УДК 338

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МФЦ : СОВРЕМЕННАЯ РОССИЙСКАЯ И МЕЖДУНАРОДНАЯ ПРАКТИКИ

Рязанова О. А.

к.э.н., доцент

Вятский государственный университет

Киров, Россия

Кошлец И.Г.

Магистрант

Вятский государственный университет

Киров, Россия

Аннотация. Цель работы: исследовать современную российскую и международную практики защиты информации в системе электронного правительства, формируемой в МФЦ. Методология проведения работы. В статье были применены общенаучные методы, используемые во всех областях, это анализ, описание, обобщение и объяснение. Результаты работы. В статье рассмотрены основные направления работы государственной информационной системы (ГИС), реализуемой в рамках проекта «Цифровое правительство» и предложена возможность использования биометрии, как дополнения к степени надежности контроля защиты информации, передаваемой чрез МФЦ. Область применения результатов: информационная система государственного управления РФ. Выводы: В условиях всеобщей цифровизации общества, Правительство Российской Федерации разрабатывает и внедряет в жизнь множество проектов нацеленных на повышение эффективности процесса оказания государственных услуг. Данные процессы встраиваются в жизнь не только на уровне России, но и других стран, в ряде которых данный опыт является более успешным. Так одним из недостатков цифрового развития государственного управления является наличие рисков взлома компьютерной информации и появление доступа к личным данным населения через многофункциональные центры (МФЦ). Для того чтобы устранить данный недостаток используется множество методов защиты информации, а также новых технологий в ряде которых используются криптографические инструменты, позволяющие не допустить взлома государственных информационных систем.

Ключевые слова: информация, контроль, многофункциональный центр, электронное правительство, криптографическая защита, биометрия, цифровизация, взломы.

ENSURING INFORMATION SECURITY OF THE MFC : MODERN RUSSIAN AND INTERNATIONAL PRACTICES

Ryazanova O. A.

Ph.D., Associate Professor

Vyatka State University

Kirov, Russia

Koshletz I. G.

Undergraduate

Vyatka State University

Kirov, Russia

Annotation. The purpose of the work: to study the modern Russian and international practices of information protection in the e-government system formed in the MFC. Methodology of the work. The article uses general scientific methods used in all fields, such as analysis, description, generalization and explanation. Results of the work. The article considers the main areas of work of the state information system (GIS) implemented within the framework of the Digital Government project and suggests the possibility of using biometrics as a supplement to the degree of reliability of monitoring the protection of information transmitted through the MFC. Scope of application of the results: information system of state administration of the Russian Federation. Conclusions: In the context of the general digitalization of society, the Government of the Russian Federation develops and implements many projects aimed at improving the efficiency of the process of providing public services. These processes are being integrated into life not only at the level of Russia, but also in other countries, in some of which this experience is more successful. Thus, one of the disadvantages of the digital development of public administration is the presence of risks of hacking computer information and the emergence of access to personal data of the population through multifunctional centers (MFC). In order to eliminate this drawback, many methods of information protection are used,

as well as new technologies, some of which use cryptographic tools to prevent hacking of state information systems.
Keywords: information, control, multifunctional center, electronic government, cryptographic protection, biometrics, digitalization, hacking.

Темп роста цифровизации, которая интегрируется фактически во все процессы жизнедеятельности в стране, отразился и на развитии информационных систем в области государственного управления. Именно в данной сфере процессы информатизации и цифровизации аккумулируются наиболее быстро. Это позволяет значительно упростить процесс взаимодействия государственной власти и населения, а также обработки поступающих документов в систему органов государственной власти, тем самым значительно повышая и ускоряя процесс оказания государственных услуг. В качестве оператора данных услуг в России создана сеть многофункциональных учреждений. Создание МФЦ стало возможным благодаря разработке единой площадки «Электронное правительство», через которую производится обмен информации между отдельными ведомствами страны, а также формируются потоки входящей и исходящей информации от разных зарубежных стран.

По состоянию на 2021 год, ГИС включает в себя более 300 ключевых функциональных сервисов, включая такие как [1]:

- Единая архитектура государственных данных;

- Цифровая трансформация органов и организаций прокуратуры Российской Федерации;

- Федеральная государственная информационная система «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» (ФГИС ЕИСУ КС, единая система).

Цель цифровой трансформации органов власти заключается в повышении эффективности их деятельности, определении условий

реализации всех функций, формирование цифровой инфраструктуры в государственной среде и повышение ее информационной безопасности.

Стоит отметить, что цифровая трансформация органов власти позволила обеспечить всем ведомствам готовность быстрого реагирования в условиях меняющейся общественно-политической и экономической ситуации, что связанно с переходом к цифровой экономике и развитием информационного пространства

Также цифровая трансформация нацелена на формирование единой сервисной модели государственной власти страны, способствующей развитию свободного и безопасного взаимодействия органов власти с гражданами, институтами гражданского общества, представителями государственной власти и местного самоуправления.

Наиболее приоритетные направления развития ИС в системе МФЦ систематизированы в таблице 1 [2].

Таблица 1- Наиболее приоритетные направления цифровой трансформации МФЦ

Приоритетное направление	Цель	Методы достижения
Высокотехнологичный надзор	формирование единой безопасной цифровой платформы, необходимой для обеспечения электронного взаимодействия всех уровней власти между собой и с другими органами	совершенствование правового и методического обеспечения автоматизированной оценки деятельности органов государственной власти; рост эффективности процесса управления; усиление активности оперативности реагирования представителей госвласти на нарушения закона, устранение причин и условий, им способствующих; снижение времени реагирования на обращения поступающие от населения; обеспечение своевременности и объективности информации о всех экономических фактах в РФ; рост обоснованности решений в исполнении функций с использованием методов автоматизированного выявления
Цифровая инфраструктура	рост качества электронного взаимодействия госвласти всех уровней	полная оптимизация и цифровизация процессов внутренней и межведомственной деятельности госвласти ;

	с гражданами, государственными органами посредством создания максимально безопасной высокотехнологичной цифровой среды.	модернизация правовых, нормативно-технических основ разработки, эксплуатации и развития создаваемых компонентов цифровой среды госвласти; развитие устойчивой и безопасной информационно-телекоммуникационной инфраструктуры, внедрение «сквозных» технологий и использование технологий обработки данных, единой облачной платформы, защита сети связи и передачи данных, использование СМЭВ, МЭДО, интегрированной сети передачи данных; разработка системы управления нормативно-справочной информацией и мастер-данными прокуратуры на всем жизненном цикле их деятельности; разработка единых требований и модели непрерывного повышения квалификации сотрудников госучреждений, использование дистанционных образовательных технологий, в вопросах реализации полномочий, оптимизации процессов подготовки и принятия решений в условиях цифровой среды.
Среда доверия	обеспечение всесторонней правовой защиты интересов граждан, представителей бизнеса и интересов государства при взаимодействии с ними в обновленной цифровой среде	формирование единой цифровой среды доверия экосистеме госвласти; формирование прозрачной среды взаимодействия с гражданами, организациями и обществом, позволяющей применять современные и перспективные каналы коммуникаций; интеграция в деятельность прокуратуры механизмов мониторинга и роста удовлетворенности граждан степенью защищенности конституционных прав и свобод повышение открытости, доступности и достоверности данных на основе внедрения прокуратурой и предоставления современных цифровых сервисов; усиление прозрачности информационного сопровождения надзорной деятельности с применением принципа обеспечения законности; обеспечение доступа граждан к открытой информации о деятельности прокуратуры, рост уровня общего доверия граждан к деятельности госвласти.

Источник : составлено автором

Указанные цели достигаются МФЦ посредством использования информационно-технических инструментов. При этом в деятельность МФЦ начинают внедряться все более новые и модернизированные информационные системы, среди которых перспективное место принадлежит автоматизированным базам данных, например, по гражданам, отбывающим условное наказание, вышедшим из мест заключения и т.п.

Успешно функционирующая информационная система в государственном управлении состоит из следующих активных информационных процессов (рисунок 1) [3].

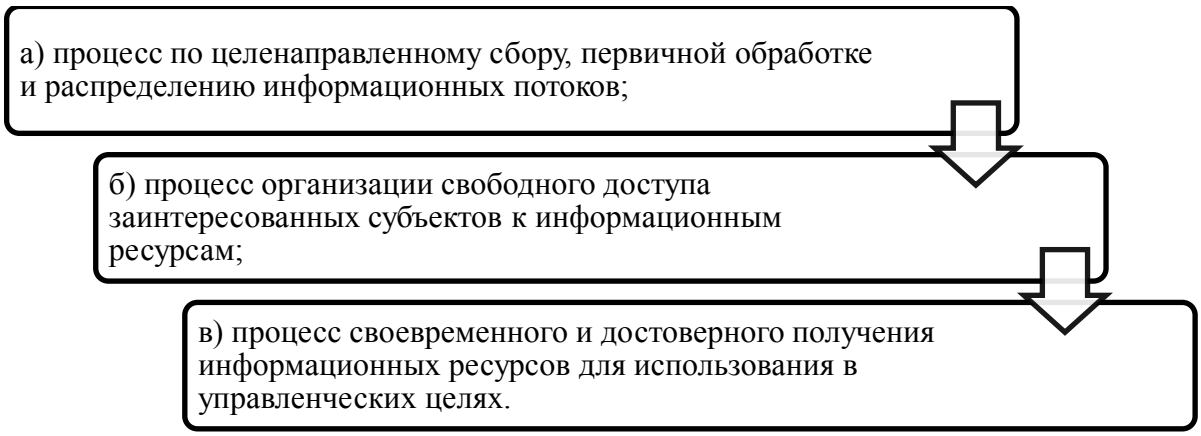

Рисунок 1- Процессы информационной системы МФЦ

источник : составлено автором

Таким образом, эволюция информационного обеспечения в среде государственного управления в России позволила сформировать эффективный процесс выполнения управленческих функций госслужащими, представляющий взаимосвязанный и взаимозависимый информационный комплекс работ, обеспечивающей успешное разрешение управленческих проблем. Возрастающая важность информационного взаимодействия приводит к встраиванию информационной функции во все виды управленческой деятельности, что свидетельствует о том, что информационное обеспечение превращается в условие эффективности деятельности государственных и муниципальных органов власти. Реализация

этой функции также позволит прояснить цели общества и разработать государственную политику в контексте появления качественно новой социальной системы, главной ценностью которой являются информация и знания, а также повысить эффективность государственного управления.

Однако проблема цифровизации и информатизации государственных ведомств, также как и МФЦ состоит в возможности их уязвимости, что становится все более угрожающим в век развития киберпреступности. К тому же пандемия коронавируса заставила практические все государственные службы срочно перейти на удаленную работу и пересмотреть подходы к безопасности.

В этих условиях начинают активно применяются новые средства защиты информации. При этом все более часто используются средства криптографии.

Поясним, что СКЗИ (средство криптографической защиты информации) представляет собой некую программу или устройство, позволяющую шифровать документы, генерируя при этом электронную подпись (ЭП) при помощи ключа электронной подписи, который подобрать вручную нереально. Этим обеспечивается надежная защита информации. Однако познания современных хакеров настолько усовершенствовались, что даже электронные подписи стали взламываться, а злоумышленники получать доступ к необходимой им информации. В этих условиях криптографические формы защиты дополняются средствами биометрической аутентификации данных. Данный тренд активно используется в зарубежных странах. Позитивен опыт Китая [5]. Вся принадлежащая государству конфиденциальная информация, передающаяся сетям передачи данных, а также все информационные системы, хранящие такие данные, используют алгоритмы базовой и общепринятой криптографии. При возникновении рисков, относящихся к используемым для этого алгоритмам, должны быть приняты немедленные меры. Закон предусматривает организацию строгого контроля за тем, как соблюдается положенный режим криптозащиты данных (контроль за соблюдением

регламентов в КНР поставлен строго, с начала года за упущения уже наказаны 383 тысячи чиновников) [6].

Каждая биометрическая технология, по сути, является независимым устройством, выполняющим задачи биометрической идентификации (распознавания лица или образа) на локальном уровне. Специфика любого подобного решения состоит в том, что они интегрируются в системы безопасности предприятий. Однако зачастую при этом сталкивается с рядом сложностей. Примером может послужить невозможность передачи запроса на получение статистики из аппаратного биометрического решения [7].

Данные технологии внедряются в госслужбы с целью проведения дополнительной биометрической проверки пользователей, которая позволяет минимизировать возможное мошенничество или нарушение внутренних правил сервиса, например, передачу аккаунтов одних зарегистрированных пользователей другим. [8].

Ключевым понятием, относящимся к «связыванию» ключей шифрования и паролей с биометрическими параметрами субъекта данных, считается преобразователь «биометрия-код» (ПБК). В России введена серия стандартов ГОСТ Р 52633, которые определяют требования к проведению процедур обработки биометрической информации и нечетких биометрических образов субъекта данных. В соответствии с ГОСТ получаемая информация в области биометрии человека преобразуется в его длинный пароль либо ключ, используемые в дальнейшей аутентификации пользователя [9].

Стоит отметить, что термины «биометрический пример» или «биометрический образ», определенные ГОСТ Р 52633 соответственно означают какой-то единичный образец биометрических данных и их совокупность. Однако понятие биометрического параметра зачастую путается с понятием признака, являющегося идентичным с позиции байесовской классификации. Поэтому на наш взгляд под биометрическим признаком и параметром биометрии в системе криптографической защиты ГИС стоит

подразумевать некоторую величину, обладающую физическим смыслом, характеризующим сам субъект.

Проведение дополнительных исследований направленных на выявление более совершенных методов компенсации изменения освещенности в полученных изображениях лиц, а так же методов классификации позволит повысить надежность алгоритма и применять программные решения на его основе в более широкой области Электронного Правительства. При этом использование международного опыта усилит эффективность данных разработок и повысит степень защиты «Электронного правительства» страны.

Таким образом, целесообразно развивать имеющиеся средства защиты ГИС в МФЦ, дополняя их технологиями биометрической аутентификации, которая ограничивает доступ к данным не только при помощи ЭЦФ, но и биометрическим анализом участников информационной системы.

Библиографический список:

1. Информационные технологии для государственных служащих / Камолов С.Г., Артемова П.В. – https://mgimo.ru/upload/iblock/edf/kamolov.pdf
2. Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информатизации и защите информации»
3. Digital Economy Agenda. Официальный сайт. Электронный ресурс. Режим доступа: https://www.commerce.gov/news/blog/2015/11/commercedepartments-digital-economy-agenda
4. Фирсов Д.В. Развитие системы информационного обеспечения в государственном управлении // Инновации и инвестиции. 2020. №1. URL: https://cyberleninka.ru/article/n/razvitie-sistemy-informatsionnogo-obespecheniya-v-gosudarstvennom-upravlenii (дата обращения: 05.04.2021).

5. Глобальное исследование по вопросам обеспечения информационной безопасности. Перспективы на 2020 год // ияЬ: http://www.pwc.ru/ru/riskassurance/publications/managing-cyberrisks.htmI (дата обращения: 28.03.2021).
6. Обзор международного рынка биометрических технологий и их применение в финансовом секторе/ январь, 2018 МОСКВА// https://cbr.ru/Content/Document/File/36012/rev_bio.pdf
7. Куприяновский В.П., Сотников А.Е., Соловьев А.И., Дрожжинов В.И., Намиот Д.Е., Мамаев В.Ю., Куприяновский П.В. Aadhaar - идентификация человека в цифровой экономике // International Journal of Open Information Technologies. 2017. №2. URL: https://cyberleninka.ru/article/n/aadhaar-identifikatsiya-cheloveka-v-tsifrovoy-ekonomike (дата обращения: 03.03.2021).
8. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

Оригинальность 97%