

Научная статья

УДК 338.24

doi: 10.34987/2712-9233.2023.71.51.009

Необходимость цифровой трансформации межведомственных взаимодействий в сфере обеспечения безопасности

Светлана Михайловна Калмыкова, Илья Иванович Калмыков, Никита Сергеевич Изупов

Сибирская пожарно-спасательная академия ГПС МЧС России, Железногорск, Россия

Автор ответственный за переписку: Никита Сергеевич Изупов, ron1230@yandex.ru

Аннотация. В этой статье исследуется глубокое влияние цифровой трансформации на межведомственное взаимодействие в сфере безопасности. Рассматривается интеграция цифровых инструментов, анализа данных и взаимосвязанных систем, подчеркивающая повышение эффективности операций по обеспечению безопасности. В статье подчеркивается ключевая роль, которую цифровизация играет в изменении и оптимизации взаимодействия между различными ведомствами и информационном обмене. Рассмотрена работа проводимая Красноярским краем в области цифровой трансформации.

Ключевые слова: цифровизация, цифровая трансформация, межведомственное взаимодействие, безопасность.

Для цитирования: Калмыкова С.М., Калмыков И.И., Изупов Н.С. Необходимость цифровой трансформации межведомственных взаимодействий в сфере обеспечения безопасности // Актуальные проблемы безопасности в техносфере 2023. № 4 (12). С. 48-52. URL: <https://doi.org/10.34987/2712-9233.2023.71.51.009>.

The need for digital transformation of interdepartmental interactions in the field of security

Svetlana M. Kalmykova, Ilya I. Kalmykov, Nikita S. Izupov

Siberian Fire and Rescue Academy EMERCOM of Russia, Zheleznogorsk, Russia

Corresponding author: Nikita S. Izupov, ron1230@yandex.ru

Abstract. This article explores the profound impact of digital transformation on interagency cooperation in the field of security. The integration of digital tools, data analysis and interconnected systems is considered, emphasizing the improvement of the effectiveness of security operations. The article highlights the key role that digitalization plays in changing and optimizing the interaction between different departments and information exchange. The work carried out by the Krasnoyarsk Territory in the field of digital transformation is considered.

Keywords: digitalization, digital transformation, interagency cooperation, security.

For citation: Kalmykova S.M., Kalmykov I.I., Izupov N.S. The need for digital transformation of interdepartmental interactions in the field of security // Actual problems of safety In the technosphere 2023. No. 4 (12). P. 48-52. URL: <https://doi.org/10.34987/2712-9233.2023.71.51.009>.

В эпоху, когда технологические достижения меняют представление о безопасности и защищенности, сближение цифровизации со сферой обеспечения безопасности стало ключевым сдвигом парадигмы. Сложное взаимодействие между различными ведомствами, участвующими в обеспечении общественной безопасности, правоохранительной деятельности, реагировании на чрезвычайные ситуации и снижении рисков, стало свидетелем глубокой трансформации, вызванной цифровыми технологиями. В этой научной статье рассматривается динамическое развитие и глубокие последствия цифровой трансформации, которая произвела революцию во взаимодействии между различными секторами и ведомствами безопасности. более безопасное и устойчивое будущее.

Развитием темы цифровых технологий, роли цифровизации, фундаментальных трансформаций современного государства под влиянием цифрового и технологического вектора занимались авторы Черногор Н.Н., Залоило М.В., Пашенцев Д.А. [1].

Цель сохранения здоровья и благополучия населения, а также создание безопасной и комфортной жизненной среды занимают важное место среди национальных приоритетов развития Российской Федерации до 2030 года, утвержденных Указом Президента от 21 июля 2020 года № 474. Стратегия развития информационного общества в России на период с 2017 по 2030 год направлена на интеграцию цифровых технологий и средств в управленческие системы всех отраслей экономики, социальной сферы, государственного управления, а также в системы обороны, обеспечения безопасности и поддержания правопорядка.

Правительство Российской Федерации развивает тему цифровизации, например, в [3] указаны основные направления развития в области цифровой трансформации государственного управления.

Цифровизация – процесс перехода на цифровые технологии, распространяющийся на все сферы жизни общества

Цифровизация в сфере безопасности подразумевает использование цифровых технологий, анализа данных и взаимосвязанных систем для улучшения и оптимизации различных аспектов обеспечения общественной безопасности. Это предполагает использование технологических достижений для улучшения реагирования на чрезвычайные ситуации, предотвращения преступности, борьбы со стихийными бедствиями и общих мер безопасности в сообществах.

Институт статистических исследований и экономики знаний высшей школы экономики поделился наблюдениями, отмечен рост финансирования практически во всех отраслях на внедрение и использование цифровых технологий (рис. 1), отмечается, что сфера государственного управления имеет относительно низкий уровень цифровизации. К субъектам, реализующим рекомендованные федеральными органами исполнительной власти и региональные проекты в иных отраслях цифровой трансформации в области обеспечения отдельных аспектов безопасности, отнесено 19 субъектов РФ или 23 % от общего количества регионов [12].

Необходимость переноса ключевых систем, обеспечивающих безопасность населения на цифровые платформы и специализированные цифровые экосистемы обусловлена всеобщим направлением цифровой трансформации. Этот процесс направлен на автоматизацию и оптимизацию текущих процессов. Эти цифровые системы и платформы должны характеризоваться высокой скоростью работы, стабильностью функционирования и обеспечением безопасности информации. Особые требования предъявляются к продуктам, применяемым в сфере обеспечения безопасности человека. Последствия от реализации и контроля рисков в этой области могут быть разнообразными - экономическими, физическими, психологическими, социальными и другими видами ущерба. Они могут быть мгновенными и ограниченными во времени или иметь долгосрочный характер. Автоматизация и оптимизация в области обеспечения безопасности призваны прежде всего предотвращать угрозы или смягчать последствия чрезвычайных ситуаций в короткие сроки.

Мировой опыт в области обеспечения безопасности населения охватывает следующие аспекты: развитие методов и средств предотвращения угроз, снижения и минимизации рисков, а также защиты от последствий этих рисков. Создание и развитие подвижных центров управления в чрезвычайных ситуациях; установку датчиков для отслеживания состояния объектов, разработку приложений для населения, мгновенно сообщающих об угрозах, таких как наводнения, землетрясения, экстремальные погодные условия, пожары, обвалы и тому подобное. Примером может служить система защиты персонала аварийных служб, использующая интеллектуальные маски, каски и костюмы, контролирующие качество воздуха и основные функции организма, и передающая информацию специалистам, ответственным за управление процессом [6].

Основы правового обеспечения цифровой безопасности в Российской Федерации были определены в документе под названием «Основные направления государственной политики в сфере обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры РФ», а также [9].

Цифровое преобразование систем гражданской обороны и чрезвычайных ситуаций, приоритетно внедряемое государственными органами, способствует повышению уровня управляемости рисков и угроз, связанных с чрезвычайными ситуациями, такими как пожарная безопасность, обеспечение безопасности на водных объектах и другими видами безопасности. Это достигается через улучшение и развитие взаимодействия между гражданами, организациями

и государственными органами (как федеральными, так и муниципальными). Одно из ключевых направлений этой инициативы — разработка и усовершенствование программно-аппаратных комплексов и технических средств для мониторинга, прогнозирования и поддержки принятия решений.

В сфере безопасности, подобно другим областям, процессы цифровизации имеют свои особенности. Многие регионы и крупные города используют различные технологии для усиления безопасности городской среды, такие как системы видеонаблюдения, обеспечивающие контроль на улицах и общественных местах, а также системы распознавания лиц, способствующие оперативному поиску лиц, совершивших преступления. Важным аспектом цифровизации является создание единой базы данных о правонарушителях и их местоположении. Также активно внедряются цифровые технологии для обеспечения безопасности дорожного движения, такие как системы обнаружения нарушений ПДД и выдачи штрафов, а также системы дистанционного контроля объектов, что помогает оперативно реагировать на потенциальные угрозы [10].



Рис. 1 индекс цифровизации отраслей

Анализируя наиболее значимые факторы оказывают существенное влияние на развитие цифровой среды:

- низкий уровень киберзащищенности цифровых процессов.
- привлекательность ИТ- сферы для мошенников и хакеров, высокий процент преступлений в интернет среде.
- высокая стоимость и сложность цифровых проектов.
- недостаточная доля компетентных в ИТ- сфере и подготовленных к использованию цифровых технологий сотрудников.
- низкая заинтересованность во внедрении цифровых технологий в связи с рисками утечки конфиденциальной информации и др.

В [5] представлены сферы применения цифровых технологий, сопряженные с наибольшими рисками, в том числе авторами делается упор на цифровое управление городом.

Однако современные технологии открывают огромные перспективы для улучшения жизни людей. Некоторые ключевые направления цифровизации в сфере общественной безопасности:

использование анализа данных, машинного обучения и искусственного интеллекта для сбора, анализа и интерпретации огромных объемов данных из различных источников (таких как датчики, камеры, социальные сети и т. д.)

внедрение передовых систем наблюдения, включая камеры видеонаблюдения, датчики, дроны и другие технологии мониторинга, для отслеживания и мониторинга общественных мест, критической инфраструктуры и зон повышенного риска в режиме реального времени.

использование цифровых инструментов и систем связи для сокращения времени и эффективности реагирования, сюда входят системы диспетчеризации, GPS-слежение, мобильные приложения для сообщения об инцидентах и инструменты распределения ресурсов, которые помогают службам экстренной помощи быстрее добраться до нужного места

использование цифровых платформ, социальных сетей, мобильных приложений и веб-сайтов для взаимодействия с общественностью

содействие сотрудничеству и обмену информацией между различными агентствами общественной безопасности (полицией, пожарными, службами скорой медицинской помощи и т. д.) через цифровые платформы и взаимосвязанные системы для улучшения координации во время чрезвычайных ситуаций или кризисов.

Проекты цифровой трансформации отрасли «Безопасность» на примере Красноярского края

С целью обеспечения безопасности в основных сферах жизни жителей Красноярского края в рамках государственной программы «Развитие информационного общества», утвержденной Постановлением Правительства Красноярского края от 30 сентября 2013 года № 504-п, осуществляют развитие, обслуживание и эксплуатацию комплексной автоматизированной системы «Безопасный город». Также проводятся мероприятия по созданию, развитию и организации автоматизированного обмена информацией в рамках регионального «Озера данных» РСЧС и усовершенствованию системы «112».

В Красноярском крае предполагается реализовать следующие решения для развития отрасли «Безопасность»:

- формирование системы управления оперативными данными в цифровом формате.
- повышение эффективности функционирования РСЧС.
- повышение степени оперативности и эффективности действий реагирующих структур.
- сокращение среднего срока простоя государственных информационных систем исполнительных органов

государственной власти.

- снижение риска простоя после компьютерных атак.
- расширение возможностей обращения в экстренные службы.
- недостаток профессиональных компетенций сотрудников.
- получение дополнительных гарантий безопасности при возникновении аварий.
- совершенствование процесса оказания финансовой помощи населению, пострадавшему в результате

ЧС природного и техногенного характера, посредством предоставления государственных услуг, в том числе в электронной форме.

Цифровое обновление отрасли безопасности неосуществимо без эффективной материальной и информационной базы, и поэтому процесс цифровизации в области безопасности должен быть тесно связан с реализацией региональных проектов. Например, развитие системы «Безопасный город» на территории Красноярского края во многом зависит от реализации другого регионального проекта под названием «Информационная инфраструктура». Этот проект направлен на расширение доступа к высокоскоростному интернету на всей территории края [12].

В рамках обновления отрасли безопасности Красноярского края поставлены важные задачи цифровизации:

касающиеся перевод в цифровой формат информационного взаимодействия со всеми органами повседневного управления территориальной подсистемы РСЧС до 2024 года.

достичь 85% обрабатываемых автоматизировано событий безопасности до 2024 года.

Заключение

Сегодня цифровизация является приоритетным направлением государственной политики Российской Федерации, данный процесс сопряжен с определенными трудностями, как показало исследование, в государственных структурах наблюдается низкая готовность к переходу на другой технологический уровень, низкая готовность к серьезной инфраструктурной трансформации. Наблюдается низкая цифровая грамотность сотрудников, в тоже время, наблюдается рост затрат на развитие цифровизации в России, однако встает вопрос о грамотном освоении вложенных инвестиций. Глобализация характеризуется состоянием, при котором решающую роль начинают играть информационные потоки и каналы обмена данными. Цифровизация государственных процессов оказывает значительное влияние граждан, способна ускорять взаимодействие между участниками процесса, преобразовывать качество отношений и скорость оказания государственных услуг.

Областью дальнейшего исследования вопроса развития цифровизации в России является анализ и систематизация информации о межведомственном взаимодействии государственных структур, внедрение информационных технологий, тем самым повышая их эффективность.

Список источников:

1. Черногор Н.Н., Залоило М.В., Пашенцев Д.А. «Концепция цифрового государства и цифровой правовой среды. Монография» М: -НОРМА, -2021 г. – 244

2. Российская Федерация. Законы. О национальных целях развития Российской Федерации на период до 2030 года Указ Президента Российской Федерации от 21.07.2020 г. № 474 // КонсультантПлюс: сайт. - URL: https://www.consultant.ru/document/cons_doc_LAW_2208834/ (дата обращения 01.12.2023)
3. Российская Федерация. Законы. Об утверждении стратегического направления в области цифровой трансформации государственного управления: Распоряжение Правительства РФ от 22 октября 2021 г. № 2998-р // КонсультантПлюс: сайт. - URL: https://www.consultant.ru/document/cons_doc_LAW_220831/ (дата обращения 01.12.2023)
4. Цифровая экономика //Институт статистических исследований и экономики знаний ВШЭ <https://ipforum.ru/upload/785333175-hpAqJdOc.pdf> (дата обращения 12.12.2023)
5. Грачева Ю. В. Риски цифровизации: виды, характеристика, уголовно-правовая оценка // Грачева Ю. В., Иванов С. А., Маликов С. В., Чучаев А. И. - М: Проспект, 2022 - 421 с.
6. Ellebrecht S., Kaufmann S. Digitalization and Its Security Manifestations // European Journal for Security Research. 2020;(5):1–3. doi: 10.1007/s41125-019-00063-8
7. Российская Федерация. Законы. О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон от 21.12.1994 № 68-ФЗ // КонсультантПлюс: сайт. - URL: (дата обращения 12.11.2023)
8. Российская Федерация. Законы. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»: Утв. Президентом РФ 03.02.2012 № 803 // КонсультантПлюс: сайт. - URL: https://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения 12.11.2023).
9. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации Федеральный закон от 26.07.2017 г. № 187-ФЗ // КонсультантПлюс: сайт. - URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 12.11.2023).
10. Морозова Г. А., Лапаев Д. Н. Современная цифровизация и обеспечение безопасности // Развитие и безопасность. 2019. № 1. С. 70–81. doi: 10.46960/74159_2019_1_70
11. Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Стратегии цифровой трансформации: https://digital.gov.ru/ru/activity/directions/1064/?utm_referrer=https%3a%2f%2fwww.google.com%2f (дата обращения 12.11.2023).
12. Стратегия в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Красноярского края <http://digital.krskstate.ru/page11464/page14216> (дата обращения 12.11.2023).

Статья поступила в редакция 11.12.2023, одобрена после рецензирования 21.12.2023, принята к публикации 21.12.2023.
The article was submitted 11.12.2023, approved after reviewing 21.12.2023, accepted for publication 21.12.2023.