УДК 338

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОФУНКЦИОНАЛЬНЫХ ЦЕНТРОВ

Рязанова О. А.

к.э.н., доцент

Вятский государственный университет

Киров, Россия

Кошлец И.Г.

Магистрант

Вятский государственный университет

Киров, Россия

Аннотация. Многофункциональные центры прочно вошли в современную жизнь, значительно упростив процесс получения государственных услуг населением. В МФЦ можно получить паспорт, водительские права, оформить право на недвижимость и множество других услуг. При этом сеть данных центров функционирует в рамках национального проекта «Электронное правительство», которое подразумевает полную цифровизацию процесса оказания государственных услуг. Проблема в данном контексте просматривается через наличие большого числа информационных рисков, которые аккумулируются посредством передачи информации из одного ведомства в другое и предоставляют возможность ее перехвата и использования в мошеннических целях. В этих условиях важным является проработка комплексной системы безопасности МФЦ, которая предусматривает высокую степень защиты от взломов баз данных, содержащих огромные потоки информации о личных и конфиденциальных данных населения страны.

Ключевые слова: многофункциональные центры, информационная безопасность, риски, взломы, утечка, защита.

ENSURING INFORMATION SECURITY OF MULTIFUNCTIONAL CENTERS

Ryazanova O. A.

Ph.D., Associate Professor

Vyatka State University

Kirov, Russia

Koshletz I. G.

Undergraduate

Vyatka State University

Kirov, Russia

Annotation. Multifunctional centers have firmly entered modern life, greatly simplifying the process of obtaining public services by the population. In the MFC, you can get a passport, a driver's license, get the right to real estate and many other services. At the same time, the network of these centers operates within the framework of the national project "E-Government", which implies the complete digitalization of the process of providing public services. The problem in this context is seen through the presence of a large number of information risks that accumulate through the transfer of information from one agency to another and provide the possibility of its interception and use for fraudulent purposes. In these conditions, it is important to develop a comprehensive security system of the MFC, which provides a high degree of protection against hacking of databases containing huge flows of information about personal and confidential data of the country's population.

Keywords: multifunctional centers, information security, risks, hacking, leakage, protection.

Портал МФЦ представляет собой полноценное электронное представительство МФЦ в цифровых каналах и включает в себя максимальное количество процессов получения государственных и муниципальных услуг населением. Для граждан доступна и полнофункциональная мобильная версия Портала МФЦ, возможности которой совпадают с компьютерной системой [1].

Реализация принципа «одного окна» в МФЦ является ключевым элементом в повышении эффективности оказания гражданам государственных услуг. МФЦ работает в системе «МФЦ-Капелла», экспертная поддержка которой дает возможность как специалистам МФЦ, так и других организаций выступать универсальными операторами, консультирующими и принимающими документы по всем услугам МФЦ [2].

Согласно проекту Минэкономразвития РФ по развитию системы многофункциональных центров «МФЦ 2.0», у граждан должно может быть только два канала взаимодействия с государством – онлайн через портал ЕПГУ и офлайн через МФЦ.

На данный момент у МФЦ имеется возможность автоматической отправки информации гражданам о статусах их заявлений. По итогу проекта появляются все более новые возможности. Среди них стоит выделить, приведенные на рисунке 1.

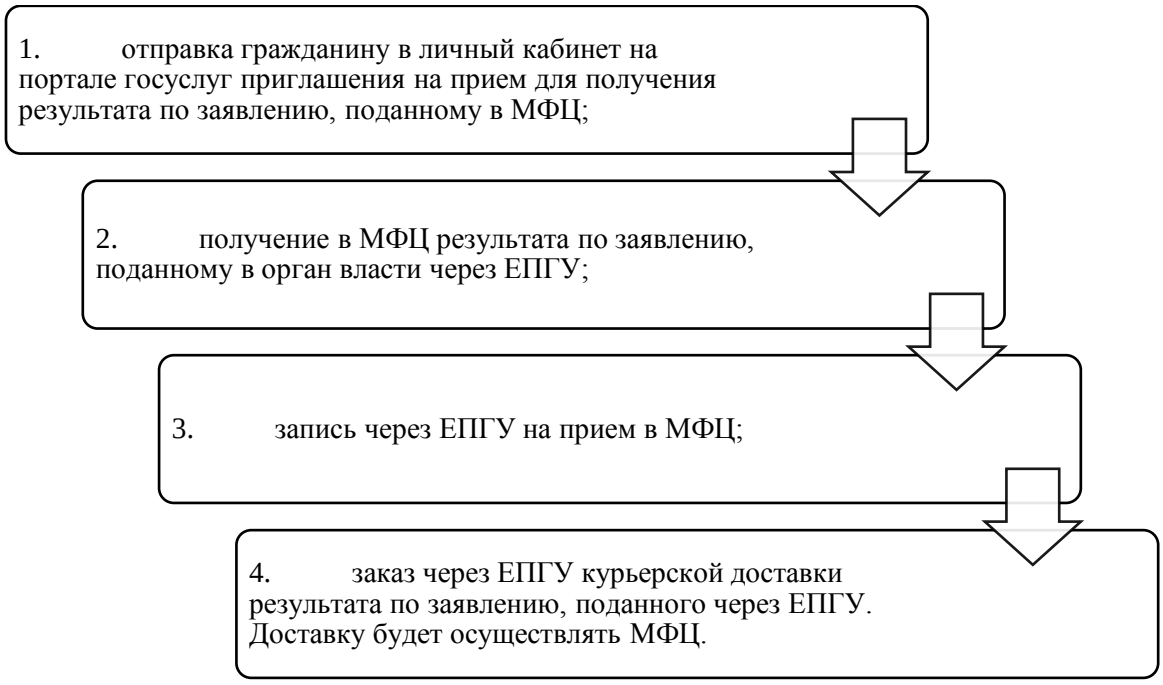

Рисунок 1 – Новые возможности МФЦ[1]

[1] Составлено автором самостоятельно

Развитие АИС МФЦ позволяет все более существенно оптимизировать работу МФЦ и процесс оказания услуг. Граждане получаются все больше государственных и муниципальных услуг в одном месте и максимально быстро и удобно [3].

Однако цифровизация и информатизация деятельности 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 применяться 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 [4]. Однако познания современных хакеров на столько 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].

Кроме верификации при физическом контроле доступа, распознавание лиц успешно заменяет пароли и ПИН-коды в задачах подтверждения платежных операций или при входе в аккаунт.

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 с целью проведения дополнительной биометрической проверки пользователей, которая позволяет минимизировать возможное мошенничество или нарушение внутренних правил сервиса, например, передачу аккаунтов одних зарегистрированных пользователей другим. Помимо поиска в реальном времени, идентификация может применяться для ретроспективного поиска в архиве видеозаписи, например при расследовании инцидента или при обнаружении VIP-персон/постоянных клиентов на объектах ритейла [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. При этом если генерируется ключ, который в той или иной степени отличается от составленного для субъекта имеет место ошибка 1-го рода, а ошибка 2-го рода может высветиться, ключ, полученный из биометрических данных субъекта, в метрике расстояний по параметрам оценивания близок к ключу другого субъекта настолько, что может быть принят за чужой ключ.

В целом при интеграции расширенного оператора локального бинарного шаблона, логика будет частично изменена. Если в базе ГИС зарегистрирована одна персона, то вероятность ее идентификации достигает максимального значения при приемлемом значении вероятности ложноположительной идентификации (ВЛПИ). В режиме верификации распознавание выполняется с большей долей точности.

Проведение дополнительных исследований, направленных на выявление более совершенных методов компенсации изменения освещенности в полученных изображениях лиц, а также 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 криптографической защиты ГИС, дополняя их технологиями биометрической аутентификации, которая ограничивает доступ к данным не только при помощи ЭЦФ, но и биометрическим анализом участников информационной системы, что позволит значительно обезопасить деятельность МФЦ и процесс получения государственных услуг населением России.

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. Tractica: Объем рынка биометрии к 2025 году достигнет $15 млрд https://iot.ru/promyshlennost/tractica-obem-rynka-biometrii-k-2025-godu-dostignet-15-mlrd

7. Обзор международного рынка биометрических технологий и их применение в финансовом секторе/ январь, 2018 МОСКВА// https://cbr.ru/Content/Document/File/36012/rev_bio.pdf
8. 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).
9. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

Оригинальность 95%