УДК 004.056

Соболев Александр Александрович
студент 3 курса
юридический факультет
Российский государственный гуманитарный университет
Россия, г. Москва
e-mail: dikiy1423@mail.ru

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ, ОБРАБОТАННЫХ В ЭЛЕКТРОННОМ ВИДЕ

Аннотация: *Актуальность темы исследования связана с тем, что в последние годы все чаще происходят утечки из баз данных, что подтверждают данные статистики. В 2022 году число утечек персональных данных по-прежнему остается высоким, хотя многие вопросы, связанные с защитой персональных данных урегулированы законодательством и подзаконными актами, однако правоприменительная практика все еще остается недостаточной. В 2022 году уже сформировалась нормативно-правовая основа защиты персональных данных: Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ устанавливает основные принципы, понятийный аппарат, регулирует виды данных и т.д., подзаконные акты, в частности, Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» регулирует вопросы защиты персональных данных при их автоматизированной обработке, в частности, раскрывает суть уровней защиты информации, а также уровни угроз, Приказ ФСБ России от 10 июля 2014 г. № 378 регулирует вопросы обеспечения защиты персональных данных операторами, особенно в части административно-организационных мер, Приказ ФСБ РФ от 9 февраля 2005 г. № 66 регулирует вопросы связанные с использованием средств криптографической защиты информации, а также устанавливает требование по обеспечению безопасности данных на них. Гражданским, трудовым, административным и уголовным законодательством предусмотрено наступление соответствующих видов ответственности за нарушения в сфере информационной безопасности и персональных данных. В целом, тенденция положительная, разрабатываются новые методы защиты данных, формируется свод единых правил защиты данных в области цифровых технологий. В статье рассмотрены вопросы правового регулирования защиты персональных данных в организации с учетом последних изменений законодательства, вступивших в силу с 1 сентября 2022 года.*

Ключевые слова: персональные данные, законодательство, автоматизированная обработка.

Sobolev Alexander Alexandrovich
3rd year student
Faculty of Law,
Russian State University for the Humanities
Russia, Moscow

PROTECTION OF PERSONAL DATA PROCESSED IN ELECTRONIC FORM

Abstract: *The relevance of the study is conditioned by numerous database leaks which the statistics confirms last years. In 2022, the number of personal data leaks is still high, although many issues related to the protection of personal data are regulated by law and regulations, but law enforcement practice in this area is still insufficient. In 2022, the legal framework for the personal data protection has already been formed: the Federal Law "On Personal Data" dated July 27, 2006 N 152-FZ establishes the basic principles, the conceptual apparatus, regulates the types of data, etc., regulations, in particular, Decree of the Government of the Russian Federation of November 1, 2012 N 1119 "On approval of the requirements for the personal data protection during the personal data processing by information systems" regulates the protection of personal data during their automated processing, in particular, reveals the essence of the levels of information protection, as well as the levels of threats. Order of the FSB of Russia of July 10, 2014 N 378 regulates the issues of ensuring the personal data protection by operators, especially in terms of administrative and organizational measures, Order of the FSB of the Russian Federation of February 9, 2005 N 66 regulates issues related to the use of cryptographic protection tools, as well as establishes a requirement to ensure the security of such a data. Civil, labor, administrative and criminal legislation provides for the occurrence of appropriate types of liability for violations in the field of information security and personal data. In general, the trend is positive, new data protection methods are developing, a set of unified data protection rules in the field of digital technologies is forming. The article considers the issues of legal regulation of the personal data protection in organization with the latest changes in legislation that came into force on September 1, 2022.*

Key words: personal data protection, database leaks, legislation, automated processing.

Защита персональных данных в организации играет важную роль в диверсификации деятельности организации и степени защиты коммерческой тайны, поскольку, как ранее уже было отмечено, персональные данные в цифровую эпоху, приобрели положение незаконного объекта гражданского оборота в предпринимательских целях, т.е. массивы персональных данных продаются и покупаются для использования в маркетинге и рекламе, а также в

других целях. На уровне государства, проблема защиты персональных данных граждан, а также отдельных субъектов (сотрудники силовых ведомств, государственные служащие и др.) имеет особое значение, а потому в целях правового регулирования в рассматриваемой сфере был принят Указ Президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [1] и сформирована национальная программа «Цифровая экономика Российской Федерации». В рамках программы предусмотрен федеральный проект «Нормирование регулирования цифровой среды», которым планируется регулировать сквозные для различных отраслей законодательства вопросы, связанные с идентификацией субъектов правоотношений в цифровой среде, электронном документообороте данных, в том числе – персональных данных. Усиление государственного контроля за оборотом персональных данных также подтверждается тем, что с 1 сентября 2022 года вступили в силу поправки к законодательству о защите персональных данных. Одной из важнейших таких поправок является обязательное уведомление Роскомнадзора о том, что лицо является оператором по обработке персональных данных. В первую очередь к таким субъектам относятся организации, осуществляющие предпринимательскую деятельность. Также вводится обязанность операторов уведомлять Роскомнадзор обо всех инцидентах, связанных с безопасностью персональных данных.

Цифровая реальность является неотъемлемым элементом современного общества, именно темпы развития информационных технологий, создают все больше сложностей, связанных с защитой персональных данных в организации как работников, так и лиц, участвующих в сделках организации. Существенный объем неподконтрольных государству средств обработки информации создают возможности для незаконного оборота персональных данных, выражающийся в продаже массивов персональных данных. Слабая защита программного обеспечения создает риски утечки персональных данных, а также другой конфиденциальной информации.

Законодательно идет процесс упорядочивания защиты персональных данных, в том числе ее автоматизированной обработки, однако, по состоянию на 2022 год, остается множество вопросов, требующих решения. Тот факт, что персональные данные приобрели положение объекта незаконных гражданских сделок, т.е. приобрели свою валютную стоимость, крайне сильно усложнил способы борьбы с их незаконной обработкой, связано это в первую очередь с тем, что юридические лица, при осуществлении предпринимательской деятельности, занимаются рекламной и маркетинговой деятельностью, а получение и последующая обработка персональных данных потенциальных клиентов создает все возможности для извлечения сверхприбыли. Но если даже юридическое лицо старается исполнять законодательство в сфере защиты персональных данных, то отдельные работники организации зачастую злоупотребляют своим должностным положением и уровнем допуска к информации и попросту продают массивы персональных данных другим лицам. Учитывая, что ответственность именно за использование персональных данных в качестве объекта гражданских сделок не установлена, т.е. нет предусмотренной ответственности именно за продажу массивов персональных данных, то и риски их незаконной обработки существенно возрастают. Да, есть общая ответственность за нарушения законодательства в сфере информации, предусмотренная уголовным законодательством, есть административная ответственность, предусмотренная за проступки, связанные с персональными данными и конфиденциальной информацией, но все административные составы также не устанавливают ответственность за продажу персональных данных. Хотя законодателем и предусмотрена ответственность за незаконную обработку персональных данных, она носит недостаточный характер, т.к. в виду высокого уровня маргинализации российского бизнеса, предприниматели сознательно идут на нарушения, получают сверхприбыли и, если привлекаются к ответственности, то платят небольшие штрафы. Также проблемой является низкая правовая грамотность самих субъектов персональных данных, это подтверждается количеством исков, т.е. почти никто не обращается за судебной

защитой нарушенных прав. Но даже если бы статистика судебных дел по защите персональных данных возросла, то само законодательство не позволяет наказать виновное лицо достаточной мерой ответственности в гражданско-правовом порядке, т.к. по существующей судебной практике средняя сумма взыскания компенсации морального вреда составляет всего лишь пять тысяч рублей.

Еще одной серьезной проблемой защиты персональных данных в организации является низкая цифровая грамотность работников. Все дело в том, что большинство работников в организации имеют знания в области цифровых технологий на уровне пользователя персонального компьютера, т.е. умеют пользоваться программными продуктами на базовом уровне. Это создает риски утечки, т.к. работник даже без умысла может осуществить передачу персональных данных другим лицам по незащищенным каналам и произойдет утечка. Для решения этой проблемы, в цифровой среде необходимы курсы повышения квалификации работников организации в области цифровых технологий с обязательным тестированием знаний.

Также в организации следует разрабатывать локальные нормативные акты в сфере защиты информации, исходя из специфики деятельности организации и в соответствии с требованиями законодательства. Но самой разработки и утверждения локальных нормативных актов недостаточно, требуется ознакомление работников с принятыми защитными приказами и инструкциями и такое ознакомление должно происходить с контролем полученных знаний после ознакомления с локальным нормативным актом.

При разработке локальных нормативных актов по защите персональных данных следует руководствоваться:

1. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

2. Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

3. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

4. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

5. Постановлением Правительства РФ от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

Использование вышеуказанных нормативно-правовых актов, при разработке локальных актов организации по защите персональных данных необходимо в той мере, в которой будет обеспечена достаточная безопасность таких данных.

Но одних только локальных актов недостаточно, требуется комплексный подход в виде просветительской деятельности ответственными специалистами всех работников организации, обучение работников на курсах повышения квалификации по защите персональных данных, введение дисциплинарной ответственности за нарушения в сфере защиты персональных данных, даже если такие нарушения могут носят формальный характер (не заблокировал компьютер, когда вышел из кабинета, использовал посторонний носитель информации на рабочем компьютере, передал коллеге документы с персональными данными, заведомо зная, что тот не имеет допуска к ним и т.д.).

Безусловно, во всех вопросах, обеспечивающих защиту персональных данных, сложно разобраться простому сотруднику, поэтому организации, осуществляющие предпринимательскую деятельность часто привлекают к этой работе сторонние организации, специализирующиеся именно в этой сфере, имеющие не только опыт, но и лицензию на деятельность по технической защите конфиденциальной информации (п. 2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных [2]).

Для построения системной работы по защите персональных данных в цифровой среде организации следует придерживаться алгоритма:

- определить тип угроз безопасности персональных данных в организации (п. 7 Требований к защите персональных данных при их обработке в информационных системах [3]);

- подобрать один из четырех уровней защищенности персональных данных, исходя из вашего типа угрозы, в соответствии с п. п. 8 - 16 Требований к защите персональных данных при их обработке в информационных системах.

Именно от этого и будет зависеть комплекс мер.

Например, если по итогам определения типа угрозы специалист предложит обеспечить минимальный (четвертый) уровень защищенности персональных данных работников, вам потребуется (п. 13 Требований к защите персональных данных при их обработке в информационных системах):

- обезопасить помещения, в которых размещена информационная система, от неконтролируемого проникновения или неправомерного доступа;
- обеспечить сохранность носителей персональных данных;
- утвердить перечень лиц, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе;
- защитить информацию с помощью средств, прошедших процедуру оценки соответствия (в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз).

Кроме того, у организации есть обязанность взаимодействовать с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В частности, потребуется уведомлять о компьютерных инцидентах из-за которых персональные данные неправомерно переданы (предоставлены, распространены и т.д.) (ч. 12 ст. 19 Закона о персональных данных).

Изменения в закон о персональных данных касаются всего порядка работы с ними: от особенностей согласия и уведомления Роскомнадзора до правил трансграничной передачи, прекращения обработки и исполнения новых сроков. За нарушение этих требований грозят не только крупные административные штрафы, но и уголовная ответственность (ст. 13.11, 13.12 и 19.7 КоАП РФ, ст. 137 и 272 УК РФ).

В заключение стоит отметить, что законодатель активно совершенствует механизмы защиты персональных данных, операторы персональных данных совершенствуют материально-технические способы и средства защиты персональных данных. По мнению автора, до тех пор, пока уровень правосознания и цифровой грамотности граждан и работников организаций будет на низком уровне, пока законодательно не будет введено такое понятие, как незаконный оборот персональных данных, как объекта гражданских сделок, не будет введена уголовная ответственность с реальным сроком лишения свободы ответственного лица с одновременным наложением штрафа на организацию в процентах от годового оборота, персональные данные так и будут находиться под угрозой участия в качестве объекта гражданских сделок с последующей их незаконной обработкой и риски утечек.

Список литературы:

1. Указ Президента РФ от 07.05.2018 № 204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Российская газета. 2018. № 97.

2. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 N 28375) // Российская газета. 2013. № 107.

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Российская газета. 2012. № 256.

4. Нам К.В. Особенности развития правового регулирования оборота и защиты персональных данных // Вестник гражданского права. 2020. № 5. С. 73-89.

5. Федеральный закон от 14 июля 2022 г. № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» // Российская газета. 2022. № 156-157

6. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // Справочно-правовая система «Консультант-Плюс».