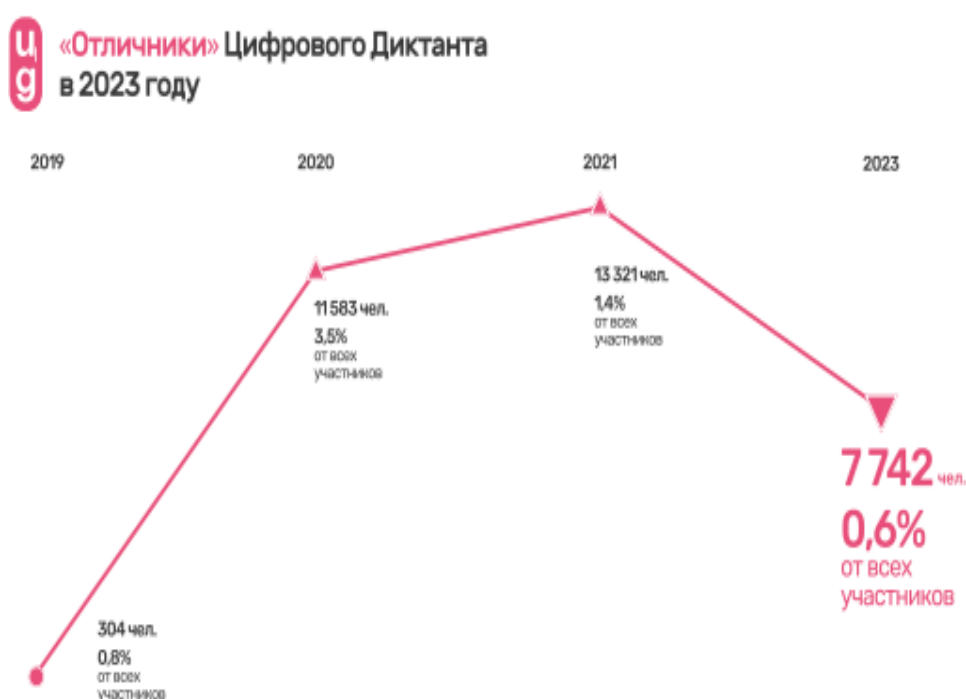


Рисунок 9 – «Отличники» Цифрового Диктанта

Сокращение «Отличников» в 2023 году, предположительно вызвано увеличением количества новых импортозамещающих сервисов и услуг, с которыми плохо знаком потребитель.

Особенностями цифровых компетенций в 2023 году выделяют то, что более 80% детей (7-13 лет) обладают низким уровнем знаний о защите конфиденциальной информации, только 32 % взрослых (18-59 лет) обладают

навыками работы с антивирусным ПО, а аудитория в возрасте 60+ лет показала дефицит знаний о том, как восстановить доступ к личным аккаунтам в социальных сетях.

В Таблице 2 представлены регионы-лидеры, а также аутсайдеры по уровню цифровой грамотности населения в период с 2019 по 2022 год.

Таблица 2 – Рейтинг регионов по уровню цифровой грамотности населения в период с 2019 по 2022 год

№ п/п	Регион	Значение	Блок
2019			
1	г. Санкт-Петербург (7,55)	≥ 7,0	1
2	Республика Алтай (7,5)		
3	Костромская область (7,49)		
4	Омская область (7,45)		
5	Ярославская область (7,44)		
6	Калужская область (7,42)		
7	Тюменская область (7,4), Рязанская область (7,39), Республика Коми (7,39), Томская область, Приморский край, Тульская область, Удмуртская Республика, Пермский край, Нижегородская область, Красноярский край (7,34), Тверская область, Архангельская область, Пензенская область, Свердловская область, г. Москва, Тамбовская область, Республика Татарстан (Татарстан), Новгородская область, Кировская область, Воронежская область, Республика Марий Эл, Саратовская область, Курганская область, Алтайский край, Московская область, Мурманская область, Ставропольский край, Владимирская область, Орловская область, Ханты-Мансийский авт. округ, Самарская область, Челябинская область, Республика Башкортостан, Республика Бурятия, Ивановская область, Оренбургская область, Брянская область, Республика Мордовия. Кемеровская область, Чувашская Республика – Чувашия, Кабардино-Балкарская Республика, Новосибирская область, Камчатский край		

Продолжение таблицы 2

№ п/п	Регион	Значение	Блок
8	Калининградская область, Хабаровский край, Ямало-Ненецкий авт.округ, Вологодская область, Амурская область, Иркутская область, Сахалинская область, Ульяновская область, Республика Дагестан, Республика Карелия, Псковская область, Республика Северная Осетия-Алания, Еврейская авт.область, Ленинградская область, Смоленская область, Республика Саха (Якутия), Липецкая область, Магаданская область, Чукотский авт.округ, Забайкальский край, Белгородская область, Республика Ингушетия, Республика Хакасия, Чеченская Республика, Карачаево-Черкесская Республика, Ненецкий авт.округ	≥6,0 <7,0	2
9	Республика Тыва (5,68)	<6	3
10	Курская область (5,61)		
2020			
1	Свердловская область (7,96)	≥ 7,0	1
2	Тамбовская область (7,84)		
3	г. Санкт-Петербург (7,84)		
4	Владимирская область (7,79)		
5	Псковская область (7,79)		
6	Орловская область (7,72), Калининградская область (7,71), Иркутская область (7,71), Ярославская область (7,70), Пензенская область, Ленинградская область, Кировская область, Липецкая область, Республика Марий Эл, Пермский край, Республика Северная Осетия-Алания, Саратовская область, Московская область, Республика Карелия, Удмуртская Республика, Ханты-Мансийский авт.округ, Воронежская область, Самарская область, Тверская область, Нижегородская область, Тюменская область, Архангельская область, Приволжский федеральный округ, Смоленская область, Мурманская область, Приморский край, Республика Татарстан (Татарстан), Брянская область, Чувашская Республика – Чувашия, Тульская область, Рязанская область, Оренбургская область, Новосибирская область, Новгородская область, Магаданская область, Курская область, г. Москва, Белгородская область, Ивановская область, Ульяновская область, Ямало-Ненецкий авт.округ, Вологодская область, Красноярский край (7,22), Еврейская авт.область, Ставропольский край, Камчатский край, Костромская область, Кемеровская область, Калужская область, Республика Хакасия, Челябинская область, Ненецкий авт.округ, Республика Коми, Алтайский край, Республика Мордовия, Томская область, Хабаровский край, Омская область, Забайкальский край, Сахалинская область		

Продолжение таблицы 2

№ п/п	Регион	Значение	Блок
7	Республика Башкортостан, Курганская область, Амурская область, Чукотский авт.округ, Карачаево-Черкесская Республика, Республика Саха (Якутия), Республика Алтай, Республика Бурятия, Кабардино-Балкарская Республика, Республика Ингушетия, Республика Дагестан, Республика Тыва (6,11)	$\geq 6,0 < 7,0$	2
9	Чеченская Республика (5,91)	< 6	3
2021			
1	Республика Карелия (7,62)	$\geq 7,0$	1
2	Нижегородская область (7,48)		
3	Тамбовская область (7,37)		
4	Удмуртская Республика (7,37)		
5	Оренбургская область (7,36), Ивановская область (7,30), г. Москва (7,30), Воронежская область (7,29), Московская область, Брянская область, Вологодская область, Тверская область, Республика Мордовия, Липецкая область, Смоленская область, Чувашская Республика – Чувашия, Свердловская область, Республика Татарстан (Татарстан), Пензенская область, Ханты-Мансийский авт.округ, Архангельская область, Мурманская область, Калининградская область, Калужская область, Саратовская область, Курская область, Ярославская область, Ленинградская область, Пермский край, Костромская область, Алтайский край, Псковская область, Ямало-Ненецкий авт.округ, Курганская область		
6	Рязанская область, Белгородская область, Кемеровская область, Ульяновская область, Новосибирская область, Самарская область, Республика Хакасия, Владимирская область, Иркутская область, Республика Коми, Хабаровский край, Орловская область, Новгородская область, Челябинская область, Ставропольский край, Республика Марий Эл, Кировская область, Магаданская область, Тульская область, г. Санкт-Петербург, Омская область, Приморский край, Ненецкий авт.округ, Тюменская область, Сахалинская область, Кабардино-Балкарская Республика, Красноярский край, Карачаево-Черкесская Республика, Республика Башкортостан, Забайкальский край, Томская область Камчатский край, Республика Северная Осетия-Алания, Республика Бурятия, Еврейская авт.область, Амурская область, Республика Саха (Якутия), Чукотский авт.округ, Республика Алтай	$\geq 6,0 < 7,0$	2
7	Республика Дагестан (5,99), Республика Тыва (5,92), Чеченская Республика (5,42), Республика Ингушетия (5,17)	< 6	3
2022			

Окончание таблицы 2

№ п/п	Регион	Значение	Блок
1	Республика Карелия (7,48)	≥ 7,0	1
2	г. Москва (7,32)		
3	Воронежская область (7,10)		
4	Архангельская область (7,09)		
5	Ивановская область (7,07), Чувашская Республика – Чувашия (7,02), Смоленская область (7,01), Пензенская область (7,01), Вологодская область, Нижегородская область		
6	Ханты-Мансийский авт.округ, Свердловская область, Ярославская область, Республика Татарстан (Татарстан), Пермский край, Курская область, Алтайский край, Республика Мордовия, Калужская область, Мурманская область, Костромская область, Калининградская область, Московская область, Орловская область, Рязанская область, Ленинградская область, Иркутская область, Самарская область, Республика Коми, Ямало-Ненецкий авт.округ, Удмуртская Республика, Псковская область, Челябинская область, Курганская область, Тамбовская область, Новгородская область, Оренбургская область, г. Санкт-Петербург (6,71), Кировская область, Липецкая область, Хабаровский край, Новосибирская область, Владимирская область, Брянская область, Саратовская область, Тюменская область, Кемеровская область, Магаданская область, Тверская область, Республика Хакасия, Ставропольский край, Ульяновская область, Ненецкий авт.округ, Красноярский край (6,52), Омская область, Приморский край, Сахалинская область, Республика Марий Эл, Белгородская область, Кабардино-Балкарская Республика, Тульская область, Карачаево-Черкесская Республика, Республика Башкортостан, Забайкальский край, Республика Бурятия, Дальневосточный федеральный округ, Республика Северная Осетия-Алания, Томская область, Республика Саха (Якутия), Камчатский край, Еврейская авт.область, Амурская область, Чукотский авт.округ, Республика Алтай	≥6,0 <7,0	2
7	Республика Дагестан (5,86), Республика Тыва (5,60), Республика Ингушетия (5,27), Чеченская Республика (5,22)	<6	3

В 2019 году 1 место по уровню цифровой грамотности населения занял г. Санкт-Петербург со значением (7,55), в 2020 году уровень грамотности в данном регионе возрос (7,84), результат занял позицию второго места разделив его с Тамбовской областью, наилучший показатель был установлен в Свердловской области со значением 7,96, что является лучшим результатом за весь исследуемый период с 2019 по 2022 год.

Значение уровня цифровой грамотности населения Красноярского края в 2019 году было зафиксировано на уровне 7,34, что является хорошим показателем, к 2023 году значение снизилось и составило 6,52.

В связи с пандемией в 2022 году вызванной короновирусной инфекцией Всероссийская акция «Цифровой Диктант.РФ» проведена не была. Данные за 2022 год были рассчитаны посредством среднеарифметической по формуле (4):

$$\bar{x} = \frac{x_1 + x_2 + \dots + x_n}{n} = \frac{\sum_{i=1}^n x_i}{n} \quad (4)$$

где x – индивидуальные значения признака;

n – число единиц в совокупности.

В связи с отсутствием данных по Южному федеральному округу из генеральной совокупности были исключены следующие регионы: Республика Адыгея (Адыгея), Республика Калмыкия, Республика Крым, Краснодарский край, Астраханская область, Волгоградская область, Ростовская область, г. Севастополь.

Среднедушевые денежные доходы населения (в месяц) - исчисляются делением годового объема денежных доходов на 12 и на среднегодовую численность населения [38]. Иначе это денежные доходы в расчете на одного человека. Фактор среднедушевые денежные доходы был выбран в связи с тем, что общий объем доходов распределяется по всему населению, включая детей всех возрастов, безработных, пенсионеров, студентов и др., а также является важнейшей характеристикой уровня жизни населения [39].

Рогачева О. А. в научной статье «Среднедушевые денежные доходы населения: сопоставление по разным источникам» отмечала: что «Денежные доходы являются определяющим фактором поведения населения относительно расходов и благосостояния в целом») [40].

Рассмотрим динамику по федеральным округам представленную на Рисунке 10.

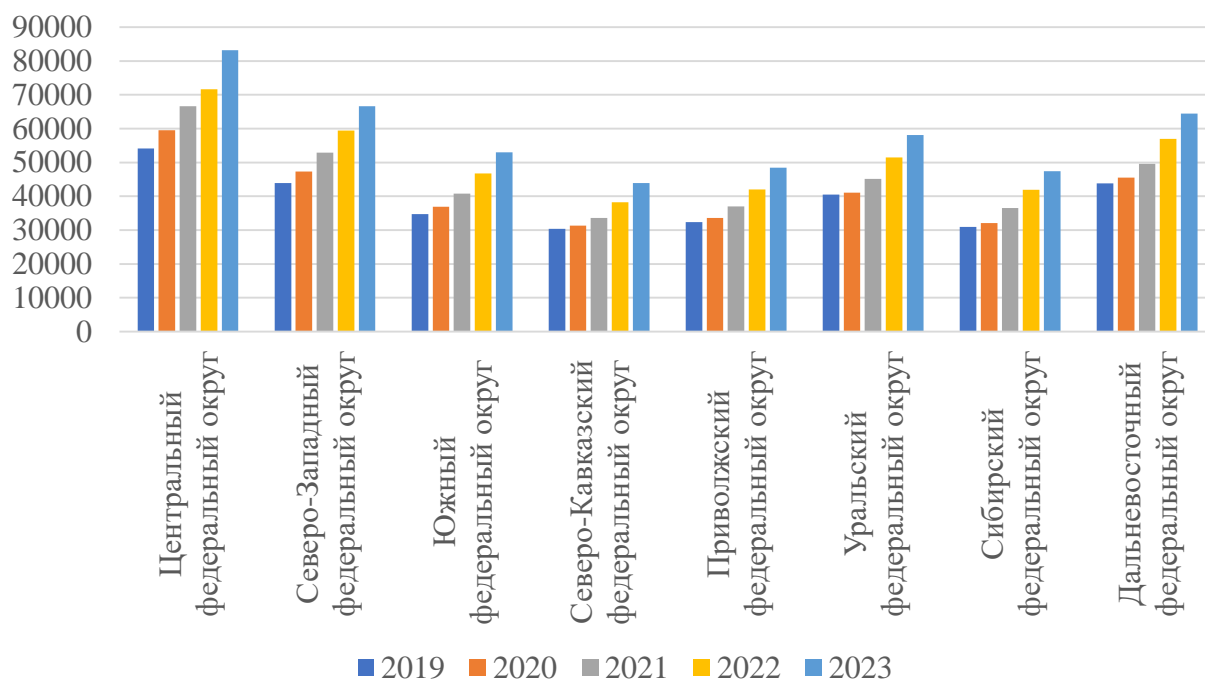


Рисунок 10 – Динамика среднедушевых денежных доходов населения по федеральным округам

Наибольший уровень среднедушевых денежных доходов населения установлен на территории Центрального Федерального округа (далее – ЦФО). Также в нем установлены наибольшие темпы роста в период с 2022 по 2023 год. Наименьший уровень среднедушевых денежных доходов населения зафиксирован в СевероКавказском Федеральном округе и на 2023 год его уровень составляет чуть более 40 000,00 рублей на одного человека, что в два раза меньше чем в ЦФО.

Выбросы в данных по показателю «Среднедушевые денежные доходы населения» отсутствуют.

Объем информации, переданной при доступе к сети Интернет выраженный в петабайтах отражает уровень развития цифровой инфраструктуры в регионах, который обеспечивает возможности распространения результатов научно-технологического развития [41]. Так,

по данным Росстата, объем информации, переданной при доступе к сети Интернет, возрос при фиксированном доступе в Интернет в 10 раз (с 8 274 петабайт в 2011 году до 87 081,7 петабайт в 2022 году), при мобильном доступе возрос в 154 раз (с 218 петабайт в 2011 году до 33 768,1 в 2022 году). Стоит отметить, что под фиксированным интернетом в настоящем контексте понимается (проводной и беспроводной) Интернет через модемное подключение посредством коммутируемой телефонной линией, ISDN – связь, цифровую абонентскую линию (технология xDSL и так далее), другую кабельную связь (включая выделенные линии, оптоволокно и другое), спутниковую связь, фиксированную беспроводную связь, беспроводную локальную сеть и WiMAX [42].

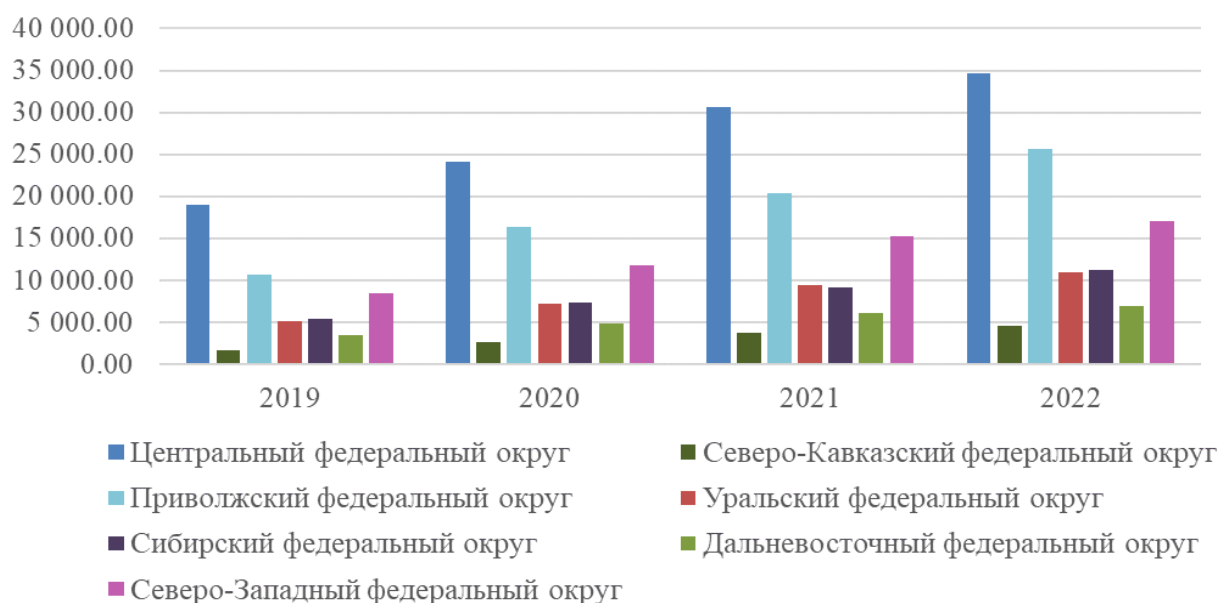


Рисунок 11 – Динамика объема информации, переданной при доступе к сети Интернет, петабайт (фиксированный доступ + мобильный доступ)

Как мы видим из представленного Рисунка 11 наибольший объем информации, передаваемой при доступе к сети Интернет установлен в Центральном федеральном округе, следом за ним идет Приволжский федеральный округ, тройку лидеров замыкает Северо-Западный федеральный округ. Динамика данного фактора у всех федеральных округов уставлена положительная, что задает тренд на дальнейший рост.

В связи с отсутствием данных по данному фактору из генеральной совокупности были исключены такие регионы как Ненецкий автономный округ, Архангельская область без авт. Округа, Ханты-Мансийский автономный округ, Ямало-Ненецкий автономный округ и Тюменская область без авт. Округов.

Фактор «Затраты на внедрение и использование цифровых технологий» определяется Росстатом на основании [43]. Данный приказ содержит форму № 3-информ, которая является годовой и обязательна для заполнения органам власти и местного самоуправления, а также учреждениям, основной вид деятельности которых относится, в частности, к группам ОКВЭД:

- лесное хозяйство, охота, рыболовство и рыбоводство;
- деятельность гостиниц и организаций общественного питания;
- деятельность в области информации и связи;
- деятельность профессиональная, научная и техническая;
- государственное управление и обеспечение военной безопасности;
- высшее образование и подготовка кадров высшей квалификации;
- деятельность в области здравоохранения и предоставления социальных услуг;
- деятельность в области культуры, спорта, организации досуга и развлечений.

Данный фактор включает в себя следующие направления расходов:

- затраты на продукты и услуги в области информационной безопасности;
- затраты на «сквозные» цифровые технологии;
- внутренние затраты на внедрение и использование цифровых технологий (на приобретение машин и оборудования, связанных с цифровыми технологиями, их техническое обслуживание, модернизацию, текущий

и капитальный ремонт, выполненные собственными силами, на приобретение программного обеспечения, на модернизацию и доработку программного обеспечения, выполненные собственными силами, оплата труда специалистов в области ИКТ, на обучение сотрудников, связанное с внедрением и использованием цифровых технологий, на оплату услуг электросвязи, на приобретение цифрового контента и другие внутренние затраты на внедрение и использование цифровых технологий);

– внешние затраты на внедрение и использование цифровых технологий (на оплату услуг сторонних организаций и специалистов, связанных с внедрением и использованием цифровых технологий (кроме услуг связи и обучения));

– прочие внешние затраты на внедрение и использование цифровых технологий.

Рассмотрим в Таблице 3 динамику затрат на внедрение и использование цифровых технологий (млн рублей).

Таблица 3 – Затраты на внедрение и использование цифровых технологий (млн рублей)

Федеральный округ	Период, год			
	2019	2020	2021	2022
Центральный федеральный округ	1 717 059,70	1 707 043,00	2 505 205,10	2 621 217,90
Северо-Западный федеральный округ	127 356,00	175 591,10	318 428,20	341 306,80
Северо-Кавказский федеральный округ	13 802,30	14 912,60	18 526,10	17 954,10
Приволжский федеральный округ	176 901,60	196 555,70	231 040,40	261 635,70

Окончание таблицы 3

Федеральный округ	Период, год			
	2019	2020	2021	2022
Уральский федеральный округ	106 103,40	123 926,50	143 228,00	156 395,40
Сибирский федеральный округ	81 955,80	105 544,60	135 483,60	164 920,20
Дальневосточный федеральный округ	47 045,60	57 811,60	83 011,00	90 172,60

Как мы видим из представленной Таблицы 3 наибольший объем средств, направленный на внедрение и использование цифровых технологий установлен в Центральном федеральном округе, на конец 2022 года его объем составил 2 621 217,90 млн рублей, что в 1,5 раз больше чем четырьмя годами ранее. Также высокие темпы роста зафиксированы в Сибирском федеральном округе, уровень затрат на внедрение и использование цифровых технологий увеличился в два раза и на конец 2022 года составил 164 920,20 млн рублей. Наименьшие темпы роста отмечены в Северо-Кавказском федеральном округе (+ 4 151,8 млн рублей) за четыре года.

Данные по фактору «Затраты на внедрение и использование цифровых технологий (млн. руб.)» имеются в полном объеме, выбросы в данных отсутствуют.

Фактор «Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения», также, как и «Объем информации, переданной при доступе к сети Интернет» отражает уровень развития цифровой инфраструктуры в регионах, который обеспечивает возможности распространения результатов научно-технологического развития [44]. Данный фактор рассчитывается Росстатом по данным Минцифры России с учетом сведений о численности постоянного населения соответствующего года. В настоящее время доступ к широкополосной связи в Интернет рассматривается как услуга, сравнивая по своему вкладу в благосостояние с основными жизненно

важными услугами [45]. Динамика данного фактора, представленная на Рисунке 12 говорит о тенденции дальнейшего роста.

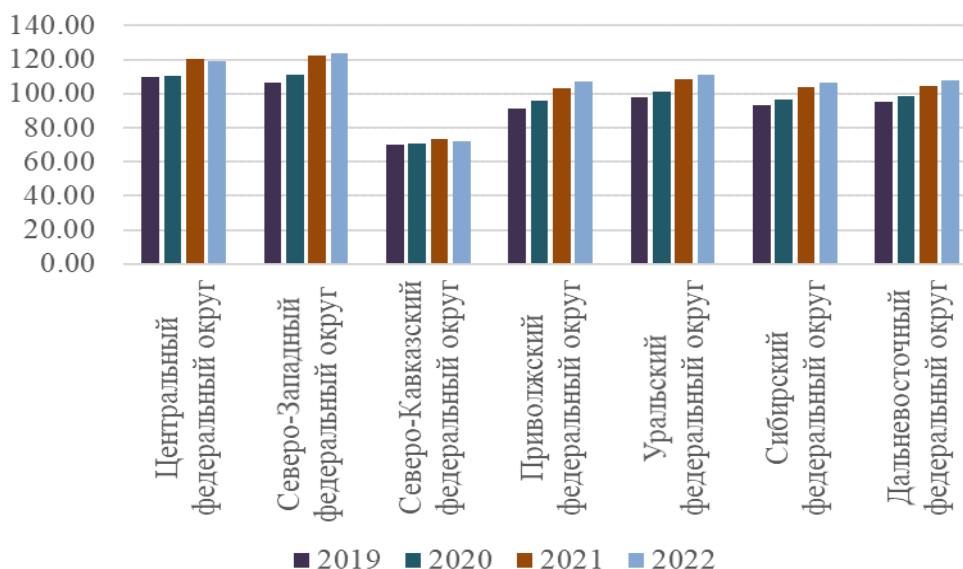


Рисунок 12 – Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения

В связи с отсутствием данных по фактору: «Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения» из генеральной совокупности были исключены такие регионы как Ненецкий автономный округ, Архангельская область без авт. Округа, Ханты-Мансийский автономный округ, Ямало-Ненецкий автономный округ и Тюменская область без авт. Округов.

Плотность населения на 1 км² является одной из важных характеристик региона наравне с его численностью, она показывает число жителей на 1 км². С помощью плотности можно определить равномерность распределения населения на территории, выделить центр тяжести. По мнению автора, эти параметры являются значимыми при определении факторов, оказывающих влияние на показатель информационной безопасности населения.

Рассмотрим заключительный фактор «Использование сети интернет населением».

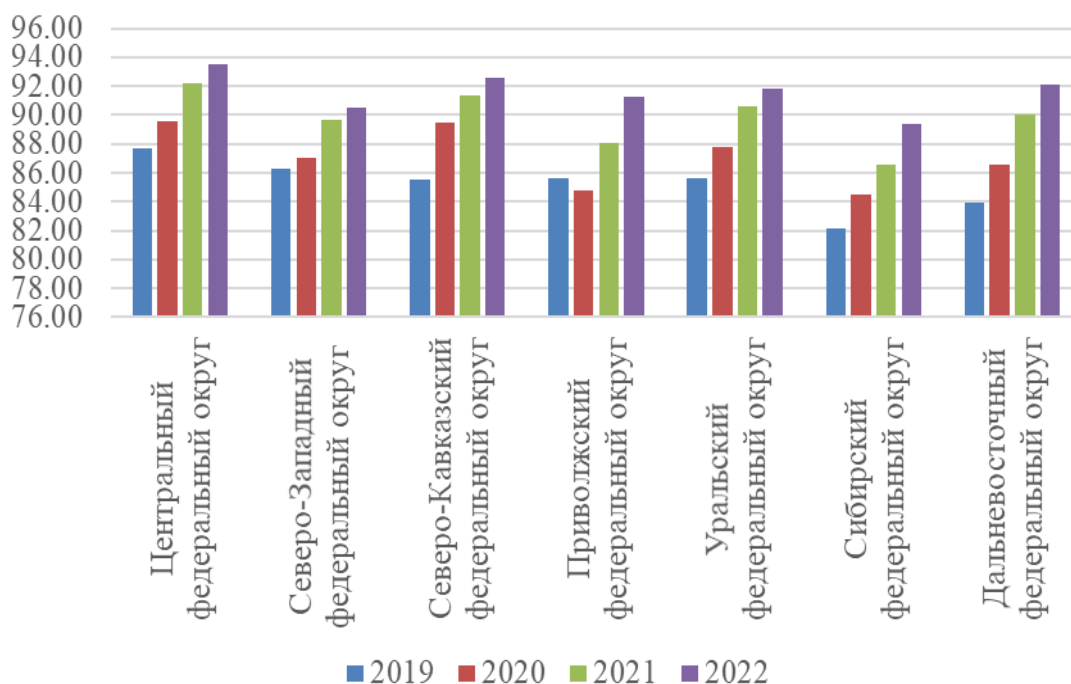


Рисунок 13 – Использование сети интернет населением

Из представленного Рисунка 13 можно сделать вывод, что за исследуемый период наблюдается значительный рост использования сети интернет населением. Наибольшее значения установлено в Центральном федеральном округе, на конец 2022 года оно зафиксировалось на уровне 93,5 %. В Сибирском федеральном округе – 89,4 %, что является наименьшим показателем. Это обусловлено большой территорией, а также вхождением в состав Сибирского федерального округа Арктической зоны, где затраты на проведение линий связи очень велики. Тем не менее ежегодно федеральное и краевое финансирование направлено на выравнивание доступности услуг связи и Интернета для населения на территории РФ, так рамках мероприятия «Субсидии бюджетам муниципальных образований на создание условий для развития услуг связи в малочисленных и труднодоступных населенных пунктах края» государственной программы «Развитие информационного общества», утвержденной постановлением Правительства Красноярского края от 30.09.2013 № 504-п, предоставляются субсидии муниципальным образованиям края на организацию услуг связи [46].

По итогам семи лет (2017-2023) 232 населенных пункта обеспечены услугами связи (нарастающим итогом), из них: 123 – услуги подвижной радиотелефонной связи (далее – ПРТС) и 142 – услуги доступа в сеть Интернет.

На 2024 год предусмотрено 111 млн рублей на обеспечение 58 населенных пунктов, из них 23 – услуги ПРТС, 35 – услуги доступа в сеть Интернет. По состоянию на 01.06.2024 35 населенных пунктов уже обеспечены услугами доступа в сеть Интернет.

2. В рамках федерального проекта «Устранение цифрового неравенства» [47] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации совместно с оператором связи ПАО «Ростелеком» обеспечивает населенные пункты численностью 100-500 услугами ПРТС стандарта 4G (мобильный Интернет).

Так, в 2021 году было обеспечено 27 населенных пунктов, в 2022 году – 17, в 2023 году – 84.

На 2024 год запланировано обеспечение 51 населённого пункта, из которых 8 будут обеспечены услугами ПРТС стандарта 4G в рамках дополнительной квоты.

2.3 Построение модели зависимости показателя информационной безопасности населения и независимыми факторами

Присвоим обозначения независимым переменным, которые предположительно оказывают статистически значимое влияние на показатель информационной безопасности населения (ИБ).

Данные собраны по 74 регионам за четыре периода с 2019 по 2022 год. Имеют панельную структуру.

Таблица 4 – Независимые переменные

№ п/п	Независимые переменные (X)	Обозначение
1	Уровень цифровой грамотности населения	CG
2	Среднедушевые денежные доходы населения	D
3	Объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме подвижных сетей)	Inf
4	Затраты на внедрение и использование цифровых технологий (млн. руб.)	Expenses
5	Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения	Abonenty
6	Плотность населения на 1 км ²	Density
7	Использование сети интернет населением	Internet

С помощью программного обеспечения Gretl проанализируем данные на наличие выбросов с помощью инструмента коробчатая диаграмма.

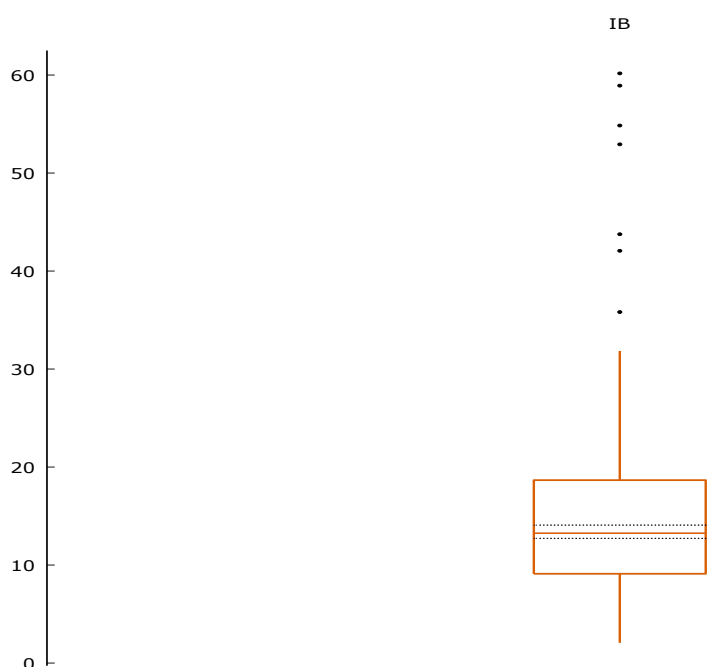


Рисунок 14 – Коробчатая диаграмма «Показатель информационной безопасности населения»

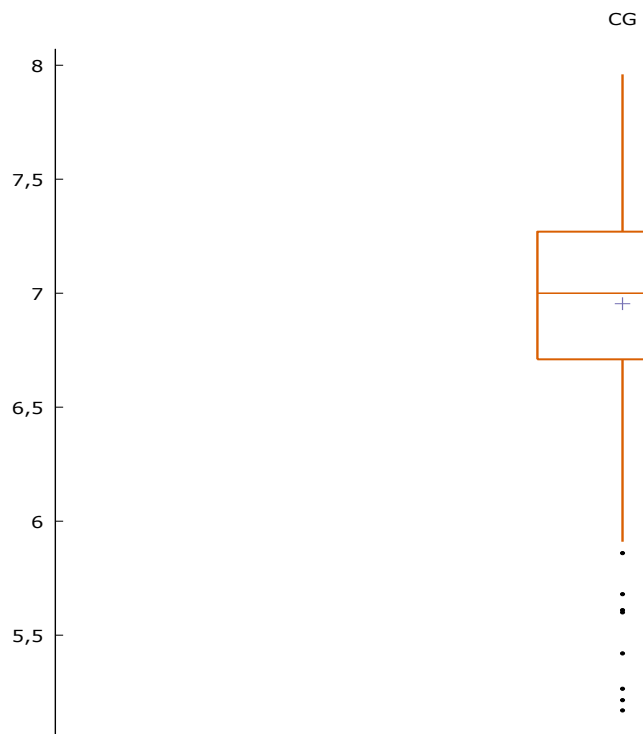


Рисунок 15 – Коробчатая диаграмма «Уровень цифровой грамотности населения»

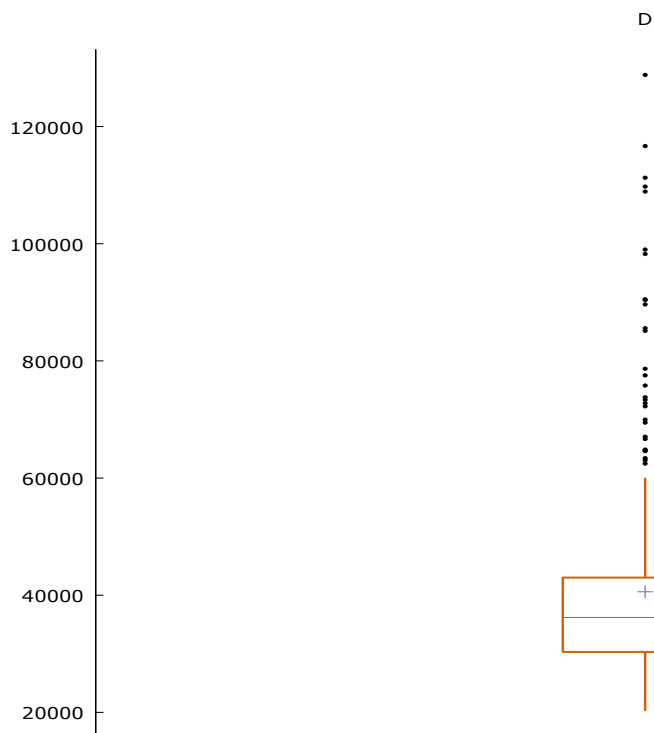


Рисунок 16 – Коробчатая диаграмма «Среднедушевые денежные доходы населения»

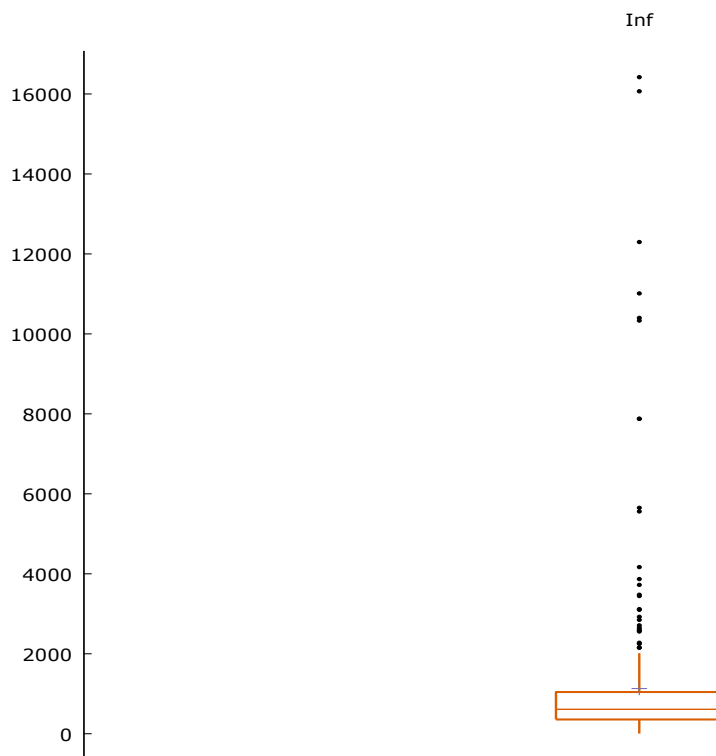


Рисунок 17 – Коробчатая диаграмма «Объем информации, переданной при доступе к сети Интернет, петабайт (фиксированный доступ+мобильный доступ)»

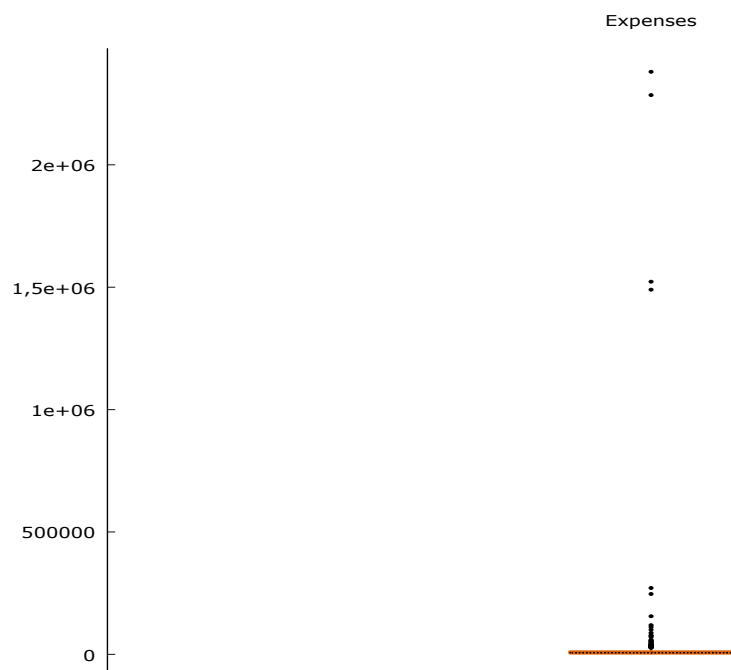


Рисунок 18 – Коробчатая диаграмма «Затраты на внедрение и использование цифровых технологий (млн. руб.)»

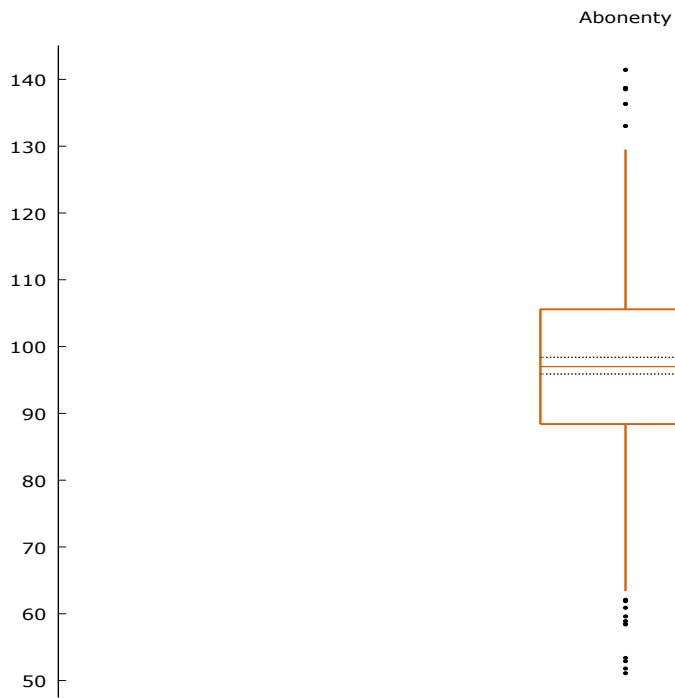


Рисунок 19 – Коробчатая диаграмма «Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения»

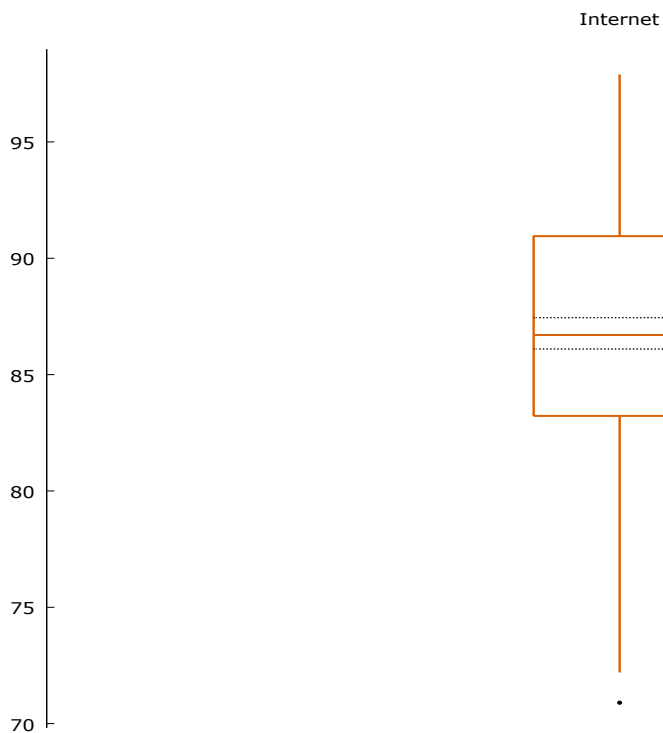


Рисунок 20 – Коробчатая диаграмма «Использование сети интернет населением»

Как мы видим из представленных коробчатых диаграмм выбросы присутствуют у каждого показателя, что говорит о неоднородности выборки. В целях уменьшения разброса в дальнейшем прологарифмируем данные, что сделает наше распределение более нормальным и более симметричным.

Сформируем описательную статистику для каждой переменной.

Таблица 5 – Описательная статистика, использованы наблюдения 1:1 – 74:4

Переменная	Среднее	Медиана	Минимум	Максимум
IB	14,850	13,255	2,0627	60,167
CG	6,9540	7,0000	5,1700	7,9600
D	40588,	36202,	20248,	1,2881e+005
Inf	1129,0	611,40	3,1000	16420,
Expenses	39663,	6676,2	216,80	2,3802e+006
Abonenty	97,210	97,000	51,100	141,43
Density	147,97	23,500	0,10000	5116,8
Internet	86,802	86,700	70,900	97,900
Переменная	Ст. откл.	Вариация	Асимметрия	Эксцесс
IB	8,6167	0,58025	1,9018	6,5212
CG	0,45530	0,065473	-0,93331	1,8562
D	16906,	0,41653	2,3535	6,6182
Inf	1984,2	1,7575	5,0848	29,801
Expenses	2,2729e+005	5,7305	8,8109	79,450
Abonenty	16,252	0,16719	-0,067828	0,83827
Density	722,51	4,8826	5,9614	34,179
Internet	5,2877	0,060916	-0,099185	-0,41357
Переменная	5% Проц.	95% Проц.	Межквартильный размах	Пропущенные набл.
IB	4,5975	28,385	9,5518	0
CG	6,2035	7,6215	0,56000	0
D	24708,	76056,	12683,	0
Inf	97,390	3448,5	687,08	0

Окончание таблицы 5

Переменная	5% Прог.	95% Прог.	Межквартильный размах	Пропущенные набл.
Expenses	951,79	60927,	9595,1	0
Abonenty	65,355	127,14	17,175	0
Density	0,70000	142,25	37,325	0
Internet	77,840	95,500	7,7250	0

Далее рассмотрим данные на нормальное распределение с помощью критерия Шапиро-Уилка. Он используется для проверки гипотезы о том, что набор данных имеет нормальное распределение. Результаты представлены в Таблице 6.

Таблица 6 – Тест Шапиро-Уилка

Показатель	Наименование переменной	Тест Шапиро-Уилка	P-значение
1. IB	Показатель информационной безопасности населения	0,864844	2,00652e-015
2. CG	Уровень цифровой грамотности населения	0,954337	5,51235e-008
3. D	Среднедушевые денежные доходы населения	0,760101	1,78098e-020
4. Inf	Объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме подвижных сетей)	0,43786	2,08332e-029
5. Expenses	Затраты на внедрение и использование цифровых технологий (млн. руб.)	0,135803	1,42779e-034
6. Abonenty	Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения	0,97638	8,40764e-005
7. Density	Плотность населения на 1 км ²	0,177437	5,88664e-034
8. Internet	Использование сети интернет населением	0,992459	0,139125

По результатам тестирования у значений выявлены ненормальные распределения, что свидетельствует о разнородности выборки, р-значение больше 0,05, распределение признается нормальным.

В целях приведения данных к нормальному распределению в дальнейшем прологарифмируем данные.

Далее проведем корреляционный анализ на наличие взаимосвязей зависимой переменной с независимыми.

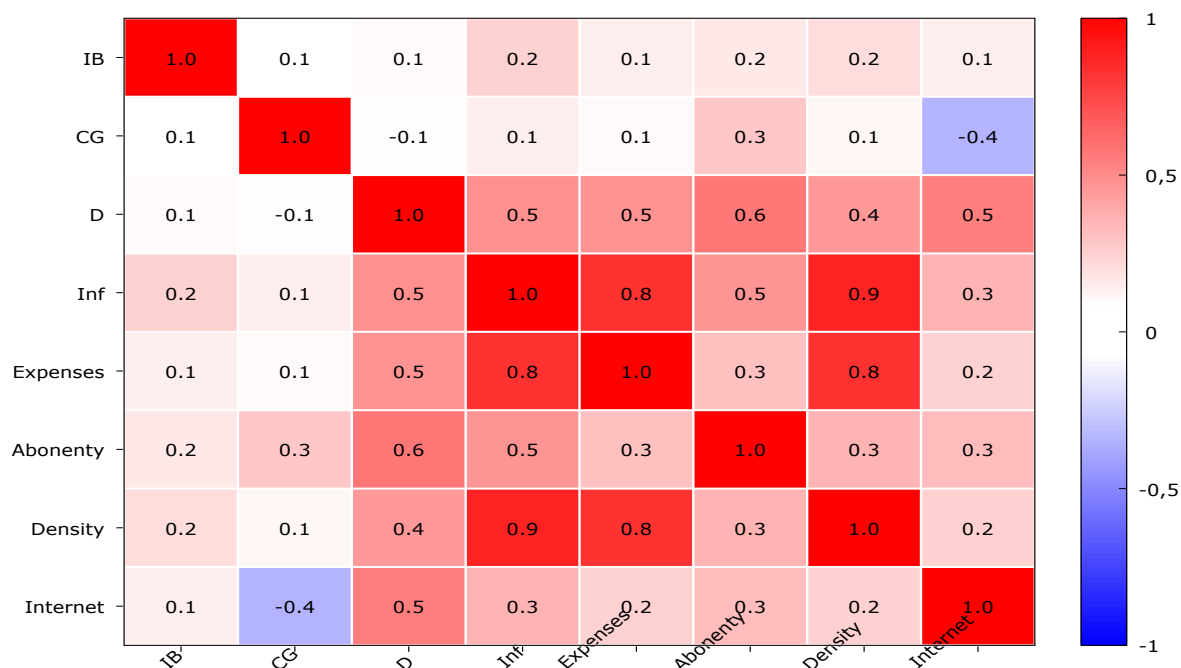


Рисунок 21 – Корреляционная матрица

Как мы видим из Рисунка 21 корреляция прослеживается между показателями:

1) (Inf) - объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме подвижных сетей) и (Density) - Плотность населения на 1 км²;

2) (Inf) - объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме

подвижных сетей) и (Expenses) затратами на внедрение и использование цифровых технологий (млн. руб.)

В свою очередь (Expenses) затраты на внедрение и использование цифровых технологий (млн. руб.) коррелируют с – Density плотность населения на 1 км².

Логарифмируем данные, с целью приведения их к нормальному распределению и повторно построим корреляционную матрицу.

Таблица 7 – Тест Шапиро-Уилка

Показатель	Наименование переменной	Тест Шапиро-Уилка	P-значение
1.1_IB	Показатель информационной безопасности населения	0,985611	0,00466191
2.1_CG	Уровень цифровой грамотности населения	0,926411	6,44681e-011
3.1_D	Среднедушевые денежные доходы населения	0,923663	3,64845e-011
4.1_Inf	Объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме подвижных сетей)	0,937309	7,13399e-010
5.1_Expenses	Затраты на внедрение и использование цифровых технологий (млн. руб.)	0,946213	6,23768e-009
6.1_Abonenty	Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения	0,944462	4,00498e-009
7.1_Density	Плотность населения на 1 км ²	0,930185	1,44188e-010
8.1_Internet	Использование сети интернет населением	0,989798	0,0364671

Построим корреляционную матрицу с учетом логарифмирования.

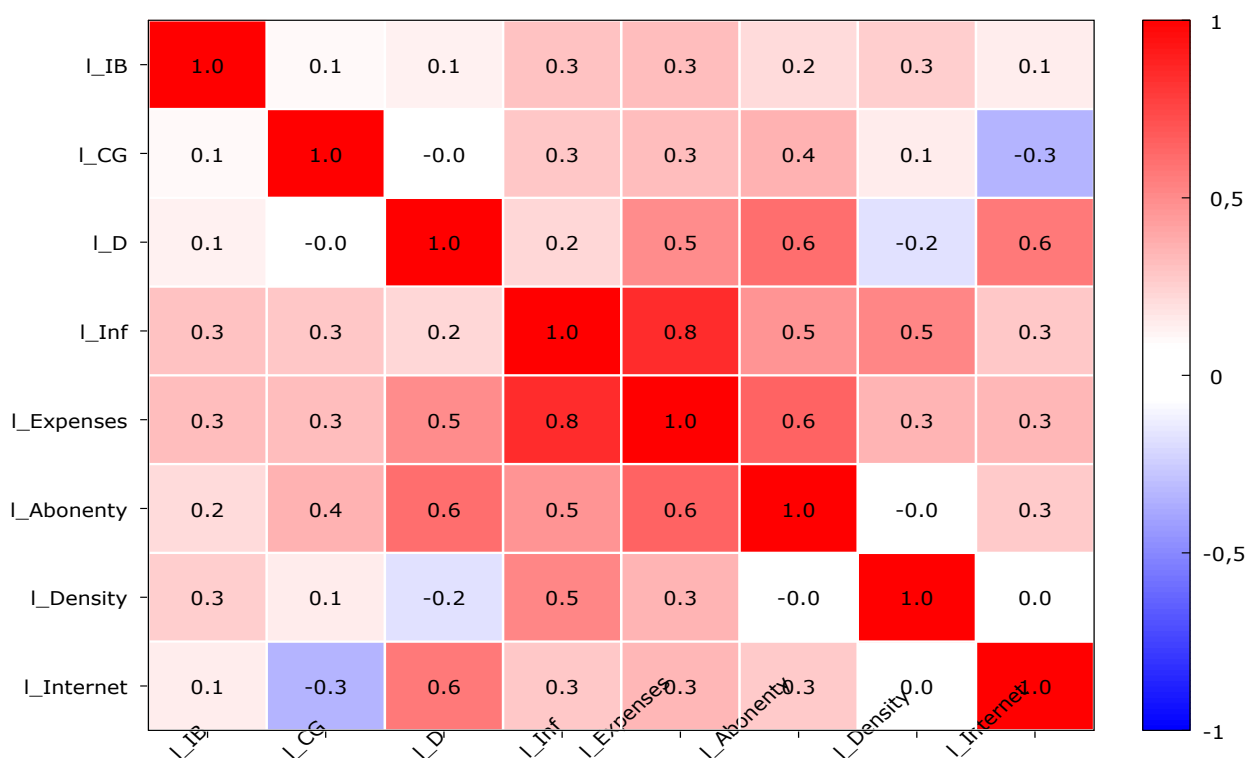


Рисунок 22 – Корреляционная матрица 2

После проведения стандартизации ярко-выраженная корреляция определена между показателями:

(Inf) - объем информации, переданной от/к абонентам сетей подвижной связи при доступе в Интернет (подвижные сети + кроме подвижных сетей) и (Expenses) - затратами на внедрение и использование цифровых технологий (млн. руб.) (0,8);

Также высокий уровень установлен при стандартизации данных между показателями (Density) - Плотность населения на 1 км² и (Expenses) - затратами на внедрение и использование цифровых технологий (млн. руб.) (0,8).

В связи с установленной корреляцией принято решение исключить показатели Inf и Density из модели.

Далее построим модель взвешенным методом наименьших квадратов.

Стоит отметить, что взвешенный метод наименьших квадратов – это метод регрессионного анализа, который учитывает неравные веса или гетероскедастичность ошибок. В обычном методе наименьших квадратов предполагается, что все наблюдения имеют одинаковый вес. Однако наши наблюдения имеют разную дисперсию и степень важности.

В качестве весов применяются оценки дисперсии ошибок для каждого наблюдения. Построим первую модель определив какие факторы оказывают статистически значимое влияние на показатель информационной безопасности населения. Всего используемых наблюдений 296, включено 74 пространственных объекта.

Таблица 8 – Модель 1

	Коэффициент	Ст. ошибка	t-статистика	p-значение	
const	2,12408	2,08631	1,018	0,3095	
I_CG	-0,485109	0,347099	-1,398	0,1633	
I_D	-0,191227	0,0839445	-2,278	0,0235	**
I_Expenses	0,122730	0,0175499	6,993	<0,0001	***
I_Abonenty	0,360413	0,148743	2,423	0,0160	**
I_Internet	0,151123	0,412767	0,3661	0,7145	

Таблица 9 – Статистика, полученная по взвешенным данным для Модели 1

Сумма кв. остатков	287,8765	Ст. ошибка модели	0,996332
R-квадрат	0,397528	Исправ. R-квадрат	0,387141
F(5, 290)	38,27009	P-значение (F)	4,17e-30
Лог. правдоподобие	-415,8873	Крит. Акаике	843,7745
Крит. Шварца	865,9167	Крит. Хеннана-Куинна	852,6398

Таблица 10 – Статистика, полученная по исходным данным для Модели 1

Среднее завис. перемен	2,543611	Ст. откл. завис. перемен	0,572769
Сумма кв. остатков	87,30190	Ст. ошибка модели	0,548672

Тест на избыточные переменные установил нулевую гипотезу:
параметры регрессии нулевые для переменной: $I_Internet$

Тестовая статистика: $F(1, 290) = 0,134045$

p -значение = $P(F(1, 290) > 0,134045) = 0,714541$

Это означает, что фактор «Использование сети интернет населением» не оказывает статистически значимого влияния на показатель информационной безопасности населения.

По результатам регрессионной модели построенной взвешенным методом наименьших квадратов определены факторы, которые оказывают статистически значимое влияние на зависимую переменную. К данным факторам относятся:

1. I_D – среднедушевые денежные доходы населения (p -значение 0,0235).
2. $I_Expenses$ – затраты на внедрение и использование цифровых технологий (млн. руб.) (p -значение $<0,0001$).
3. $I_Abonenty$ – численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения (p -значение 0,0160).

Отрицательный коэффициент у переменной I_CG – уровень цифровой грамотности населения говорит о том, что при увеличении уровня цифровой грамотности показатель информационной безопасности населения уменьшится, что является логичным заключением, чем большими компетенциями в области информатизации и связи будет обладать население, тем реже они будут сталкиваться с проблемами информационной безопасности.

Отрицательный коэффициент у переменной I_D – среднедушевые денежные доходы населения говорит о том, что при увеличении уровня денежных доходов показатель информационной безопасности населения

уменьшится, что также является логичным заключением и подтверждает выдвинутую гипотезу.

Положительные значения коэффициентов $I_Expenses$ – затраты на внедрение и использование цифровых технологий (млн. руб.), $I_Abonenty$ – численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения, $I_Internet$ – использование сети интернет населением, свидетельствуют о том, что дальнейшее развитие цифрового общества будет увеличивать показатель информационной безопасности населения, что является неутешительной тенденцией, требующей внимания.

R-квадрат установлен на уровне 0,4, это говорит о том, что модель факторы на 40% объясняют полученную модель, что является неплохим результатом.

Результаты теста на избыточные переменные указали на нулевые параметры регрессии для переменной $I_Internet$ – использование сети интернет населением. Исключим данную переменную из модели и построим новую.

Таблица 11 – Модель 2

	Коэффициент	Ст. ошибка	t-статистика	p-значение	
const	2,63813	1,01963	2,587	0,0102	**
I_CG	-0,540078	0,304420	-1,774	0,0771	*
I_D	-0,166388	0,0808652	-2,058	0,0405	**
$I_Expenses$	0,122310	0,0164899	7,417	<0,0001	***
$I_Abonenty$	0,362690	0,143134	2,534	0,0118	**

Таблица 12 – Статистика, полученная по взвешенным данным для Модели 2

Сумма кв. остатков	289,1113	Ст. ошибка модели	0,996750
R-квадрат	0,379088	Исправ. R-квадрат	0,370553

Продолжение таблицы 12

F(4, 291)	44,41641	P-значение (F)	4,32e-29
Лог. правдоподобие	-416,5207	Крит. Акаике	843,0415
Крит. Шварца	861,4933	Крит. Хеннана-Куинна	850,4292

Таблица 13 – Статистика, полученная по исходным данным для Модели 2

Среднее завис. перемен	2,543611	Ст. откл. завис. перемен	0,572769
Сумма кв. остатков	87,46522	Ст. ошибка модели	0,548241

При исключении переменной качество модели снижается незначительно R-квадрат 0,37. При исключении переменной I_Internet – использование сети интернет населением, статистически значимое принимает значение I_CG -уровень цифровой грамотности населения (p-значение - 0,0771).

Проведем тест на нормальность остатков.

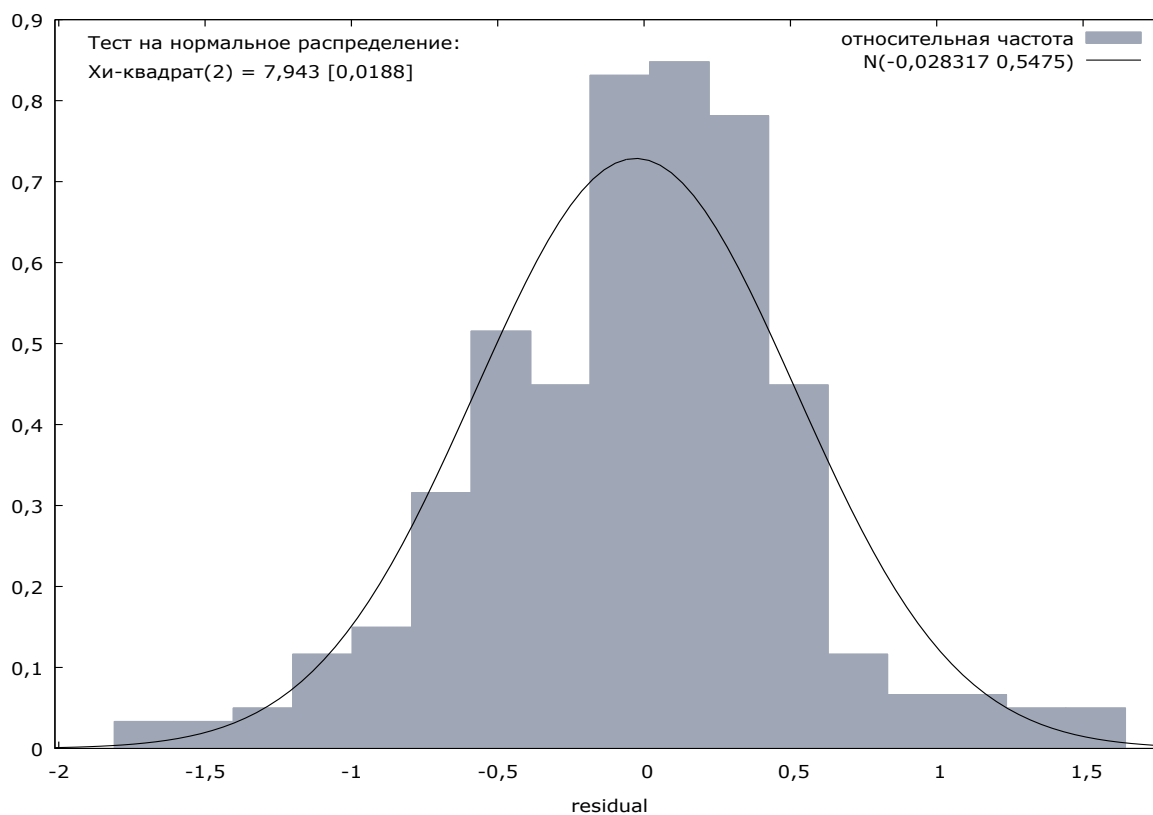


Рисунок 23 – Тест на нормальность остатков

Остатки имеют нормальное распределение, с незначительной правосторонней асимметрией.

Еще одним из способов визуализации нормального распределения остатков является построение графика квантилей нормального распределения.

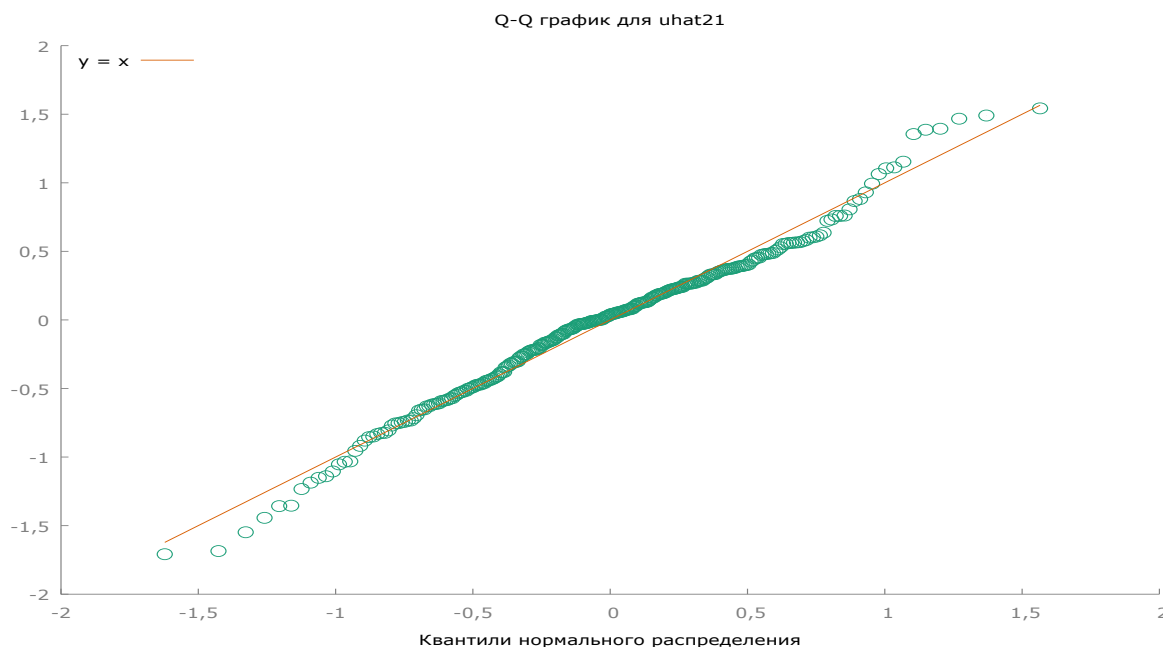


Рисунок 24 – Квантили нормального распределения

Представленный график на Рисунке 24 сравнивает эмпирические квантили остатков с теоретическими квантилями нормального распределения.

Точки на выше представленном графике располагаются вдоль прямой линии, что также свидетельствует о нормальном распределении остатков.

Проведем тест Песарана на зависимость поперечного сечения (Pesaran CD test). Нулевая гипотеза: Нет зависимости поперечного сечения

Асимптотическая тестовая статистика: $z = -0,73536$

p-значение = 0,46212

Результаты теста Песарана свидетельствуют об отсутствии статистически значимой кросс-секционной зависимости в данных, несмотря на умеренную степень корреляции между поперечными сечениями. Это означает, что в данных нет существенной взаимосвязи между регионами.

Исходя из полученных результатов корреляционно–регрессионная модель будет иметь вид, представленный в формуле 5.

$$y = 2,6 + (-0,54 I_{CG}) + (-0,17 I_D) + (0,12 I_{Expenses}) + (0,36 I_{Abonenty}), \quad (5)$$

Данное уравнение показывает, что показатель информационной безопасности будет равен 2,6, если все статистически значимые независимые переменные будут равны 0. При увеличении уровня цифровой грамотности населения на 1 единицу, показатель информационной безопасности населения снизится на 0,54 %. Это означает что население будет реже сталкиваться с проблемами информационной безопасности. Рост доходов населения также будет способствовать снижению показателя информационной безопасности населения, что является благоприятной тенденцией. С ростом затрат на внедрение и использование цифровых технологий (млн. руб.), а также численностью активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения показатель информационной безопасности будет увеличиваться, что будет снижать качество жизни населения.

Таким образом, проведенный в работе анализ позволил вывить важные факторы, влияющие на показатель информационной безопасности населения.

3 Направления повышения уровня информационной безопасности населения

3.1 Практическая значимость предложенной модели

Практическая значимость показателя информационной безопасности населения заключается в возможности его применения при оценке уровня защищенности граждан в информационной среде, анализа показателя в динамике, принятие решений в цифровой среде опираясь на полученные расчетные данные.

Одними из первоочередных целей развития Российской Федерации предусмотренных Указом Президента РФ № 309 От 07.05.2024 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» является:

- технологическое лидерство;
- цифровая трансформация государственного и муниципального управления, экономики и социальной сферы [48].

Показатели достижения вышеуказанных целей отражены в Таблице 14.

Таблица 14 – Показатели национальных целей развития

№ п/п	Технологическое лидерство	Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы
1	увеличение к 2030 году доли отечественных высокотехнологичных товаров и услуг, созданных на основе собственных линий разработки, в общем объеме потребления таких товаров и услуг в Российской Федерации в полтора раза по сравнению с уровнем 2023 года	достижение к 2030 году «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта
2	увеличение к 2030 году выручки малых технологических компаний не менее чем в семь раз по сравнению с уровнем 2023 года	формирование рынка данных, их активное вовлечение в хозяйственный оборот, хранение, обмен и защита
3		увеличение доли домохозяйств, которым обеспечена возможность качественного высокоскоростного широкополосного доступа к информационно-телекоммуникационной сети «Интернет», в том числе с использованием сетей (инфраструктуры) спутниковой и мобильной связи и с учетом роста пропускной способности магистральной инфраструктуры, до 97 процентов к 2030 году и до 99 процентов к 2036 году
4		обеспечение в 2025 - 2030 годах темпа роста инвестиций в отечественные решения в сфере информационных технологий вдвое выше темпа роста валового внутреннего продукта
5		переход к 2030 году не менее 80 процентов российских организаций ключевых отраслей экономики на использование базового и прикладного российского программного обеспечения в системах, обеспечивающих основные производственные и управленческие процессы

Окончание таблицы 14

№ п/п	Технологическое лидерство	Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы
6		увеличение к 2030 году до 95 процентов доли использования российского программного обеспечения в государственных органах, государственных корпорациях, государственных компаниях и хозяйственных обществах, в уставном капитале которых доля участия Российской Федерации в совокупности превышает 50 процентов, а также в их аффилированных юридических лицах
7		увеличение к 2030 году до 99 процентов доли предоставления массовых социально значимых государственных и муниципальных услуг в электронной форме, в том числе внедрение системы поддержки принятия решений в рамках предоставления не менее чем 100 массовых социально значимых государственных услуг в электронной форме в проактивном режиме или при непосредственном обращении заявителя, за счет внедрения в деятельность органов государственной власти единой цифровой платформы
8		формирование системы подбора, развития и ротации кадров для органов государственной власти и органов местного самоуправления на основе принципов равных возможностей, приоритета профессиональных знаний и квалификаций, включая механизмы регулярной оценки и обратной связи в рамках единой цифровой платформы
9		обеспечение к 2030 году повышения уровня удовлетворенности граждан качеством работы государственных и муниципальных служащих и работников организаций социальной сферы не менее чем на 50 процентов
10		создание системы эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, и снижения ущерба от их совершения
11		обеспечение сетевого суверенитета и информационной безопасности в информационно-телекоммуникационной сети «Интернет»

Как мы видим из Таблицы 14 первоочередной целью цифровой трансформации государственного и муниципального управления, экономики и социальной сферы является достижение к 2030 году «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, предполагающей автоматизацию большей части транзакций в рамках единых отраслевых цифровых платформ и модели управления на основе данных с учетом ускоренного внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта.

Расчет «цифровой зрелости» государственного и муниципального управления, ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования осуществляется в соответствии Приказом Минцифры России от 18.11.2020 № 600 «Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «Цифровая трансформация» (вместе с «Методикой расчета целевого показателя «Достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления», «Методикой расчета целевого показателя «Достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления» для субъекта Российской Федерации», «Методикой расчета целевого показателя «Увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95 процентов», «Методикой расчета показателя «Доля домохозяйств, которым обеспечена возможность широкополосного доступа к сети Интернет», «Методикой расчета целевого показателя «Увеличение вложений в отечественные решения в сфере информационных технологий», «Методикой расчета целевого показателя «Увеличение вложений

в отечественные решения в сфере информационных технологий» для субъекта Российской Федерации») [49].

В соответствии с данным приказом «цифровая зрелость» рассчитывается по пяти отраслям экономики:

- городское хозяйство и строительство,
- общественный транспорт,
- здравоохранение,
- образование (общее),
- государственное управление.

Алгоритм расчета показателя следующий:

$$ЦЗО = \frac{\sum_{i=1}^n И_{цзо_i}}{n}, \quad (5)$$

где ЦЗО – достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления (процентов);

$И_{цзо_i}$ – индекс, характеризующий «цифровую зрелость» i -ой отрасли из 5-ти отраслей экономики и социальной сферы:

- городское хозяйство и строительство,
- общественный транспорт,
- здравоохранение,
- образование (общее),
- государственное управление;
- n - количество отраслей ($n = 5$).

Перечень показателей, характеризующих достижение «цифровой зрелости» каждой из перечисленных отраслей представлен в Приложении А.

Методики расчета каждого из показателей, включая состав компонентов и источники данных, утверждаются президиумом Правительственной

комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности после согласования с профильными федеральными органами исполнительной власти по соответствующим отраслям.

Индекс, характеризующий «цифровую зрелость» отрасли, рассчитывается по формуле:

$$I_{цзо, i} = \frac{\sum_{j=1}^{k_i} x_{ij}}{k_i} * 100, \quad (6)$$

где $I_{цзо, i}$ – индекс, характеризующий «цифровую зрелость» i -ой отрасли из 5-ти отраслей экономики и социальной сферы (процентов);

x_{ij} – индекс, характеризующий отношение j -го показателя «цифровой зрелости» i -ой отрасли на конец отчетного месяца к целевому значению в 2030 году;

k_i – количество индексов «цифровой зрелости» i -ой отрасли, которые учитывались в расчете «цифровой зрелости» данной отрасли на конец отчетного периода.

$$x_{ij} = \frac{y_{ij}}{z_{ij}}, \quad (7),$$

где x_{ij} – индекс, характеризующий отношение j -го показателя «цифровой зрелости» i -ой отрасли на конец отчетного месяца к целевому значению в 2030 году;

y_{ij} – значение j -го показателя «цифровой зрелости» i -ой отрасли на конец отчетного месяца;

z_{ij} – значение j -го показателя «цифровой зрелости» i -ой отрасли в 2030 году (целевое значение).

В случае, если фактическое значение j -го показателя превышает целевое на 2030 год и $x_{ij} > 1$, для расчета индекса «цифровой зрелости» отрасли x_{ij} принимается равным 1 (единице).

Визуализируем применение показателя информационной безопасности населения при расчете «уровня цифровой зрелости» регионов.

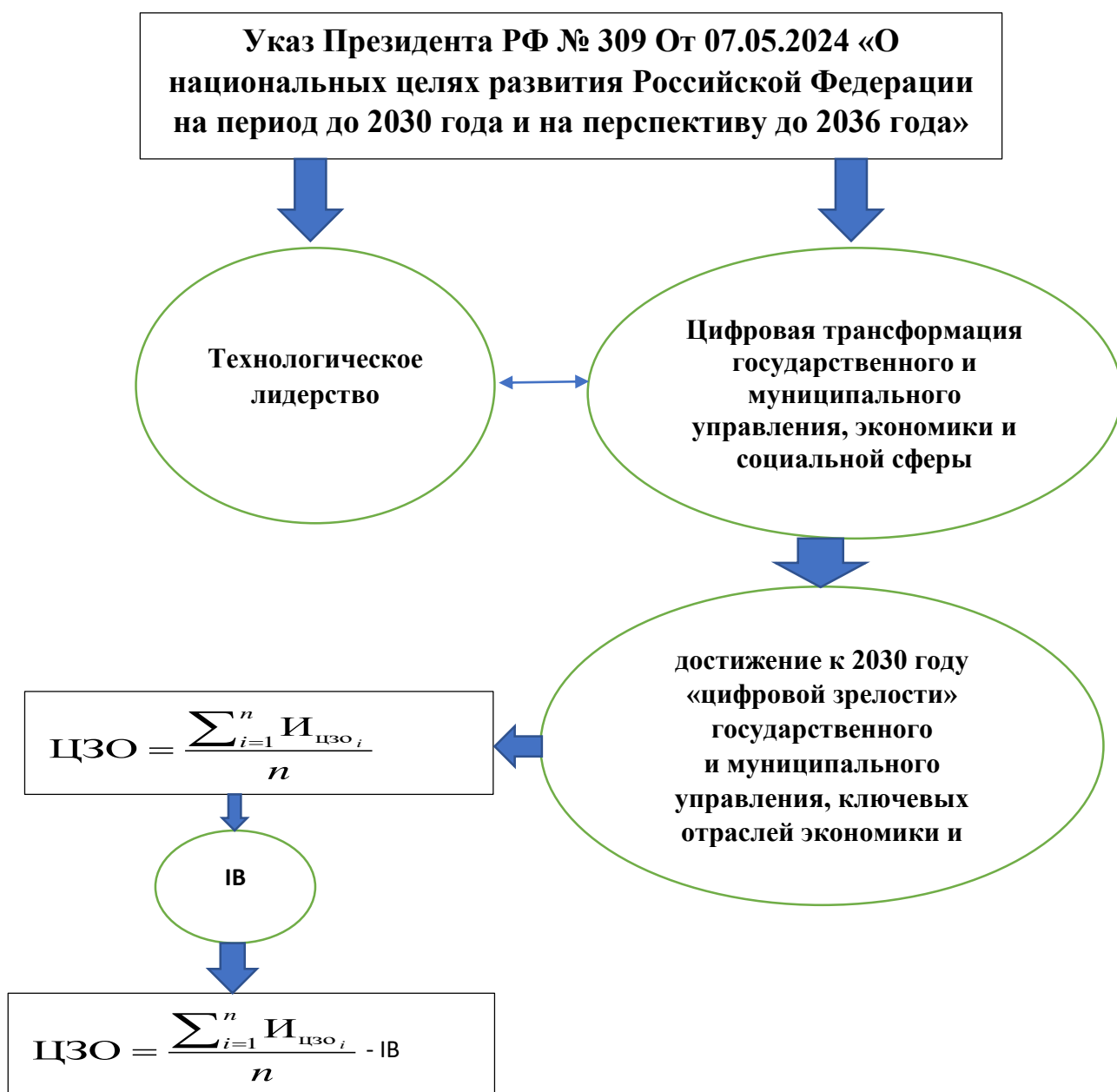


Рисунок 26 – Модель применения показателя информационной безопасности населения

3.2. Использование показателя информационной безопасности населения как индикатора в национальном проекте

Также достижению «цифровой зрелости» будет способствовать новый национальной проект «Экономика данных и цифровая трансформация государства» разработка которого предусмотрена Перечнем поручений по реализации Послания Президента Федеральному Собранию (утв. Президентом РФ 30.03.2024 № Пр-616) [50].

Основные направления предусматривают:

1. Финансирование в 2025 – 2030 годах реализации за счет бюджетных ассигнований федерального бюджета в размере не менее 700 млрд. рублей.

2. Включение в национальный проект мероприятий, обеспечивающих, в том числе:

темп роста в 2025 – 2030 годах инвестиций в отечественные решения в сфере информационных технологий вдвое выше темпа роста валового внутреннего продукта;

формирование к 2030 году цифровых платформ во всех ключевых отраслях экономики и социальной сферы, а также в сфере государственного управления;

поддержку компаний и стартапов, разрабатывающих и производящих оборудование для хранения и обработки данных, а также создающих программное обеспечение;

повышение доли предоставляемых массовых социально значимых государственных и муниципальных услуг в электронном виде в проактивном режиме с использованием в том числе технологий искусственного интеллекта в общем объеме таких услуг;

увеличение к 2030 году совокупной мощности отечественных суперкомпьютеров не менее чем в 10 раз;

возможность качественного высокоскоростного доступа к информационно-телекоммуникационной сети «Интернет» к 2030 году не менее 97 процентов домохозяйств, в том числе на основе сетей (инфраструктуры) спутниковой и мобильной связи.

Подводя итоги выделено два направления применения показателя информационной безопасности населения:

1. Предложение применения показателя информационной безопасности населения в качестве количественного результирующего показателя в новом национальном проекте «Экономика данных и цифровая трансформация государства».

2. Учет показателя информационной безопасности населения при расчете «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления.

ЗАКЛЮЧЕНИЕ

В эпоху становления информационного общества его квинтэссенцией становится информация и уровень ее применения. Ее доступность кардинальным образом влияет на экономические и социокультурные условия жизни граждан, стабильность функционирования определяется качеством информационно-технологических решений. Одновременно данный процесс имеет амбивалентный смысл: с одной стороны, устойчивое развитие общества невозможно без целенаправленной глобальной информатизации, а с другой, это приводит к повышению уязвимости населения перед информационным воздействием. Актуальность темы исследования определяется, в том числе, новизной самой проблемы информационной безопасности.

В магистерской диссертации выполнено научное обоснование и разработка рекомендаций по повышению информационной безопасности населения на основе анализа и оценки факторов, оказывающих на него влияние путем поэтапного решения задач, в том числе: проведен анализ нормативно-правовой базы и теоретических источников выделены подходы к определению информационной безопасности и факторы на нее влияющие, определена методическая основа расчета показателя, характеризующего информационную безопасность населения, на основе имеющихся статистических данных произведены расчеты, установлены статистически значимые зависимости между показателем информационной безопасности населения и независимыми переменными, на основе полученных данных разработаны практические рекомендации направленные на совершенствование политики в области информатизации и связи с целью повышения информационной безопасности населения.

По результатам корреляционно-регрессионного анализа:

Гипотеза 1. Уровень цифровой грамотности населения оказывает статистически значимое влияние на показатель информационной

безопасности населения подтвердилась, чем выше уровень цифровой грамотности населения, тем оно меньше подвержено угрозам информационном безопасности;

Гипотеза 2. Численность активных абонентов мобильного широкополосного доступа к сети Интернет на 100 человек населения оказывает статистически значимое влияние на показатель информационной безопасности населения, а также гипотеза 4 – затраты на внедрение и использование цифровых технологий оказывают статистически значимое влияние на показатель информационной безопасности населения подтвердилась, в процессе цифровизации общества, уровень столкновения с проблемами информационной безопасности будет увеличиваться;

Гипотеза 3. Уровень среднедушевых денежных доходов населения оказывает статистически значимое влияние на показатель информационной безопасности населения подтвердилась с ростом уровня доходов населения проблемы информационной безопасности буду затрагивать его в меньшей степени, что вполне логично.

По результатам была предложена модель применения показателя информационной безопасности населения, его уровень предложено учитывать при расчете «цифровой зрелости» регионов, что позволит отслеживать динамику данного показателя, а также будет способствовать принятию конкретных мероприятий, направленных для его снижения, а именно учете при количественной оценке мероприятий, установленных в разрабатываемом национальном проекте «Экономика данных и цифровая трансформация государств

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» = Information technology. Security techniques. Information security management systems. Overview and vocabulary : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 813-ст : введен впервые : дата введения 2013-12-01. – Москва : Стандартинформ, 2019.

2. Российская Федерация. Законы. Об участии в международном информационном обмене : Федеральный закон от 04.07.1996 № 85-ФЗ : (редакция от 29.06.2004) // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

3. Российская Федерация. Президент (Путин В. В.). Указы. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

4. Концепции информационной безопасности сетей связи общего пользования Российской Федерации : проект.

5. Цифровая экономика Российской Федерации : национальная программа : утверждена президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам : протокол от 04.06.2019 № 7 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

6. Обеспечение информационной безопасности / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: <https://digital.gov.ru/ru/activity/directions/466/> (дата обращения: 18.06.2024).

7. Российская Федерация. Правительство Российской Федерации. Распоряжения. Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации : Распоряжение Правительства РФ от 22.12.2022 № 4088-р // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

8. Российская Федерация. Президент (Путин В. В.). Указы. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ № 309 от 07.05.2024 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

9. Российская Федерация. Президент (Путин В. В.). Указы. О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы : Указ Президента РФ от 09.05.2017 № 203 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

10. Российская Федерация. Правительство Российской Федерации. Постановления. Об утверждении государственной программы Российской Федерации «Информационное общество» : Постановление Правительства РФ от 15.04.2014 № 313 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

11. Баринов, С. В. О правовом определении понятия «Информационная безопасность личности» / С. В. Баринов // Актуальные проблемы российского права. – 2016. – № 4 (65). – URL: <https://cyberleninka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti> (дата обращения: 17.06.2024).

12. Грачев, Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – Москва : Изд-во РАГС, 1998. – 125 с.

13. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для вузов / А. А. Малюк. – Москва : Горячая линия – Телеком, 2004. – 280 с.

14. Мазуров, В. А. Понятие и принципы информационной безопасности / В. А. Мазуров, В. В. Невинский // Известия АлтГУ. – 2003. – № 2. – URL: <https://cyberleninka.ru/article/n/ponyatie-i-printsipy-informatsionnoy-bezopasnosti> (дата обращения: 17.06.2024).

15. Еркин, А. В. Понятия «информация» и «информационная безопасность»: от индустриального общества к информационному / А. В. Еркин ; Волгоградская академия государственной службы // Информационное общество. – 2012. – Вып. 1. – С. 68–74. – URL: <http://emag.iis.ru/arc/infosoc/emag.nsf/BPC/14e84717e098226344257a13003bdeb2> (дата обращения: 18.06.2024).

16. Шавва А. И. Анализ подходов к определению понятия «информационная безопасность» в условиях глобализации / А. И. Шавва, Д. Е. Хаблов // Теория и практика современной науки. – 2018. – № 5 (35). – URL: <https://cyberleninka.ru/article/n/analiz-podhodov-k-opredeleniyu-ponyatiya-informatsionnaya-bezopasnost-v-usloviyah-globalizatsii> (дата обращения: 17.06.2024).

17. Золотар, О. А. Информационная безопасность человека: доктринальные подходы к определению категории / О. А. Золотар // SCI-ARTICLE. – 2017. – № 52. – URL: <https://sci-article.ru/stat.php?i=1513689444> (дата обращения: 18.06.2024).

18. Тер-Акопов, А. А. Безопасность человека: Теоретические основы социально-правовой концепции / А. А. Тер-Акопов. – Москва : Изд-во МНЭПУ, 1998. – 196 с.

19. Орлова, А. А. Систематизация подходов к пониманию информационной безопасности / А. А. Орлова, А. С. Бакун. – URL: https://elib.bsu.by/bitstream/123456789/294028/1/orlova_sbornik29.pdf (дата обращения: 18.06.2024).

20. Королёв, Ю. А. Теоретические подходы в исследовании информационной безопасности / Ю. А. Королёв // Информационная безопасность регионов. – 2011. – № 1. – URL: <https://cyberleninka.ru/article/n/teoreticheskie-podhody-v-issledovanii-informatsionnoy-bezopasnosti> (дата обращения: 17.06.2024).

21. Мороз, Н. О. Подходы к определению термина «информационная безопасность» в контексте международного сотрудничества / Н. О. Мороз // Право.by. – 2021. – № 4 (72). – С. 120–126.

22. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. – URL: <http://www.scrf.gov.ru/security/information/document155/> (дата обращения: 18.06.2024).

23. Брумштейн, Ю. М. Комплексный анализ факторов информационной и интеллектуальной безопасности регионов / Ю. М. Брумштейн, А. Н. Подгорный // Информационная безопасность регионов. – 2011. – № 1. – URL: <https://cyberleninka.ru/article/n/kompleksnyy-analiz-faktorov-informatsionnoy-i-intellektualnoy-bezopasnosti-regionov> (дата обращения: 29.03.2024).

24. Брумштейн, Ю. М. Информационная безопасность региона: анализ содержания термина, моделей оценки и некоторых вопросов управления / Ю. М. Брумштейн, А. Н. Подгорный // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2011. – № 1. – URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-regiona-analiz-soderzhaniya-termi-na-modeley-otsenki-i-nekotoryh-voprosov-upravleniya> (дата обращения: 16.04.2024).

25. Зефирова, С. Л. Способы оценки информационной безопасности организации / С. Л. Зефирова, В. М. Алексеев // НиКа. – 2011. – URL: <https://cyberleninka.ru/article/n/sposoby-otsenki-informatsionnoy-bezopasnosti-organizatsii> (дата обращения: 16.06.2024).

26. Козачок, В. И. Факторы определяющие информационную безопасность корпорации / В. И. Козачок, С. А. Власова // Среднерусский вестник общественных наук. – 2014. – № 5 (35). – URL: <https://cyberleninka.ru/article/n/factory->

opredelyayuschie-informatsionnyu-bezopasnost-korporatsii (дата обращения: 29.03.2024).

27. Модели оценки защищённости данных в информационно-управляющих системах реального времени / Д. А. Миков, Т. И. Булдакова, В. В. Сюзев [и др.] // Проблемы современной науки и образования. – 2019. – № 11-1 (144). – С. 15–20.

28. Шепелёва, О. Ю. Оценка информационной безопасности предприятия как составная часть стратегического корпоративного управления / О. Ю. Шепелева, П. Ю. Шепелев, С. М. Газуль // Правовая информатика. – 2020. – № 4. – URL: <https://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-predpriyatiya-kak-sostavnaya-chast-strategicheskogo-korporativnogo-upravleniya> (дата обращения: 16.06.2024).

29. Самохвалов, Ю. Я. Оценка информационной безопасности организации по критерию уверенности / Ю. Я. Самохвалов, Н. Н. Браиловский // Захист інформації. – 2019. – Т. 21, № 1. – С. 13-24.

30. Барыбина, А. З. Оценка состояния информационной безопасности как процесса / А. З. Барыбина // Вестник Академии знаний. – 2023. – № 6 (59). – URL: <https://cyberleninka.ru/article/n/otsenka-sostoyaniya-informatsionnoy-bezopasnosti-kak-protsessa> (дата обращения: 16.06.2024).

31. Огютчу, Г. Анализ поведения и осведомленности в области личной информационной безопасности / Г. Огютчу, О. М. Тестик, О. Чусейноглу // Вычислительная безопасность. – 2016. – № 56. – С. 83–93.

32. Ли, Д. Распределение внутренних ресурсов для информационной безопасности умных городов с использованием модели эволюционной игры / Д. Ли, К. Цзоу, Л. Син // Дискретная динамика в природе и обществе. – 2022. – URL: <https://doi.org/10.1155/2022/6932163> (дата обращения: 18.06.2024).

33. Венди, Ю. Показатели проверки безопасности для партнерств по обмену информацией / Ю. Венди, А.З. Коллиер, Ш. Текди // Анализ рисков. – 2024. – URL: <https://doi.org/10.1111/risa.14267> (дата обращения: 18.06.2024).

34. Васильева, М. М. Становление информационного общества в России в условиях глобального информационного пространства / М. М. Васильева // Вестник Московского государственного лингвистического университета. Общественные науки. – 2020. – № 3 (840). – URL: <https://cyberleninka.ru/article/n/stanovlenie-informatsionnogo-obschestva-v-rossii-v-usloviyah-globalnogo-informatsionnogo-prostranstva> (дата обращения: 10.06.2024).

35. Стукаленко, Е. А. Риски цифровизации жизни населения и пути их снижения / Е. А. Стукаленко // Идеи и идеалы. – 2021. – № 4-1. – URL: <https://cyberleninka.ru/article/n/riski-tsifrovizatsii-zhizni-naseleniya-i-puti-ih-snizheniya> (дата обращения: 10.06.2024).

36. Росстат / Федеральная служба государственной статистики [сайт]. – URL: <https://rosstat.gov.ru/> (дата обращения: 18.06.2024).

37. Цифровой диктант 2023. – URL: <https://digitaldictation.ru/> (дата обращения: 18.06.2024).

38. Среднедушевые денежные доходы населения // ЕМИСС : государственная статистика. – URL: <https://www.fedstat.ru/indicator/57039> (дата обращения: 18.06.2024).

39. Севрюкова, С. В. Формирование денежных доходов населения как социально-экономический аспект регулирования уровня жизни / С. В. Севрюкова, О. Н. Коростелева // Концепт : научно-методический электронный журнал. – 2017. – № 11. – С. 151–155.

40. Рогачёва, О. А. Среднедушевые денежные доходы населения: сопоставление по разным источникам / О. А. Рогачева // Journal of new economy. – 2011. – № 4 (36). – URL: <https://cyberleninka.ru/article/n/srednedushevye-denezhnye-dohody-naseleniya-sopostavlenie-po-raznym-istochnikam> (дата обращения: 15.06.2024).

41. Волкова, Н. Н. Рейтинг научно-технологического развития субъектов российской федерации / Н. Н. Волкова, Э. И. Романюк // Вестник Института экономики Российской академии наук. – 2023. – № 2. – URL:

<https://cyberleninka.ru/article/n/rejting-nauchno-tehnologicheskogo-razvitiya-subektov-rossiyskoj-federatsii> (дата обращения: 15.06.2024).

42. Регионы России. Социально-экономические показатели. 2023 : статистический сборник / Росстат. – Москва, 2023. – 914 с.

43. Об утверждении форм федерального статистического наблюдения для организации федерального статистического наблюдения за деятельностью в сфере образования, науки, инноваций и информационных технологий : Приказ Росстата от 30.07.2021 № 463 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

44. Волкова, Н. Н. Рейтинг научно-технологического развития субъектов российской федерации / Н. Н. Волкова, Э. И. Романюк // Вестник Института экономики Российской академии наук. – 2023. – № 2. – URL: <https://cyberleninka.ru/article/n/rejting-nauchno-tehnologicheskogo-razvitiya-subektov-rossiyskoj-federatsii> (дата обращения: 15.06.2024).

45. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации. – URL: <http://www.scrf.gov.ru/security/information/document155/> (дата обращения: 18.06.2024).

46. Российская Федерация. Правительство Красноярского края. Постановления. Об утверждении государственной программы Красноярского края «Развитие информационного общества» : Постановление Правительства Красноярского края от 30.09.2013 № 504-п : (редакция от 23.04.2024) // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

47. Устранение цифрового неравенства: федеральный проект.

48. Российская Федерация. Президент (Путин В. В.). Указы. О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года: Указ Президента РФ № 309 От 07.05.2024 // Консультант плюс : справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

49. Об утверждении методик расчета целевых показателей национальной цели развития Российской Федерации «Цифровая трансформация»: Приказ Минцифры России от 18.11.2020 № 600 // Консультант плюс: справочная правовая система. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

50. Экономика данных и цифровая трансформация государства: национальной проект // Консультант плюс: справочная правовая система. – Перечень поручений по реализации послания президента федеральному собранию: утвержден Президентом РФ 30.03.2024 № Пр-616. – Ст. 8. – URL: <http://www.consultant.ru> (дата обращения: 18.06.2024).

ПРИЛОЖЕНИЕ А

Состав показателей, входящих в оценку уровня «цифровой зрелости» отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления на уровне субъекта российской федерации

I. «Городское хозяйство и строительство»

№	Наименование показателя	Целевое значение на 2030 год
1	Доля общих собраний собственников помещений в многоквартирных домах, проведенных посредством электронного голосования, от общего количества проведенных общих собраний собственников	80%
2	Доля услуг по управлению многоквартирным домом и содержанию общего имущества, оплаченных онлайн	80%
3	Доля коммунальных услуг, оплаченных онлайн	80%
4	Доля управляющих организаций, раскрывающих информацию в полном объеме в государственную информационную систему жилищно-коммунального хозяйства	100%
5	Доля ресурсоснабжающих организаций, раскрывающих информацию в полном объеме в государственную информационную систему жилищно-коммунального хозяйства	100%
6	Доля диспетчерских служб муниципальных районов и городских округов, подключенных к системам мониторинга инцидентов и аварий на объектах жилищно-коммунального хозяйства	100%
7	Доля аварийного жилого фонда, внесенного в цифровой реестр аварийного жилья	100%
8	Доля жителей городов в возрасте старше 14 лет, зарегистрированных на специализированных информационных ресурсах по вопросам городского развития	80%

II. «Общественный транспорт»

№	Наименование показателя	Целевое значение на 2030 год
1	Доля автобусов, осуществляющих регулярные перевозки пассажиров в городском, пригородном и междугородном (в пределах субъекта Российской Федерации) сообщении, оснащенных системами безналичной оплаты проезда	100%
2	Доля автобусов, осуществляющих регулярные перевозки пассажиров в городском, пригородном и междугородном (в пределах субъекта Российской Федерации) сообщении, для которых обеспечена в открытом доступе информация об их реальном движении по маршруту	100%
3	Доля автобусов, осуществляющих регулярные перевозки пассажиров в городском, пригородном и междугородном (в пределах субъекта Российской Федерации) сообщении, оснащенных системами видеонаблюдения салонов (с функцией записи), соответствующих требованиям о защите персональных данных	100%

III. «Здравоохранение»

№	Наименование показателя	Целевое значение на 2030 год
1	Доля записей на прием к врачу, совершенных гражданами дистанционно	70%
2	Доля граждан, являющихся пользователями Единого портала государственных и муниципальных услуг (функций), которым доступны электронные медицинские документы в Личном кабинете пациента "Мое здоровье" по факту оказания медицинской помощи <*>	100%
3	Доля граждан, находящихся под диспансерным наблюдением, для которых обеспечен дистанционный мониторинг состояния	50%

	здоровья, в том числе с использованием Единого портала государственных и муниципальных услуг (функций)	
4	Доля медицинских организаций, осуществляющих централизованную обработку и хранение в электронном виде результатов диагностических исследований	50%
5	Доля консультаций, проводимых врачом с пациентом, в том числе на Едином портале государственных и муниципальных услуг (функций), с использованием видео-конференц-связи	50%
6	Доля граждан, которым доступны врачебные назначения (рецепты) в форме электронного документа в том числе на Едином портале государственных и муниципальных услуг (функций)	80%
7	Доля станций (отделений) скорой медицинской помощи, подключенных к централизованной системе (подсистеме) "Управление системой оказания скорой медицинской помощи и медицинской эвакуацией (в том числе санитарно-авиационной) в повседневном режиме и в режиме чрезвычайной ситуации" государственных информационных систем в сфере здравоохранения субъектов Российской Федерации	100%
8	Число граждан, воспользовавшихся услугами (сервисами) в Личном кабинете пациента "Мое здоровье" на Едином портале государственных услуг и функций	<*>
9	Доля медицинских организаций государственной и муниципальной систем здравоохранения, использующих медицинские информационные системы для организации и оказания медицинской помощи гражданам, обеспечивающих информационное взаимодействие с ЕГИСЗ	100%
10	Доля случаев оказания медицинской помощи, по которым предоставлены электронные медицинские документы в подсистемы ЕГИСЗ	100%
11	Доля медицинских организаций государственной и муниципальной систем здравоохранения, подключенных к централизованным подсистемам государственных информационных систем в сфере здравоохранения субъектов Российской Федерации	100%

<*> Значение определено индивидуально для каждого субъекта Российской Федерации в соответствии с федеральным проектом "Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)" национального проекта "Здравоохранение".

IV. «Образование (общее)»

№	Наименование показателя	Целевое значение на 2030 год
1	Доля учащихся, по которым осуществляется ведение цифрового профиля	100%
2	Доля учащихся, которым предложены рекомендации по повышению качества обучения и формированию индивидуальных траекторий с использованием данных цифрового портфолио учащегося	80%
3	Доля педагогических работников, получивших возможность использования верифицированного цифрового образовательного контента и цифровых образовательных сервисов	100%
4	Доля учащихся, имеющих возможность бесплатного доступа к верифицированному цифровому образовательному контенту и сервисам для самостоятельной подготовки	100%
5	Доля заданий в электронной форме для учащихся, проверяемых с использованием технологий автоматизированной проверки	70%

V. «Государственное управление»

№	Наименование показателя	Целевое значение на 2030 год
1	Доля зарегистрированных пользователей ЕПГУ, использующих сервисы ЕПГУ в текущем году в целях получения	65%

	государственных и муниципальных услуг в электронном виде, от общего числа зарегистрированных пользователей ЕПГУ	
2	Доля электронного юридически значимого документооборота между органами исполнительной власти, местного самоуправления и подведомственными им учреждениями в субъекте Российской Федерации	100%
3	Количество видов сведений, представляемых в режиме онлайн органами государственной власти в рамках межведомственного взаимодействия при предоставлении государственных услуг и исполнении функций, в том числе коммерческим организациям, в соответствии с законодательством	6 у.е.
4	Доля органов государственной власти, использующих государственные облачные сервисы и инфраструктуру	100%
5	Доля проверок в рамках контрольно-надзорной деятельности, проведенных дистанционно, в том числе с использованием чек-листов в электронном виде	85%
6	Количество государственных услуг, предоставляемых органами государственной власти в реестровой модели и (или) в проактивном режиме с предоставлением результата в электронном виде на Едином портале государственных и муниципальных услуг (функций)	95 <*> у.е.
7	Уровень удовлетворенности качеством предоставления массовых социально значимых государственных и муниципальных услуг в электронном виде с использованием Единого портала государственных и муниципальных услуг (функций)	4,7 баллы
8	Доля обращений за получением массовых социально значимых государственных и муниципальных услуг в электронном виде с использованием Единого портала государственных и муниципальных услуг (функций), без необходимости личного посещения органов государственной власти, органов местного самоуправления и многофункциональных центров предоставления государственных и муниципальных услуг, в общем количестве таких услуг	80%
9	Доля массовых социально значимых государственных и муниципальных услуг, доступных в электронном виде, предоставляемых с использованием Единого портала	95%


	государственных и муниципальных услуг (функций), в общем количестве таких услуг, предоставляемых в электронном виде	
10	Количество реализованных на базе единой платформы сервисов обеспечения функций органов государственной власти и органов местного самоуправления, в том числе типовых функций	95 штук
11	Доля расходов на закупки и/или аренду отечественного программного обеспечения и платформ от общих расходов на закупку или аренду программного обеспечения	85%

<*> Если установленное целевое значение показателя больше, чем 95% от количества услуг в Региональном перечне МСЗУ субъекта Российской Федерации, целевое значение показателя на 2030 год приравнивается к 95% от количества услуг в Региональном перечне МСЗУ субъекта Российской Федерации (с округлением до целого числа в меньшую сторону).

Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, государственного управления и финансов
Базовая кафедра цифровых финансовых технологий Сбербанка России

УТВЕРЖДАЮ
Заведующий кафедрой


 Д. В. Солнцев
подпись
« 18 » июня 2024 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

ИССЛЕДОВАНИЕ ФАКТОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
НАСЕЛЕНИЯ

38.04.01 «Экономика»
(код и наименование направления)

38.04.01.17 «Финансово-экономическая аналитика и принятие решений в
цифровой среде»
код и наименование магистерской программы

Научный
руководитель  18.06.24 доцент, к.э.н.

Ю.И. Черкасова

Выпускник  18.06.2024 г.

К.А. Болдырь

Рецензент  доцент, к.э.н.

В.М. Грязнов

Нормоконтролер  18.06.2024 г.

Э.Ф. Мамедова

Красноярск 2024