

УДК 364-7:004.9

**СТРАТЕГИИ УПРАВЛЕНИЯ СОЦИАЛЬНОЙ ЗАЩИТОЙ
В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ОПЫТ И СПЕЦИФИКА ДНР****Ромодан Ю.О.,**ФГБОУ ВО «Донецкая Академия Управления И Государственной Службы», Донецк,
email: juliaromodan@gmail.com

Аннотация. В статье исследуется процесс интеграции органов социальной защиты Донецкой Народной Республики (ДНР) и системы государственного управления Российской Федерации с акцентом на вызовы, связанные с необходимостью внедрения цифровых технологий и автоматизации процессов в сфере социальной защиты. Рассматривается влияние цифровизации на ускоренную модернизацию работы социальных служб, с особым вниманием к преодолению временных отставаний в области обработки и управления данными. Подчеркивается важность приведения работы социальных учреждений к федеральным стандартам, что требует не только усовершенствования технологий, но и адаптации персонала к новым условиям. Обсуждаются проблемы, возникающие в связи с ростом объемов информации, необходимостью эффективного взаимодействия с различными государственными и общественными органами, а также улучшением качества обслуживания населения. Также акцентируется внимание на важности правильного подхода к обучению и подготовке работников социальной сферы для успешного внедрения и освоения новых цифровых инструментов.

Ключевые слова: сфера социальной защиты, цифровая трансформация, стратегия управления.

**STRATEGIES FOR MANAGING SOCIAL PROTECTION IN THE CONTEXT
OF DIGITALIZATION: EXPERIENCE AND SPECIFICITY OF THE DPR****Romodan Y.O.,**Donetsk Academy of Management and Public Service, Donetsk,
email: juliaromodan@gmail.com

Abstract. The article examines the process of integration of social protection bodies of the Donetsk People's Republic (DPR) into the public administration system of the Russian Federation, with an emphasis on the challenges associated with the need to introduce digital technologies and automate processes in the field of social protection. The impact of digitalization on the accelerated modernization of social services is considered, with particular attention to overcoming time lags in data processing and management. The importance of bringing the work of social institutions to federal standards is emphasized, which requires not only improving technologies, but also adapting personnel to new conditions. The problems arising from the growth of information volumes, the need for effective interaction with various state and public bodies, as well as improving the quality of public service are discussed. Attention is also focused on the importance of the right approach to training and preparing social workers for the successful implementation and mastering of new digital tools.

Keywords: social protection sector, digital transformation, management strategy.

Система социальной защиты играет ключевую роль в обеспечении стабильности и развития общества, особенно в периоды кризисов и трансформаций. В послед-

ние десятилетия социальная защита стала неотъемлемым элементом государственной политики, направленной на борьбу с бедностью, неравенством и уязвимостью населения. Она выполняет не только роль временной поддержки, но и создает условия для устойчивого повышения качества жизни граждан, стимулируя их активное участие в экономической и социальной жизни страны. Этот комплекс мер приобретает особую значимость в условиях глобальных изменений, таких как цифровизация и автоматизация общественных процессов.

Цифровизация сегодня выступает основным направлением развития государственных систем и структур, в том числе, в сфере социальной защиты. Ее внедрение призвано повысить доступность, оперативность и прозрачность предоставления социальных услуг, минимизировать бюрократические барьеры, а также улучшить взаимодействие между гражданами и государством. Однако реализация данных задач в регионах, сталкивающихся с вызовами инфраструктурного и социального характера, таких как ДНР, требует особого подхода. Интеграция органов государственной власти ДНР и единой системы Российской Федерации создало дополнительные сложности, связанные с необходимостью модернизации существующих структур, внедрения федеральных стандартов и адаптации работников социальной сферы к новым условиям.

Особенность региона заключается в сложных экономических и социальных реалиях, где система социальной защиты не только выполняет свою традиционную функцию поддержки, но и становится инструментом обеспечения стабильности в условиях кризисных ситуаций. На этом фоне исследование механизмов эффективного управления и адаптации системы социальной защиты ДНР к современным вызовам приобретает исключительную важность.

Главная цель органов социальной защиты заключается не только в предоставлении временной помощи, но и в создании условий для устойчивого улучшения качества жизни граждан [6].

Цель исследования

Цель исследования заключается в разработке эффективных стратегий управления и адаптации системы социальной защиты ДНР к условиям цифровизации, акцентируя внимание на повышении ее эффективности через внедрение инновационных методов управления и совершенствование работы с персоналом. В работе также рассматриваются современные подходы к управлению в государственной службе, предложенные разными исследователями в этой области [2-4].

Материал и методы исследования

В 2017 году правительство России утвердило программу «Цифровая экономика» [1]. На первом этапе её реализации основной задачей стало создание условий для формирования новой основы управления государственными процессами с акцентом на цифровизацию. В долгосрочной перспективе создание цифровой экономики должно обеспечить более эффективный переход всех сфер жизни к новым технологиям, способствующим укреплению независимости и конкурентоспособности экономики в условиях глобальных вызовов.

Интеграция государственной службы ДНР и структуры государственной власти РФ состоялась лишь спустя четыре года, что стало серьезным испытанием для системы управления. Этот процесс потребовал срочного преодоления цифрового

разрыва, особенно в сфере социальной защиты, которая охватывает широкий круг граждан. Возникла необходимость пересмотра устоявшихся методов работы и их приведения в соответствие с современными цифровыми технологиями и новыми стандартами предоставления государственных услуг.

Ключевую часть пользователей услуг социальной защиты составляют пожилые люди и граждане с ограниченными возможностями здоровья. Эти категории населения требуют особого подхода, так как процесс освоения современных технологий для них представляет значительные трудности. Проблемы с использованием электронных сервисов и онлайн-форм существенно замедляют доступ к необходимым услугам и снижают эффективность работы всей системы социальной помощи. Кроме того, низкая цифровая подготовленность, как среди граждан, так и среди сотрудников усложняет внедрение новых технологий и затрудняет контроль за реализацией социальных программ.

Сложившаяся ситуация привела к увеличению нагрузки на систему, что потребовало не только обучения населения основам работы с цифровыми платформами, но и повышения квалификации сотрудников социальной защиты. Их подготовка к использованию новых технологических решений и взаимодействию с другими цифровизированными государственными структурами стала важной задачей на пути повышения эффективности и модернизации социальной службы. Согласно исследованию компании McKinsey & Company, к 2036 году до 50% рабочих процессов будет автоматизировано [2], что подтверждает глобальную тенденцию к цифровизации и автоматизации административных процессов.

В связи с этим необходимо адаптировать существующие управленческие системы в организациях, включая их ключевые функции, чтобы эффективно интегрировать новые технологии. В других регионах России и в зарубежных странах процесс цифрового перехода был начат значительно раньше, и стоит учесть их опыт в адаптации работников к цифровым изменениям.

Цифровизация становится важным инструментом для продолжения выполнения функций социальной защиты, особенно в условиях кризиса, когда необходимо обеспечивать удалённый доступ к услугам. Благодаря этому, государственные учреждения становятся более гибкими и устойчивыми в условиях современных вызовов.

Однако не стоит забывать о людях, формирующих кадровый состав предприятий социальной сферы. Помимо всех тех жизненных проблем, с которыми сталкивались граждане Республики на протяжении последних 10 лет, персонал сферы социальной защиты населения претерпевает сейчас дополнительную нагрузку, вызванную необходимостью полного изменения своего привычного рабочего уклада в связи с цифровой трансформацией его сферы деятельности.

Для того чтобы подчеркнуть значимость работы сотрудников, необходимо регулярное признание достигнутых результатов. Это может быть выражено через публичную оценку успехов или символическое поощрение, что особенно актуально в контексте внедрения новых технологий. Регулярная оценка их работы помогает поддерживать интерес к процессу изменений и способствует интеграции новых подходов в организацию.

Примером подобного подхода является проект «Герои среди нас» [5], который был инициирован в ДНР. Этот проект позволяет публично освещать трудовые подвиги работников бюджетных организаций, в частности сотрудников социальной сферы, которые, несмотря на сложные условия, продолжают выполнять свою

миссию. Признание их труда на широком уровне помогает общественности оценить значимость их работы в условиях кризиса.

Проект включает размещение серии плакатов, рассказывающих о трудовых подвигах работников, несмотря на все трудности, с которыми им приходится сталкиваться. Такие инициативы помогают общественности осознать ценность работы этих людей и привлекают внимание к их вкладу в общественное благо.

Подобные инициативы также могут быть важным элементом внутренней корпоративной культуры. Они создают атмосферу признания и уважения к труду сотрудников, что способствует улучшению взаимодействия внутри организации и с внешними партнерами.

Одной из важнейших стратегий управления является создание возможностей для карьерного роста внутри организации. В государственных учреждениях, где нет частных владельцев, сотрудники имеют шанс на продвижение по службе, основанное на их профессиональных качествах и уровне ответственности. Возможность роста внутри структуры мотивирует сотрудников продолжать развиваться и улучшать свои навыки.

В условиях цифровых изменений это становится особенно важным, так как освоение новых технологий открывает дополнительные пути для профессионального роста. Использование новых программ и платформ становится важной частью работы, что позволяет улучшать квалификацию сотрудников и способствует повышению эффективности организации в целом.

Организация должна создавать условия для профессионального развития сотрудников, предоставляя им доступ к обучению и семинарам по освоению новых программных решений и технологий. В условиях цифровой трансформации экономики России, специалисты, которые оперативно осваивают новые инструменты и системы, получают преимущества в карьерном росте и улучшении квалификации.

Не стоит забывать и о стрессовых факторах, с которыми вынуждены будут столкнуться работники предприятий, находящихся в процессе цифровой трансформации. Для нивелирования подобных негативных стрессовых факторов необходимо обратиться к зарубежному опыту привлечения работников к процессу принятия управленческих решений. Данное действие повлечёт за собой повышение ответственности персонала к своей деятельности.

Другой немаловажной стратегией управления является формирование цифровых каналов обратной связи. Во-первых, это позволяет оперативно получать отзывы от граждан, что помогает корректировать качество работы. Во-вторых, это дает возможность значительно сократить время при передачи управленческих решений по иерархической цепочке предприятия. В-третьих, подобные цифровые каналы взаимодействия позволяют осуществлять организацию дистанционного формата работы. Это было особенно актуально в период пандемии COVID-19.

Для успешной реализации стратегий управления персоналом в условиях цифровой трансформации необходимо учесть ряд некоторых аспектов, которые формируют устойчивое взаимодействие между руководителем и работником.

Первым и наиболее значимым аспектом является персонализация. Данный аспект предполагает создание внутренних профилей на каждого работника, по аналогии с социальными сетями, только внутри организации. Данный аспект помогает работникам лучше интегрироваться в цифровую среду.

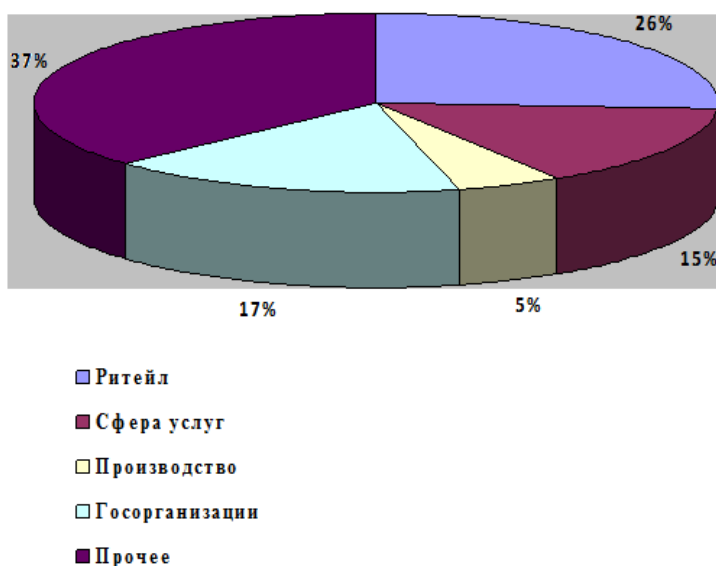


Рис. 1. Распределение утечек по количеству инцидентов в отраслях

Источник: составлено на основании [7].

Следующим немаловажным аспектом является ясность. Данный аспект касается необходимости постановки конкретных и доступных целей, чтобы каждый сотрудник четко понимал, что от него требуется. Это повышает эффективность работы и способствует лучшему выполнению задач.

Еще одним важным аспектом является открытость. Данный аспект имеет особое значение для создания доверительных отношений в организации. Работники должны быть уверены, что обещания, сделанные организацией, будут выполнены. Это уменьшает уровень недовольства и способствует нормализации рабочих процессов.

Участие в принятии решений связано с необходимостью создания возможностей для сотрудников выразить своё мнение. Это может быть достигнуто через платформы для обмена мнениями, которые позволяют работникам влиять на организационные процессы и высказывать идеи по улучшению работы.

Другим важным фактором является обеспечение цифровой безопасности, как личных данных самих работников, так и личных данных граждан. Отдельно стоит обратить внимание на то, что в сфере социальной защиты присутствуют личные данные всех граждан республики, и их защита от утечек являет первоочередной задачей на пути построения безопасного цифрового пространства.

Группа компаний «Солар» представила аналитический отчет центра мониторинга цифровых угроз Solar AURA, в котором зафиксировано 569 случаев утечек данных за первые девять месяцев 2024 года. Этот показатель на 80% превышает данные за аналогичный период предыдущего года. По результатам внешнего анализа, в 55% случаев утечки привели к полной публикации данных в открытом доступе, тогда как в остальных ситуациях информация распространялась в виде фрагментов баз данных, размещенных на теневых платформах и в даркнете [7].

Лидерами по числу зафиксированных утечек данных за первые девять месяцев 2024 года стали компании розничной торговли, где было зарегистрировано 182 инцидента. За ними следуют организации сферы услуг с 101 случаем и государственные учреждения с 45 инцидентами. В то же время финансовый сектор демонстрирует наиболее высокий объем утекших данных, достигший 409 миллионов строк. Аналитики связывают увеличение числа утечек с ростом фишинговых атак, количество выявленных и заблокированных ресурсов которых возросло на 116% по сравнению с предыдущим годом. Кроме того, отмечается активизация использования злоумышленниками фишинговых доменов третьего и более глубоких уровней, что усложняет их автоматическую идентификацию, так как такие домены чаще обходятся без упоминания известных брендов.

Как видно на рисунке 1 на долю госорганизаций приходится 17% всех утечек личных данных граждан.

Организациям рекомендуется уделять внимание созданию многоуровневой системы киберзащиты, включающей обучение своих работников в области информационной безопасности, регулярное наблюдение за состоянием внутренней IT-инфраструктуры и применение современных специализированных технологий.

Главной угрозой утечек данных на сегодняшний день является фишинг. Это вид кибератаки, при которой злоумышленники пытаются обманным путем получить конфиденциальную информацию, такую как персональные данные. Обычно фишинг осуществляется через электронные письма, текстовые сообщения, сайты или звонки, которые маскируются под законные организации или доверенные источники.

Фишинговые атаки продолжают набирать популярность и демонстрируют значительный рост, как в количественном, так и в качественном аспектах. В сравнении с аналогичным периодом прошлого года, за девять месяцев 2024 года количество обнаруженных и заблокированных фишинговых ресурсов увеличилось на 116%, согласно данным, предоставленным сервисом AURA [7]. При этом отмечается усложнение методов, используемых злоумышленниками, что существенно повышает их эффективность.

Современные реалии требуют разработки новых методов анализа доменных имен и веб-ресурсов для эффективного обнаружения фишинговых атак. При этом значительный прогресс достигнут в ускорении блокировки таких угроз. По данным Solar AURA, среднее время нейтрализации фишингового сайта в настоящее время составляет чуть более четырех часов, причем более половины вредоносных ресурсов блокируются еще быстрее. Добиться таких результатов удалось благодаря внедрению комплексных технических решений, автоматизации обработки жалоб на фишинг, а также укреплению взаимодействия с регистраторами доменных имен, хостинг-провайдерами и другими ключевыми участниками в сфере противодействия киберугрозам.

Согласно заявлению заместителя председателя правления Сбербанка С. Кузнецова, персональные данные около 90% взрослого населения России уже находятся в открытом доступе в результате утечек. Данную информацию он представил в рамках выступления на SOC-форуме [8].

По итогам анализа, проведенного Сбербанком в конце 2023 и начале 2024 годов, основными источниками компрометации данных стали интернет-магазины и медицинские учреждения. Как подчеркнул С. Кузнецов, вопреки распространенному

мнению, кредитные организации обеспечили лишь около 2% от общего объема утечек. Также отмечено, что 2023 год стал пиковым по числу утечек данных, тогда как в 2024 году наблюдается некоторое снижение их количества, хотя проблема остается актуальной.

Персональные данные клиентов, как правило, включают такие сведения, как фамилия, имя, отчество, паспортные данные, номера телефонов, адреса регистрации и электронной почты, а также другие идентификационные данные. Эта информация активно используется злоумышленниками для организации фишинговых атак и осуществления различных мошеннических операций, часто с применением методов социальной инженерии, направленных на введение клиентов в заблуждение.

По данным аналитиков InfoWatch, в 2023 году из финансовых организаций России было утрачено 170,3 миллиона записей, содержащих персональные данные клиентов. Всего зафиксировано 64 инцидента утечек, что на 3,2 раза больше по объему и на 12,3% чаще по числу случаев по сравнению с 2022 годом. При этом банки оказались ответственными за 46,9% всех утечек данных в финансовом секторе [8].

Результаты исследования и их анализ

Для успешного внедрения современных цифровых технологий в деятельность сферы социальной защиты населения ДНР необходима разработка эффективных стратегий управления.

Учитывая темпы цифровизации и особенности работы в социальной сфере, важно сосредоточиться на создании условий для внедрения инноваций, ориентированных не только на повышение технической квалификации, но и на устойчивость работы с населением в изменяющихся условиях.

Возможность работать дистанционно становится не только необходимостью в условиях ограничений, таких как пандемия, но и важной составляющей гибкости работы в условиях кризисных ситуаций. Это также помогает снизить риски для здоровья сотрудников, особенно в регионах с повышенной угрозой безопасности. Введение удаленной работы с использованием современных информационных технологий создает пространство для сотрудников социальной защиты развивать свои профессиональные навыки без необходимости постоянно находиться в офисе, что, в свою очередь, способствует сохранению трудовых ресурсов.

Таким образом, успешное внедрение цифровых технологий в социальной сфере невозможно без комплексного подхода, который охватывает как технические, так и организационные аспекты работы. Важно, чтобы все процессы, связанные с цифровизацией, были направлены на улучшение качества обслуживания населения, а также на создание условий для стабильной и эффективной работы сотрудников в условиях новых вызовов.

Выводы

Интеграция органов государственной власти ДНР и системы управления Российской Федерации создало дополнительные вызовы для системы социальной защиты, требуя оперативного преодоления цифрового отставания и адаптации процессов обработки данных. Необходимо было привести работу социальных служб в соответствие с федеральными стандартами, что вызвало увеличение объема задач, связанных с дополнительной обработкой данных и поддержанием эффективного функционирования системы.

Тем не менее, данные изменения открывают новые возможности для улучшения работы социальной защиты. Внедрение современных технологий и повышение качества обслуживания граждан могут значительно повысить эффективность системы. В результате этого сотрудники социальной сферы получают возможности для роста и повышения квалификации, что способствует улучшению общей производительности и адаптивности системы в условиях новых реалий.

Литература

1. Программа «Цифровая экономика Российской Федерации». [Электронный ресурс]. URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf> (дата обращения: 06.11.2024).
2. Марихин С.В., Журбин А.А., Калашникова Д.А. Методы мотивации и адаптации молодых специалистов в период цифровизации // Материалы Афанасьевских чтений. 2023. № 1 (43). С. 75-77.
3. Ромодан Ю.О., Малахова Е.М. Внедрение системы наставничества в современных организациях // Управление стратегическим развитием основных сфер и отраслей народного хозяйства в условиях современных вызовов: Материалы международной научно-практической конференции (Донецк, 02–03 ноября 2022 г.). Донецк: Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики. 2022. С.153-158.
4. Ромодан Ю.О., Кинаш А.О. Участие работников в управлении организацией // Управление стратегическим развитием основных сфер и отраслей народного хозяйства в условиях современных вызовов: Материалы международной научно-практической конференции (Донецк, 02–03 ноября 2022 г.). Донецк: Донецкая академия управления и государственной службы при Главе Донецкой Народной Республики. 2022. С.149-153.
5. «Герои среди нас»: В ДНР стартовал социальный проект о людях, проявляющих героизм. [Электронный ресурс]. URL: <https://www.donetsk.kp.ru/daily/27559/4884699> (дата обращения: 05.11.2024).
6. Докторова Н.П. Особенности формирования системы социального обеспечения населения // Сборник научных работ серии «Государственное управление». 2021. № 24. С. 123-128.
7. Ключевые внешние цифровые угрозы для российских компаний в I-III кварталах 2024 года // Центр мониторинга цифровых угроз Solar AURA. [Электронный ресурс]. URL: <https://rt-solar.ru/analytics/reports/4838/> (дата обращения: 05.11.2024).
8. «Сбер» оценил долю утекших данных взрослых россиян в 90% // Информационное издание РБК. [Электронный ресурс]. URL: <https://www.rbc.ru/finances/06/11/2024/672b2da59a79470df56c61e7> (дата обращения: 09.11.2024).