УДК 342

Кудинов А.С., аспирант
5.1.2. Публично-правовые (государственно-правовые) науки
Тверской Государственный Университет
Россия, г. Тверь

ЗАЩИТА ЛИЧНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМАХ ЭЛЕКТРОННОГО УПРАВЛЕНИЯ МЕСТНЫМ САМОУПРАВЛЕНИЕМ

Аннотация: *В данной статье рассмотрена практика использования цифровых технологий в работе органов МСУ. Дана подробная характеристика формулировке «персональные данные». Разобрана специфика защиты персональных данных с помощью цифровых систем безопасности. Исследовано правовое регулирование данного вопроса, а также характеристики эффективности работы систем информационной системы персональных данных (ИСПДн). Проведен анализ безопасности защиты персональных данных (ПДн) на платформе Госуслуги, на основании практики взятой из открытого доступа на портале МВД по республике Тыва. Дана характеристика эффективности работы системы идентификации при входе в учетную запись на Госуслугах. Предложены способы совершенствования правового регулирования данного вопроса.*

Ключевые слова: *защита персональных данных, системы электронного управления, правовое регулирование защиты персональных данных, безопасность персональных данных, организация обработки и защиты информации в органах местного самоуправления, персональные данные в информационных системах органов МСУ.*

PROTECTION OF PERSONAL DATA IN E-GOVERNMENT SYSTEMS OF LOCAL SELF-GOVERNMENT

Abstract: *This article examines the practice of using digital technologies in the work of LSG bodies. A detailed description of the wording «personal data» is given. The specifics of personal data protection using digital security systems are analyzed. The legal regulation of this issue is investigated, as well as the characteristics of the efficiency of the ISPDn systems. An analysis of the safety of PD protection on the Public Services platform was carried out, based on the practice taken from the open access portal of the Ministry of Internal Affairs of the Republic of Tyva. The characteristic of the effectiveness of the identification system when logging into an account on Public Services is given. The ways of improving the legal regulation of this issue are proposed.*

Keywords: *personal data protection, electronic management systems, legal regulation of personal data protection, personal data security, organization of information processing and protection in local governments, personal data in information systems of local self-government.*

Цифровизация управления стала неотъемлемой частью современной административной практики, особенно на уровне местного самоуправления. Интеграция информационных технологий в управленческие процессы обеспечивает не только повышение эффективности и прозрачности, но и способствует более активному взаимодействию между гражданами и органами власти. В условиях стремительно развивающегося цифрового общества особое значение приобретает защита личных персональных данных.

Система государственного управления модернизируется и активно использует возможности цифровых систем для повышения эффективности работы. Прежде чем воспользоваться возможностями цифровых систем

государственных органов и программ, резиденту Российской Федерации (далее РФ) придётся указать все свои персональные данные.

С начала 2002 года органы местного самоуправления взаимодействуют между собой и гражданами РФ с помощью цифровых систем в рамках ФЦП[1] «Электронная Россия». Основная цель данной программы - повышение эффективности коммуникации государственных органов с населением. На основании данной программы были разработаны системы, которые доказали свою эффективность в процессе работы:

- Автоматизированная [2] информационная система (АИС) представляет собой совокупность информации, экономико-математических методов и моделей, технических, программных, технологических средств и специалистов, предназначенных для обработки информации и принятия управленческих решений.

Назначение программы:

- Информационно-техническая база, которая помогает формировать основу для анализа и прогнозирования, что позволяет органам местного самоуправления более эффективно управлять ресурсами и планировать развитие территорий.;

- обслуживания специалистов и обеспечения обработки экономических, социальных и хозяйственных прогнозов, местных бюджетов, контроля и регулирования деятельности всех звеньев социально-экономических областей города, административного района и т. д.

- организационно - правовая база сведений о деятельности органов МСУ.

- Программный комплекс «Муниципальное самоуправление-СМАРТ»: централизованная, информационная система муниципальных

[1] ФЦП «Электронная Россия (2002–2010 годы)» Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Утверждена постановлением Правительства Российской Федерации от 28 января 2002 г. №65

[2] Желдыбина Ю.В Исаенко Ю.С. Информатизация органов МСУ.//Сетевое издание Международный студенческий научный вестник

образований на уровне региона (муниципального района), интегрирующая в себе информационное хранилище о деятельности органов местного самоуправления (далее МСУ).

Назначение данной системы:

- Похозяйственный учет муниципального округа: данные о населении МО, землях, объектах недвижимости и тд.

- Регистрационный учет населения: сведенья о месте регистрации, пребывания граждан, воинский учет;

- Налоговая ревизия на местном уровне: информация имущества физических лиц и информации об их правообладателях, оценка налоговых поступлений;

- Оказание государственных и муниципальных услуг населению: выдача справок и сведений из единого документооборота, реестров и тд.

- Межведомственное взаимодействие в структуре органов государственного управления: обработка, передача и хранение информации.

- Электронный муниципалитет [3] - государственная программа, которая представляет собой систему активного применения цифровых технологий в деятельности органов местного самоуправления.

Назначение программы:

- оказание муниципальных и государственных услуг населению через мобильные сервисы и приложения;

- электронная карта;

- единый центр многофункциональный центр (далее МФЦ) по принятию и обработке обращений населения.

Программа подразумевает создание единого цифрового окна по организации вопросов коммуникации населения с органами МСУ. Так как

[3] Шевандрин А.В. «Электронный муниципалитет, как перспективная модель эффективного местного самоуправления. Приоритеты России 31 (124)Режим доступа: https://cyberleninka.ru/article/n/elektronnyy-munitsipalitet-kak-perspektivnaya-model-effektivnogo-mestnogo-samoupravleniya/viewer

программа получает 100 % доступ к информации ПДн, она предусматривает определенную подготовку сотрудников, и правовой регламент для защиты персональной информации.

Структура обмена информации в данных цифровых системах представляет собой единую базу, с возможностью постоянного доступа для разных операторов и пользователей. Объем доступной информации определяется полномочиями, а также статусом «оператор» или «пользователь».

Вопросы обработки документов, содержащих персональные данные физических лиц (далее — ПД), регулируют следующими нормативно - правовыми актами (далее НПА):

- Федеральные законы № 152-ФЗ от 27.07.2006 «О персональных данных», № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»
- Трудовой кодекс РФ (глава 14);
- Постановления Правительства РФ № 687 от 15.9.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», № 211 от 21.03.2012 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом» О персональных данных», № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», № 996 от 05.09.2013Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ», № 1046 от 29.06.2021 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» и др;

- Приказы Роскомнадзора № 178 от 27.10.2022 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона» , № 179 и 180 от 28.10.2022 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных» и др.

Более того, если раньше под формулировку «персональные данные» (далее ПДн) попадали исключительно информация удостоверяющая личность, с появлением биометрии, к ПДн относятся данные, способные идентифицировать физическое лицо, как субъекта ПДн[4].

Таким образом, с правовой точки зрения персональные данные разделены на 4 категории, для которых характерны определенные требования организации, обработки и обеспечению безопасности хранения информации, данные сведенья представлены на рисунке 1[5].

[4] Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 6 февраля 2023 г.) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 11.
[5] Назаров, Д. М. Н19 Основы обеспечения безопасности персональных данных в организации [Текст]: учеб. пособие / Д. М. Назаров,К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. — 118 с.

Рисунок 1. Категории персональных данных

Особенности цифрового документооборота информации в органах местного самоуправления связаны со сложной иерархической структурой. Именно автоматизированная система позволяет быстро взаимодействовать данной структуре, однако не исключает возможность утечки информации от самих сотрудников. В связи с этим законодательство устанавливает требования обработки для каждой категории информации ПДн, и ответственность за их несоблюдение.

Субъектами, осуществляющими регулирование в области защиты ПДн, являются:

• Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - контроль и надзор за соответствием обработки ПДн требованиям законодательства.

• Федеральная служба по техническому и экспортному контролю (ФСТЭК России) разработка требований и способов защиты информации в

цифровых системах (без использования криптографических способов зашифровки информации);

• Федеральная служба безопасности (ФСБ России) устанавливает методы и способы защиты информации в информационных системах криптографическими методами.

В полномочия данных органов входит контроль, надзор, разработка нормативно - правовой документации, утверждение регламента работы сотрудников, которые имеют доступ к ПДн. Особое внимание в данном вопросе уделено подготовке кадров. В данном контексте назначается ответственные лица, которые формируют штат сотрудников, и подготавливают документацию для утверждения и подготовки технического оснащения для обработки данных.

Процесс защиты персональных данных происходит на нескольких уровнях и представляет собой систему ч.2 ст.19 152-ФЗ «О персональных данных», включающую:

1. Организационные меры:

- разработка и регулирование на законодательном уровне, разработка нормативно - правовой базы: политика защиты ПДн, обработка пользователей ПДн сайтов; положения о порядке уничтожения ПДн, о внутреннем аудите работы с персональными данными и т.д.
- контроль соблюдения действующего законодательства, назначение ответственного;
- подготовка операторов:
- организация и подготовка технического оснащения и комнаты для хранения цифровых носителей;
- выявление и устранение нарушений;
- проведение анализа процесса обработки информации, уничтожения и тд.

- регулярная смена паролей в учетных записях цифровых систем и на цифровых носителях.

Для организации деятельности операторов МФЦ разработан и эффективно действует правовой регламент [6] «Политика в отношении обработки персональных данных ГАУ БО «МФЦ», который устанавливает порядок работы с субъектами ПДн, срок и условия прекращения обработки, а также ответственность за разглашение информации субъекта ПДн. Все операции в системе фиксируются с указанием данных оператора.

2. Технические меры:

техническое оснащение, используемое при обработке информации, куда следует отнести: компьютеры, цифровые носители, информационные системы, необходимо тоже подвергать необходимым техническим мерам по защите ПДн.

Для предотвращения несанкционированного использования информации определяются условия, которые могут привести к доступу третьих лиц. Система предусматривает все возможные операции с данными для определения типа угрозы. Федеральная служба по техническому контролю и экспорту (ФСТЭК) выпустила документ, поясняющий, что информационные системы персональных данных (ИСПДн) делятся на группы по различным критериям. Для каждой группы определяется базовый уровень защищенности. Если система обладает 70% критериев с высокой защищенностью, ее общий уровень будет высоким. Если 70% с высокой или средней защищенностью, общий уровень будет средним.

Согласно постановлению Правительства № 1119, существуют 3 типа угроз для информационной системы персональных данных[7]:

[6] Политика обработки персональных данных. Государственное автономное учреждение «Иркутской области многофункциональный центр предоставления государственных и муниципальных услуг»

[7] Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

- Угрозы первого типа присутствуют, если в системном программном обеспечении для обработки ПДн есть недокументированные возможности.
- Угрозы второго типа присутствуют, если недокументированные возможности есть в прикладном программном обеспечении.
- Третий тип предполагает наличие угроз, не связанных с недокументированными возможностями в системном и прикладном программном обеспечении.

Тип угроз определяет оператор обработки ПДн на основании оценки вреда для ИСПДн. Законодательство выделяет несколько уровней защищенности ПДн[8]

- УЗ1 – высший уровень защиты для специальных и биометрических ПДн при угрозах первого типа.
- УЗ2 – защита общедоступных ПДн при угрозах первого типа и специальных ПДн при угрозах второго типа.
- УЗ3 – защита общедоступных ПДн при угрозах первого типа и иных ПДн при угрозах второго типа.
- УЗ4 – защита общедоступных и иных ПДн при угрозах третьего типа.

Система обрабатывает не только данные сотрудников внутри организации, но и ПДн других лиц, поступающие от оператора, которым в данном случае выступает орган МСУ.

ИСПДн классифицируются по принадлежности (государственные и муниципальные органы, юридические и физические лица), территориальному размещению (распределенные, городские, корпоративные распределенные,

[8] Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».// Режим доступа: https://base.garant.ru/70252506/

кампусные, локальные), доступу в интернет, операциям с данными и разграничению доступа.

Цифровизация ежедневно создает новые условия взаимодействия между оператором и субъектом ПДн через мобильные и стационарные устройства. Портал Госуслуг представляет собой единое цифровое окно для удаленного взаимодействия с населением. Идентификация по номеру телефона субъекта ПДн связана с риском кражи данных.

ПДн в данном случае постоянно сохраняется в базе Госуслуг, для сохранения конфиденциальности была разработана специальная система идентификации личности при входе в личный кабинет. Данная модель представляет собой идентификацию по номеру телефона субъекта ПДн. Однако данная модель состоит в категории риска кражи данных ПДн [9] по причине обычного человеческого фактора.

Изучая статистику МВД по взломам Госуслуг в разных регионах России, можно заключить, что система идентификации несовершенна. Причины следующие:

1. Субъекты ПДн сами предоставляют доступ к своим данным в магазинах, на сайтах, переходя по вредоносным ссылкам. Магазины, подписывая соглашения об обработке ПДн, не могут гарантировать отсутствие утечек от своих сотрудников. Большинство работает по системам УЗ3, УЗ4, не защищающим от угроз первого и второго типа.

2. Субъекты становятся жертвами мошенников, предоставляя доступ к учетной записи Госуслуг. Мошенники звонят под видом операторов, запрашивая код активации, что дает им доступ к ПДн.

3. Утечки могут произойти из-за некачественных приложений или халатности провайдеров, не соблюдающих требования 152-ФЗ.

[9]Незаконный доступ к порталу Госуслуг.//Электронный ресурс Министерство внутренних дел по Республике Тыва. Режим доступа: https://17.мвд.рф/news/item/49546922

Система идентификации не может предотвратить человеческий фактор, так как ее задача – предотвращение технических ошибок. МВД эффективно публикует информацию о подобных случаях для предупреждения. За кражу ПДн предусмотрены штрафы до 300 000 рублей (ст. 13.11 КоАП РФ). Уголовная ответственность предусмотрена по статьям 137, 159 и 272 УК РФ, но наказание зачастую ограничивается штрафом. Необходимо совершенствовать законодательство и повышать юридическую грамотность населения, так как 30% IT-преступлений в России остаются нераскрытыми[10].

Для предотвращения кражи ПДн важно совершенствовать законодательство, например, введение обязательной профилактической программы во всех учебных заведениях, включающей регулярные занятия по правовой грамотности и повышению юридической грамотности населения. В Республике Беларусь активно проводит разъяснительную работу Национальный центр защиты персональных данных [11] .В РФ аналогичную работу ведет Портал ПДн Роскомнадзора.

Законодательство должно быть понятно как операторам, так и субъектам ПДн. Прозрачные формулировки помогут улучшить защиту персональных данных и предотвратить их кражу.

Литература:

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Режим доступа:

[10] Садыкова К.А. Жонина Д.Е. Егорышева Е.А. «Некоторые проблемы раскрытия и расследования преступлений в сфере информационных технологий. //Киберленинка// Режим доступа: https://cyberleninka.ru/article/n/nekotorye-problemy-raskrytiya-i-rassledovaniya-prestupleniy-v-sfere-informatsionnyh-tehnologiy/viewer

[11] Сходства и отличия законодательных подходов к защите личной информации в России, Беларусси и Казахстане.// Электронный ресурс.// Режим доступа: https://rt-safety.com/articles/skhodstva-i-otlichiya-zakonodatelnykh-podkhodov-k-zashchite-lichnoy-informatsii-v-rossii-belarusi-i-/

https://www.consultant.ru/document/cons_doc_LAW_28399/bcddbd9060e44ed6085b65a1af0fb90aa3ef0175/

2. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) «О персональных данных» Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/be83e944acb538254bfc9bf073ece847ea189143/

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (последняя редакция) 27 июля 2006 года N 149-ФЗ Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61798/

4. Безопасность персональных данных - 1. Категории персональных данных. Медиабезопасность. Комитет по образованию.// Электронный ресурс. Режим доступа: https://komitet.kngcit.ru/obshaya-informaciya/bezopasnost/mediabezopasnost/bezopasnost-personalnykh-dannykh?start=1

5. ФЦП «Электронная Россия (2002–2010 годы)» Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Утверждена постановлением Правительства Российской Федерации от 28 января 2002 г. №65// Режим доступа: https://digital.gov.ru/ru/activity/programs/6/

6. Программный комплекс «Муниципальное самоуправление-СМАРТ».//Электронный ресурс.// Режим доступа: https://old.keysystems.ru/products/municipality/MunSelfSMART/

7. Назаров, Д. М. Н19 Основы обеспечения безопасности персональных данных в организации [Текст] : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. — Екатеринбург: Изд-во Урал. гос. экон. ун-та, 2019. — 118 с. https://aciso.ru/files/news/uchebnik.pdf

8. Желдыбина Ю.В., Исаенко Ю.С. Информатизация органов местного самоуправления. // Международный студенческий научный вестник.

– 2018. – № 4-6. URL: https://eduherald.ru/ru/article/view?id=19023 (дата обращения: 15.05.2024).

9. Садыкова К.А. Жонина Д.Е. Егорышева Е.А. «Некоторые проблемы раскрытия и расследования преступлений в сфере информационных технологий. //Киберленинка// Режим доступа: https://cyberleninka.ru/article/n/nekotorye-problemy-raskrytiya-i-rassledovaniya-prestupleniy-v-sfere-informatsionnyh-tehnologiy/viewer

10. Политика обработки персональных данных. Государственное автономное учреждение «Иркутский областной многофункциональный центр предоставления муниципальных и государственных услуг».// Режим доступа: https://mfc38.ru/activities/eg/popd

11. Техническая защита персональных данных. Проектирование и оценка соответствия системы защиты ПДн требованиям законодательства. режим доступа: https://www.radium-it.ru/solutions/pd/protection/

12. Алешина О. Защита персональных данных в 2024 году. //Электронный ресурс.// Режим доступа:https://ppt.ru/art/personal-data/zashchita-personalnykh-dannykh

13. Незаконный доступ к порталу Госуслуг.//Электронный ресурс Министерства внутренних дел по Республике Тыва. Режим доступа: https://17.мвд.рф/news/item/49546922

14. Сходства и отличия законодательных подходов к защите личной информации в России, Беларусси и Казахстане.// Электронный ресурс.// Режим доступа: https://rt-safety.com/articles/skhodstva-i-otlichiya-zakonodatelnykh-podkhodov-k-zashchite-lichnoy-informatsii-v-rossii-belarusi-i-/