Руководство по защите персональных данных

Душанбе - 2021

Идораи ҳуқуқи Инсон
ва Риояи Қонуният
Bureau of Human Rights
and Rule of Law
Бюро по правам человека
и соблюдению законности

Руководство
по защите персональных данных

Душанбе - 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Данное Руководство разработано общественной организацией «Бюро по правам человека и соблюдению законности» и основано на законодательстве Республики Таджикистан в сфере информации и защиты персональных данных.

В Руководстве приведены международные стандарты защиты данных, в частности, документы Организации Объединенных Наций и европейские стандарты. Стандарты Совета Европы и Европейского Союза в области защиты персональных данных не являются юридически обязательными для Республики Таджикистан, однако, приводятся для сравнения и разъяснения основных терминов и понятий.

Данное Руководство, в основном, предназначено для организаций гражданского общества, однако, может быть использовано широким кругом заинтересованных лиц, органов и организаций.

I. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ[1]

Согласно Всеобщей декларации прав человека (статья 12) «никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». [2]

Международный пакт о гражданских и политических правах (статья 17) провозглашает, что «1. Никто не должен подвергаться произвольному или незаконному вмешательству в его личную жизнь, семью, жилище или переписку, а также незаконным

[1] Подборка международных документов основана на подборке, включенной в Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

[2] https://www.un.org/ru/universal-declaration-human-rights/index.html

посягательствам на его честь и репутацию. 2. Каждый имеет право на защиту закона от такого вмешательства или посягательств».[3]

68/167 Резолюция ООН - Право на неприкосновенность личной жизни в цифровой век, принята Генеральной Ассамблеей 18 декабря 2013 года. [4]

Обновленная Резолюция ООН о праве на неприкосновенность частной жизни в эпоху цифровых технологий от 21 ноября 2016 года, в которой подтверждается необходимость ограничивать полномочия спецслужб, осуждается массовое наблюдение и, кроме того, указывается на обязанность частного сектора уважать права человека, информировать пользователей о сборе, использовании, совместном использовании и хранении личных данных и установить прозрачные политики обработки.[5]

Руководящие принципы регламентации компьютеризованных картотек (файлов), содержащих данные личного характера, принята резолюцией 45/95 Генеральной Ассамблеи от 14 декабря 1990 года. В Резолюции говорится об основных принципах, касающихся минимальных гарантий, которые должны быть предусмотрены национальным законодательством.[6]

Конвенция Совета Европы о защите физических лиц в отношении автоматической обработки персональных данных (Конвенция 108). Конвенция открыта для подписи с 1981 года, применяется ко всей обработке данных, осуществляемой как частным, так и государственным секторами, включая обработку данных судебными и правоохранительными органами. Она защищает людей от злоупотреблений, которые могут сопровождать обработку персональных данных, и в то же время регулирует трансграничные потоки персональных данных.[7]

---

[3] https://www.ohchr.org/ru/professionalinterest/pages/ccpr.aspx
[4] https://undocs.org/ru/A/RES/68/167
[5] https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1&Lang=R
[6] https://www.un.org/ru/documents/decl_conv/conventions/computerized_data.shtml
[7] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078c46

Дополнительный протокол (№181) к Конвенции Совета Европы (108) о защите физических лиц при автоматизированной обработке персональных данных, касающийся наблюдательных органов и трансграничной передачи данных. Был принят в 2001 году, ввел положения о трансграничных потоках данных в страны, не являющиеся сторонами, так называемые третьи страны, и об обязательном создании национальных надзорных органов по защите данных.[8]

Модернизированная конвенция 108+

Конвенция 108 в 2018 году прошла процесс модернизации который был завершен принятием протокола CETS No. 223 (Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных)[9] Модернизация преследовала две основные цели: решить проблемы, возникающие в результате использования новых информационных и коммуникационных технологий, и повысить эффективность ее осуществления.

(EU) 2016/679 GDPR (General Data Protection Regulation)[10] - это общее положение о защите данных в Европейском союзе (ЕС) и Европейском экономическом пространстве (EEA). GDPR был принят 14 апреля 2016 года и вступил в силу с 25 мая 2018 года. Поскольку GDPR - нормативный документ, он является непосредственно обязательным и применимым. GDPR стало образцом для многих национальных законов за пределами ЕС, включая Чили, Японию, Бразилию, Южную Корею, Аргентину и

[8] https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=181
[9] https://www.coe.int/ru/web/conventions/full-list?module=treaty-detail&treatynum=223
[10] Общий/Генеральный регламент по защите персональных данных. 25 мая 2018 года во всех государствах-членах Европейского Союза был введен новый закон о защите персональных данных.

Кению. GDPR также рассматривается передача персональных данных за пределы зон ЕС и ЕЕА. [11]

Согласно GDPR персональные данные означают любую информацию, относящуюся к идентифицированному или идентифицируемому человеку (физическому лицу (субъекту данных).

Параллельно Европейский союз принял Директиву 2016/680 о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или преследования за совершение уголовных преступлений или исполнения уголовных наказаний и о свободном перемещении таких данных. Директива установила комплексную систему защиты персональных данных в контексте правоохранительной деятельности, а также признала особенности обработки данных, связанных с общественной безопасностью.

С 2017 года Европейская комиссия работает над новым документом, который заменит Директиву 2002/58/ЕС и приведет в соответствие правила, регулирующие электронные коммуникации, обеспечит эффективную защиту прав на защиту данных пользователей коммуникационных услуг.

II. ПРИНЦИПЫ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

В GDPR (статья 5) изложены следующие принципы обработки персональных данных:

• Законность, справедливость и прозрачность
• Ограничение цели
• Минимизация данных
• Точность данных
• Ограничение хранения

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
https://gdpr-info.eu/

• Целостность и безопасность
• Подотчетность

В статье 4 Закона РТ «О защите персональных данных» Республики Таджикистан закреплены следующие принципы сбора, обработки и защиты персональных данных:

- соблюдение прав и свобод гражданина и человека;
- законность;
- справедливость;
- гласность и прозрачность;
- конфиденциальность персональных данных ограниченного доступа;
- равенство прав субъектов, обладателей и операторов;
- обеспечение безопасности личности, общества и государства.

III. НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ

Частная жизнь - широкое понятие, которому невозможно дать исчерпывающее определение. Оно включает сферу, внутри которой каждый человек может свободно развиваться и реализовывать свой потенциал. Сбор и хранение данных об отдельных лицах, как и доступ к ним или последующее использование информации, относятся к

Защите персональных данных. Право на уважение частной жизни и право на защиту персональных данных тесно связаны так как оба стремятся защитить автономию и достоинство людей. В праве Европейского Союза защита персональных данных признана фундаментальным правом, отдельным от основного права на уважение частной жизни, в то время как во многих других странах защита данных рассматривается как часть и правовой механизм, обеспечивающий защиту частной жизни.

Статья 5 Конституции Республики Таджикистан гарантирует, что «Жизнь, честь, достоинство и другие естественные права человека неприкосновенны».
Статья 23 Конституции РТ закрепляет: «Обеспечивается тайна переписки, телефонных переговоров, телеграфных и иных личных сообщений за исключением случаев, предусмотренных законом. Сбор, хранение, использование и распространение сведений о личной жизни человека без его на то согласия запрещаются».
Статья 21 Конституции РТ гарантирует защиту прав потерпевшего со стороны закона, а также государственную гарантию судебной защиты и возмещения нанесенного ему ущерба.

В соответствии с Гражданским кодексом РТ «Гражданин имеет право на охрану тайны личной жизни, в том числе тайны переписки, телефонных переговоров, дневников, заметок, записок, интимной жизни, усыновления, рождения, врачебной, адвокатской тайны, тайны вкладов…» *(статья 175)*.

Уголовный кодекс Таджикистана[12] предусматривает уголовную ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, а также более серьезную уголовную ответственность (от штрафа до ареста сроком до 4-х месяцев) за нарушение этих прав, если они совершены лицом с использованием своего служебного положения или специальных технических средств для негласного получения информации.

Статья 24 Закона РТ «Об электрической связи» также гарантирует гражданам РТ тайну телефонных разговоров, телеграфных, электронных и иных сообщений.

Законом РТ «Об информации» запрещается сбор, хранение, использование и распространение информации о частной жизни, а равно информации, разглашающей личную и семейную тайну,

[12] Статья 146 часть 2 УК РТ

тайну телефонных переговоров, почтовых, телеграфных и иных сообщений личности без ее на то согласия, кроме случаев, предусмотренных законодательством РТ. [13]

Незаконное собирание или распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия либо распространение таких сведений в публичном выступлении, произведении, СМИ или сети интернет, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам гражданина, а также, если эти действия совершены лицом с использованием своего служебного положения, влекут уголовную ответственность от штрафа до ареста.[14]

IV. ПЕРСОНАЛЬНЫЕ ДАННЫЕ И ИХ ЗАЩИТА

4.1 Понятие персональных данных

«Понятие и определение персональных данных обширно. К персональным данным относится любая информация, касающаяся идентифицированного или идентифицируемого физического лица.

Понятие персональных данных включает в себя любую информацию и не ограничивается информацией, которая относится к узкой интерпретации частной или семейной жизни человека. Персональные данные включают информацию о человеке (имя, фамилия, идентификационный номер, дата рождения, возраст, пол и т. д.) и его любой деятельности, включая профессиональную или общественную, контактную, финансовую, медицинскую, место проживания или работы, образование, семейное положение, интересы и увлечения, видео, аудиозаписи или фотографии и т. д.

С развитием технологий развивается и концепция персональных данных. Например, использование адресов интернет-протокола

[13] Статья 20 Закона РТ «Об информации»
[14] Статья 144 Уголовного кодекса РТ

(IP) и так называемых файлов cookie для создания профилей о поведении людей в Интернете вызвало широкие дискуссии о том, являются ли IP-адрес и файлы cookie персональными данными. Введение нового определения персональных данных, которое прямо включает онлайн-идентификаторы, расставило в этом споре все по местам».[15]

Согласно GDPR «персональные данные означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу (субъекту данных)».

В августе 2018 года в Таджикистане был принят Закон «О защите персональных данных», согласно которому персональные данные – это любая информация о человеке (сведения о фактах, событиях, обстоятельствах жизни), позволяющая идентифицировать (распознать) его личность.[16]

Ранее такое понятие, как «персональные данные» человека уже были включены в Закон РТ «Об информации» от 2002 года.[17] Согласно статье 20 данного Закона «Основными данными о личности (персональными данными) являются национальность, образование, семейное положение, материальное положение, религиозная принадлежность, состояние здоровья, а также адрес и место рождения. Закон РТ «О защите персональных данных» значительно расширяет понятие персональных данных, относя к ним «любую информацию» о человеке, с помощью которой человека можно идентифицировать.

Имя, фамилия, отчество, изображение человека, которые также относятся к персональным данным человека, защищаются гражданским законодательством РТ. Так, согласно Гражданскому кодексу РТ *(часть 5 статьи 20)* «Вред, причиненный гражданину в

---

[15] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.
[16] Статья 1 Закона РТ «О защите персональных данных».
[17] В редакции Закона РТ от 03.07.2012г.№848, от 27.11.2014г.№1164

результате неправомерного использования его имени, подлежит возмещению...»

Гражданский кодекс РТ *(статья 176) также* защищает право на собственное изображение: «1. Никто не имеет право использовать изображение какого-либо лица без его согласия, а в случае его смерти без согласия наследников. 2. Опубликование, воспроизведение и распространение изобразительного произведения (картина, фотография, кинофильм и другие), в котором изображено другое лицо, допускается лишь с согласия изображенного, а после его смерти с согласия его детей и пережившего супруга. Такого согласия не требуется, если это установлено законом, либо изображенное лицо позировало за плату».

4.2 Доступ субъекта персональных данных к информации

Субъект имеет право на получение информации, касающейся сбора и обработки его персональных данных, в том числе содержащей:

- подтверждение факта сбора и обработки;
- правовые основания и цели сбора и обработки;
- цель и применяемые способы сбора и обработки;
- наименование и место нахождения обладателя, оператора и третьего лица, сведения о лицах (за исключением работников обладателя, оператора и третьего лица), имеющих доступ к персональным данным, или которым могут быть раскрыты персональные данные;
- сроки сбора и обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом прав, предусмотренных настоящим Законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных.[18]

[18] Часть 4 статьи 22 Закона РТ «О защите персональных данных»

Согласно Закону РТ «Об информации» Каждое лицо имеет право на ознакомление с информацией, собранной о нем, требовать ее полноты и соответствия действительности; имеют право знать в период сбора информации, кем, какие сведения о них и с какой целью собираются, как, кем и с какой целью они используются.[19]

Обладатель, оператор и третье лицо обязаны представить субъекту или его законному представителю информацию, относящуюся к нему, в течение трёх рабочих дней со дня получения обращения.[20]

Информация о персональных данных человека предоставляется ему бесплатно. За предоставление информации может взиматься плата, не превышающая себестоимость услуг, связанных с ее предоставлением (например, если информация распечатана на бумаге, плата может взиматься за стоимость бумаги).[21]

Информация о личности относится к категории конфиденциальной информации и охраняется законодательством РТ.

Согласно Кодексу об административных правонарушениях (статья 88) отказ должностным лицом в предоставлении гражданину собранной в установленном порядке информации, непосредственно затрагивающей его права и свободы, либо несвоевременное предоставление такой информации, а также непредоставление информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или недостоверной информации, при отсутствии признаков преступления, влекут наложение штрафа в размере от 30 до 40 показателей для расчетов[22].

Биометрические персональные данные – это личные (индивидуальные) данные, которые принадлежат только конкретному человеку и не могут быть такими же у другого

[19] Статья 27 Закона РТ «Об информации»
[20] Часть 1 статьи 25 Закона РТ «О защите персональных данных»
[21] Статья 15 Закона РТ «О праве на доступ к информации».
[22] По состоянию на 2021 год один показатель для расчетов составляет 60 сомони

человека (отпечаток пальца, рисунок радужной оболочки глаза, код ДНК и др.).

Биометрические персональные данные могут обрабатываться только при наличии письменного согласия человека, кроме некоторых исключений. Такие исключения составляют: уголовное преследование и правосудие, исполнение судебных актов, а исполнение уголовного наказания и в некоторых других случаях (противодействии терроризму, экстремизму, коррупции и легализации (отмыванию) доходов, полученных преступным путём, финансированию терроризма и др.)[23]

Обладателем базы персональных данных в РТ является государственный орган, физическое и юридическое лицо, имеющие в соответствии с законодательством РТ право владения, пользования, распоряжения базой данных.

«Примерами держателя (обладателя) данных являются больницы, банки, правительственные учреждения и неправительственные организации. Парикмахер тоже может быть контролером данных, если хранит данные (имя, номер телефона, даты приема, полученные или требуемые услуги) клиентов в журнале. Многие контролеры сами обрабатывают данные и не нуждаются в услугах обработчиков. Примерами обработчиков данных являются компании по исследованию рынка, которые могут хранить или обрабатывать персональную информацию от имени контролера данных. Облачные (cloud service) провайдеры также хранят данные как обработчики».[24]

Оператором базы персональных данных в РТ является государственный орган, физическое и юридическое лицо, осуществляющие на основании законодательства или договора с обладателем обработку и защиту персональных данных.

---

[23] Статья 17 Закона РТ «О защите персональных данных».

[24] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

Субъект персональных данных - это физическое лицо, к которому относятся персональные данные.

Третье лицо – это лицо, не являющееся субъектом, обладателем и оператором, но связанное с ними обстоятельствами или правоотношениями по персональным данным.

Уполномоченным государственным органом в сфере защиты персональных данных в Республике Таджикистан является **Служба связи при Правительстве РТ.**

4.3 Доступность персональных данных

Персональные данные в Таджикистане подразделяются на общедоступные и ограниченного доступа.

Обладатель, оператор и третье лицо, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность.

В целях информационного обеспечения населения используются общедоступные источники персональных данных: биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации.[25]

Запрещается доступ посторонних лиц к сведениям о другом лице, собранным в соответствии с действующими нормативно-правовыми актами, если не имеется согласия лица, о котором собраны сведения, а если его нет в живых, то его наследника. При отсутствии наследников доступ к подобным сведениям разрешается по решению государственных органов, организаций или органов местной власти, являющихся собственниками информации.

Все организации, собирающие информацию о гражданах, должны до начала работы с ней осуществить государственную регистрацию соответствующих баз данных.[26]

---

[25] Статья 9 Закона РТ «О защите персональных данных»

[26] Статья 27 Закона РТ «Об информации»

Не подлежат предоставлению для ознакомления по информационным запросам официальные документы, содержащие конфиденциальную информацию, к коим относятся и персональные данные, а также информацию, касающуюся личной жизни граждан.[27]

Информация, содержащая сведения (в том числе, персональные данные) о частной жизни другого лица, не подлежит предоставлению по запросам без согласия человека.[28]

4.4 Условия и основания для сбора и обработки персональных данных

- Наличие согласия субъекта персональных данных на сбор и обработку.
- Сбор и обработка ПД ограничиваются достижением конкретных, заранее определенных и законных целей.
- Субъект данных должен быть уведомлен о собираемых в отношении него данных, ему обеспечивается доступ к касающимся его данным, а также он вправе требовать исправления неточных или вводящих в заблуждение данных.[29]

В законодательстве Таджикистана не указан способ и порядок предоставления согласия субъекта персональных данных. Однако, во избежание недоразумений, желательно, чтобы согласие субъекта было выражено в письменной форме на бумажном носителе, либо в форме электронного документа, подписанного в соответствии с законодательством РТ.[30]

---

[27] Статья 33 Закона РТ «Об информации»
[28] Статья 14 часть 1 Закона РТ «О праве на доступ к информации».
[29] Статья 8 Закона РТ «О защите персональных данных»
[30] Электронная цифровая подпись регулируется Законом РТ «Об электронной цифровой подписи»

Обладатель, оператор и третье лицо обязаны представлять доказательства о получении согласия субъекта на сбор и обработку его персональных данных.[31]

4.5 Сбор и обработка персональных данных без согласия субъекта данных

Сбор персональных данных - это действия, направленные на получение персональных данных.

Обработка персональных данных – это действия, направленные на запись, систематизацию, хранение, изменение, дополнение, извлечение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных.

Сбор и обработка персональных данных без согласия субъекта или его законного представителя производятся в случаях:

- выполнения государственными органами функций, предусмотренных законодательством РТ;
- защита конституционных прав и свобод человека и гражданина[32].

4.6 Уведомление субъекта данных

Обладатель или оператор, передавший персональные данные другим (третьим) лицам без согласия человека, а также лицо, получившее персональные данные не от самого человека, обязаны в трёхдневный срок направить субъекту данных уведомление, в котором должны быть указаны следующие сведения:

- ✓ фамилия и имя человека или организации, получивших персональные данные;
- ✓ цель обработки персональных данных;
- ✓ источник, из которого получены персональные данные.

[31] Часть 1 статьи 25 Закона РТ «О защите персональных данных»
[32] Статья 12 Закона РТ «О защите персональных данных»

Такое уведомление не требуется, если человек сам дал свое согласие на передачу персональных данных.[33]

4.7 Обезличивание данных

Анонимизация данных — это процесс, в котором все идентифицирующие элементы удаляются из набора данных таким образом, что субъект данных больше не идентифицируется. Это означает, что для анонимности данных в информации нельзя оставлять элементы, которые при определенных усилиях могли бы служить для повторной идентификации соответствующего лица. Успешно обезличенные данные не являются персональными данными, и законодательство о защите данных к ним больше не применяется. [34]

В Законе Республики Таджикистан "О защите персональных данных" не употребляется термин "анонимизация", однако, содержится понятие «обезличивание персональных данных», что означает «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных».[35]

При обработке персональных данных для проведения статистических, социологических, научных исследований обладатель, оператор и третье лицо обязаны их обезличить.[36]

В европейском законодательстве встречается еще один термин – псевдонимизация, он означает "обработку персональных данных таким образом, что персональные данные больше не могут быть отнесены к конкретному субъекту данных без использования дополнительной информации, при условии, что такая

---

[33] Статья 21 Закона РТ «О защите персональных данных»
[34] Руководство по защите персональных данных, Общественный фонд "Гражданская инициатива интернет политики", опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.
[35] Статья 1 Закона РТ «О защите персональных данных»
[36] Статья 19 Закона РТ «О защите персональных данных»

дополнительная информация хранится отдельно и подлежит техническим и организационным мерам по обеспечению того, чтобы персональные данные не приписывались идентифицированному или идентифицируемому физическому лицу". Один из способов псевдонимизации данных - шифрование. В отличие от анонимных данных, псевдонимные данные по-прежнему являются персональными данными и, следовательно, подпадают под действие законодательства о защите данных.

4.8 <u>Уничтожение данных</u>

Персональные данные подлежат уничтожению обладателем, оператором и третьим лицом в следующих случаях:

- по истечении срока хранения. Срок хранения персональных данных определяется датой достижения целей их обработки.[37]
- При прекращении правоотношений между субъектом и обладателем, оператором или третьим лицом.
- При вступлении в законную силу решения суда.[38]

Обладатель, оператор и третье лицо обязаны принимать меры по уничтожению персональных данных в случае достижения цели их сбора и обработки.[39]

4.9 <u>Хранение данных</u>

Согласно европейским стандартам (GDPR) «Контролеры и обработчики обязаны обеспечивать безопасность данных. Они должны рассмотреть возможность внедрения современных мер безопасности, соответствующих рискам, связанным с их деятельностью. Например, риски могут исходить от случайного или незаконного уничтожения хранимых данных или несанкционированного раскрытия, доступа или изменения. Меры

---

[37] Часть 3 статьи 14 Закона РТ «О защите персональных данных»
[38] Статья 20 Закона РТ «О защите персональных данных»
[39] Часть 1 статьи 25 Закона РТ «О защите персональных данных»

безопасности могут включать анонимность или шифрование данных, резервное копирование».[40]

По законодательству Республики Таджикистан «Непринятие мер должностными лицами, обеспечивающими безопасность хранения или обработки информации в учреждениях и предприятиях, независимо от форм собственности, повлекшее ее хищение, уничтожение или иные последствия, при отсутствии признаков преступления», влекут за собой административную ответственность в виде штрафа.[41]

4.10 Требования к техническим средствам сбора и обработки информации

Все технические средства сбора, обработки, хранения, накопления, уничтожения информации в целях их защиты, в том числе здания и сооружения, оргтехника, инженерные сети, предметы интерьера и быта, используемые в помещениях, где обрабатывается информация, подлежат проверке, проводимой Государственным унитарным предприятием «Центр технической защиты информации, сертификации и экспертизы» уполномоченного органа, на соответствие установленным стандартам, техническим условиям, нормам Государственной комиссии но радиочастотам РТ и иным нормам, в том числе международным, национальным стандартам других стран, введенным в действие на территории РТ. При получении положительного результата проверки они идентифицируются знаками соответствия установленного образца, утвержденными уполномоченным органом.

Персонал, имеющий отношение к информатизации, использующий электрические средства связи на территории РТ, подлежит проверке, и при положительном результате специалисту выдается

---

[40] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

[41] Статья 521 Кодекса об административных правонарушениях РТ

удостоверение, а при наличии высшего образования-сертификата уполномоченного органа.

4.11 Защита информации и данных

Защита персональных данных включает в себя комплекс мер, направленных на недопущение незаконного (несанкционированного) раскрытия или любых других незаконных действий в отношении персональных данных.

Обладатель, оператор и третье лицо обязаны принимать необходимые меры по защите персональных данных, направленных на:

- предотвращение несанкционированного доступа к персональным данным;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.[42]

Требования и правила по защите информации в технических средствах обработки информации устанавливаются Главным управлением по защите государственных секретов при Правительстве Республики Таджикистан.[43]

В соответствии со статей 16 Закона Республики Таджикистан "О защите информации" обязательной сертификации подлежит средства, предназначенные для защиты информации, в том числе, ограниченного доступа, подлежащей защите, к примеру, программы идентификации и аутентификации терминалов и

[42] Часть 2 статьи 25 Закона РТ «О защите персональных данных»

[43] Правила об условиях зашиты информации в технических средствах обработки информации, утверждено постановлением Правительства РТ от 6 июня 2005 года № 203, (в редакции Постановления Правительства РТ от 2.08.2010г.№402, от 10.10.2017г.№474), п.п. 4, 5, 6

пользователей, технические средства защиты информации от утечки и др.[44]

Нарушение правил технической защиты информации, в том числе, использование без соответствующего сертификата уполномоченного органа технических средств защиты информации, поступившей из-за границы; поставка (реализация) и использование технических средств защиты информации, не соответствующих требованиям стандартов влекут административную ответственность в виде штрафа.[45]

Согласно международным стандартам контролер (обладатель) или обработчик (оператор) несут ответственность за любой материальный и нематериальный ущерб в результате нарушения права на защиту данных.

Помимо права на подачу жалобы в надзорный орган, люди должны иметь право на эффективное средство судебной защиты и на подачу иска в суд. Физические лица, контролеры или обработчики данных, которые хотят оспорить юридически обязательное решение надзорного органа, тоже могут возбудить дело в суде.[46]

4.12 <u>Ответственность за нарушение законодательства о защите персональных данных</u>

На сегодняшний день, в законодательстве РТ отсутствует ответственность за нарушение законодательства о защите персональных данных. Однако, гражданин, который считает, что распространение его персональных данных нанесло ему

---

[44] Положение о сертификации средств защиты информации по требованиям безопасности информации, аттестации объектов информатизации, порядка их государственной регистрации, утверждено постановлением Правительства РТ от 1 октября 2004г. № 404, (в редакции Постановления Правительства РТ от 2.11.2007г.№555, от 2.08.2010г.№402)

[45] Статья 507 Кодекса РТ об административных правонарушениях

[46] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

ущерб, вправе обратиться в суд с гражданским иском о возмещении морального вреда. Так, согласно Гражданскому кодексу РТ *(статья 171)* «Если гражданину причинен моральный вред (физические и нравственные страдания) действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину другие нематериальные блага», то он может потребовать путем обращения в суд компенсации указанного вреда.

Кодекс об административных правонарушениях РТ не содержит ответственности за нарушение законодательства о защите персональных данных, однако, статья 664 кодекса предусматривает ответственность в виде административного штрафа сотрудников государственных органов и организаций за «использование в личных или групповых интересах информации, полученной при исполнении государственных функций, если законом таковая не подлежит распространению».

Уголовное законодательство Таджикистана предусматривает ответственность за незаконное собирание и распространение информации о частной жизни человека *(статья 144)*.

Кроме того, Уголовный кодекс РТ предусматривает уголовную ответственность за преступления в сфере информационной безопасности, такие, как неправомерный доступ к компьютерной информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты *(статья 298);* модификация компьютерной информации, включающая изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившее значительный ущерб или создавшее угрозу его причинения *(статья 299);* незаконное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием

компьютерной связи *(статья 301);* Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети *(статья 302);* разработка, использование и распространение вредоносных программ *(статья 303).*

V. СБОР, ХРАНЕНИЕ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ТРУДОВЫХ ПРАВООТНОШЕНИЯХ

Трудовой кодекс (ТК) Республики Таджикистан содержит Главу (4) Сбор, обработка и защита персональных данных работника), посвященную персональным данным работника.

Согласно ТК в полномочия работодателя входит сбор, обработка и защита персональных данных работника. Целями такого сбор и обработки являются, в том числе, обеспечение личной безопасности работника.

Однако, работодатель обязан обрабатывать персональные данные работника с предварительным уведомлением и с согласия работника.

За сбор, обработку и защиту персональных данных работника отвечает руководитель организации, в которую принимается работник.

Работодатель обязан соблюдать следующие требования для защиты персональных данных (ПД) работника:

- не передавать персональные данные работника третьему лицу без письменного согласия работника;
- разрешать доступ к персональным данным работника только специально уполномоченным лицам. При этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций, и соблюдать режим конфиденциальности;

- осуществлять распространение персональных данных работника в пределах организации в соответствии с требованиями, установленными законодательством РТ;
- предупреждать лиц, которым разрешен доступ к персональным данным работника, о том, что они обязаны использовать их исключительно с соблюдением законодательства РТ и не допускать их передачу третьим лицам;
- по требованию работника вносить изменения и дополнения в его персональные данные;
- обеспечивать порядок хранения персональных данных работника с соблюдением установленных законодательством РТ требований.

Работодатель не имеет права требовать у работника информацию:

- о его политических, религиозных и иных убеждениях, а также о частной жизни;
- о его членстве или деятельности в общественных объединениях, в том числе в профессиональных союзах. [47]

В свою очередь, работник имеет право на:

- доступ к своим персональным данным, на получение копий записей, содержащих персональные данные работника;
- требовать внесения изменений и дополнений, блокирования, уничтожения персональных данных, сбор и обработка которых осуществлены с нарушением требований трудового законодательства и других нормативных правовых актов РТ;
- обжаловать в суд действия (бездействие) работодателя, допущенные при сборе, обработке и защите его персональных данных.

Например, в судебной практике Российской Федерации **раскрытие размера зарплаты было признано грубым нарушением трудовых**

[47] Статья 57 ТК РТ

обязательств и послужило основанием для увольнения сотрудника (см. апелляционное определение Московского городского суда от 14.06.2016 по делу №33-22906/2016). В частности, в одном из дел системный администратор частной компании, получивший доступ к персональным данным коллег через программу 1С, стал распространять информацию о повышении зарплаты одного из менеджеров. Судом было признано, что сведения о заработной плате работника являются его персональными данными и не подлежат публичному разглашению работодателем или третьими лицами, получившими доступ к этой информации. Следует учитывать, что персональными данными считается не только зарплата, но и другие данные сотрудников, а также клиентов компании.

В судебной практике РФ также имеются случаи, когда разглашением была признана отправка информации на электронную почту, в мессенджеры или копирование на съемный носитель. [48]

В контексте трудового законодательства РТ размер заработной платы может подпадать под служебную тайну. Согласно Трудовому кодексу РТ *(статья 18)* работник несет обязанность по неразглашению сведений, составляющих государственные секреты, служебную, коммерческую или иную, охраняемую законом тайну, ставших ему известными в связи с выполнением трудовых обязанностей.

В трудовом законодательстве РТ одной из причин, которая может стать основанием для увольнения работника, указано разглашение работником сведений, составляющих охраняемую законом тайну.[49]

В случае умышленного разглашения служебной, коммерческой тайны, если условия сохранения ее предусмотрены законодательством РТ и трудовым договором, работник несет еще

[48] Источник: https://www.kommersant.ru/doc/4241072
[49] Статья 42 ТК РТ

и материальную ответственность в размере причиненного работодателю ущерба.[50]

VI. СБОР И ОБРАБОТКА ДАННЫХ ДЛЯ ЦЕЛЕЙ ЗАЩИТЫ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И ПРАВОСУДИЯ

«Ценность сбора и обработки персональных данных для защиты общественной безопасности и порядка, предотвращения и расследования преступлений неоспорима … Тщательное и полное соблюдение принципов пропорциональности и минимизации данных имеет огромное значение, особенно когда данные обрабатываются правоохранительными органами.

В своей деятельности правоохранительные органы должны уважать право на личную жизнь. Вмешательство в частную жизнь допускается только когда это является строго необходимым для достижения законной цели».[51]

Конституция РТ и ряд кодексов и законов Таджикистана гарантирует тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений *(см. подробно в Разделе III)*.

Согласно Закону «Об оперативно-розыскной деятельности» (ОРД) проведение оперативно-розыскных мероприятий, ограничивающих конституционные права человека и гражданина на невмешательство в частную жизнь, допускается по мотивированному постановлению органов, осуществляющих оперативно-розыскную деятельность, по ходатайству прокурора и с санкции судьи.[52]

---

[50] Статья 190 ТК РТ

[51] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

[52] Статья 8 Закона

Прослушивание телефонных разговоров и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжкого или особо тяжкого преступления.[53]

Законом об ОРД предусмотрено «оперативное отождествление личности и иных объектов, установление и идентификация лица и иных объектов по индивидуализирующим их статическим и динамическим неизменяемым признакам, а равно при помощи других способов, позволяющих с достаточной степенью вероятности опознать личность или иной объект» *(статья 1)*.

Также Закон об ОРД предусматривает оперативный контроль почтовых отправлений, телеграфных и иных сообщений, снятие информации с технических каналов связи, получение компьютерной информации *(статья 1)*.

При проведении оперативно-розыскных мероприятий орган, осуществляющий оперативно-розыскную деятельность, обеспечивает соблюдение прав человека и гражданина на неприкосновенность личной жизни, личной и семейной тайны, неприкосновенность жилища, на тайну переписки, телефонных переговоров, телеграфных и иных личных сообщений *(статья 5 Закона об ОРД)*.

Лицо, виновность которого в совершении преступления не была доказана и которое располагает фактами проведения в отношении его оперативно-розыскных мероприятий и считает, что были нарушены его права, вправе истребовать от органа, осуществляющего оперативно-розыскную деятельность, сведения о полученной о нем информации в пределах, допускаемых требованиями конспирации и исключающих возможность разглашения государственных секретов *(часть 3 статьи 5 Закона об ОРД)*.

Полученные в результате проведения оперативно-розыскных мероприятий материалы в отношении лиц, виновность которых в

[53] Часть 5 статьи 8 Закона об ОРД

совершении преступления не доказана, хранятся в течение шести месяцев после принятия постановления об отказе в возбуждении уголовного дела либо прекращения уголовного дела, а затем уничтожаются, если служебные интересы или правосудие не требуют иного порядка. Фонограммы и другие материалы, полученные в результате прослушивания телефонных разговоров и иных переговоров лиц, в отношении которых не было возбуждено уголовное дело, уничтожаются в течение шести месяцев с момента прекращения прослушивания *(часть 6 статьи 5 Закона об ОРД)*.

Органы, осуществляющие ОРД, не вправе разглашать сведения, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и иные интересы граждан и которые стали известными в процессе проведения оперативно-розыскных мероприятий, без согласия граждан, за исключением случаев, предусмотренных законодательством РТ *(часть 7 статьи 5 Закона об ОРД)*.

Если человек считает, что при осуществлении оперативно-розыскной деятельности были нарушены его права и свободы, он вправе обжаловать эти действия в вышестоящий орган, прокурору или в суд (судье) *(статья 5 Закона об ОРД)*.

VII. ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Рекомендации, закрепленные в международных документах

GDPR и Модернизированной Конвенцией 108 предлагаются следующие правила и механизмы защиты данных:

- Регулярно информировать всех сотрудников о правилах безопасности и обязательствах по защите конфиденциальности данных;
- Документировать свою деятельность: разработать документ, описывающий, какие данные обрабатываются, для каких целей и как долго они хранятся.

- Оценивать воздействие планируемых операций обработки на защиту персональных данных там, где обработка может привести к высокому риску для прав и свобод физических лиц, в том числе в случае профилирования, крупномасштабной обработки специальных категорий данных, широкомасштабном и систематическом мониторинге общедоступных мест.
- Придерживаться принципов конфиденциальности при проектировании и конфиденциальности по умолчанию (во время определения средств обработки, планирования обработки и во время самой обработки внедрять надлежащие технические и организационные меры, предназначенные для эффективного внедрения принципов защиты персональных данных).
- Четко распределять ответственность и компетенции в вопросах обработки данных, предоставлять доступ к данным ограниченному количеству сотрудников только по принципу служебной необходимости.
- Регулярно проверять авторизацию для доступа к местоположению, оборудованию и программному обеспечению для операций по обработке данных; ✓ Регистрировать (журналировать) и хранить журнал всех действий (включая доступ, копирование, изменения, удаление, экспорт, печать и т. д.) конкретных пользователей системы, вести регулярный мониторинг их действий
- Тщательно документировать другие формы раскрытия информации, помимо автоматического доступа к данным.
- Применять специальные контрольные системы для защиты от утечек и использовать протоколы для обнаружения отклонений и подозрительных действий в системе.
- В случае обнаружения нарушений немедленно проводить служебные проверки в соответствии с политикой информационной безопасности.

- Назначать сотрудника по защите данных и обеспечивать его участие в принятии решений, связанных с обработкой данных.
- Уведомлять надзорные органы и субъекты об определенных нарушениях/утечках данных, если они могут поставить под угрозу права и свободы субъектов.[54]

7.2 Дополнительные рекомендации для организаций, осуществляющих сбор, обработку и хранение персональных данных сотрудников, клиентов и других лиц, в целях осуществления своей деятельности

1. Разработать и внедрить в организации Политику информационной безопасности и Политику конфиденциальности, включающую раздел «Порядок сбора, хранения и защиты персональных данных».
2. Получать письменное информированное согласие сотрудников, клиентов и других лиц, в отношении которых осуществляется сбор, обработка и хранение персональных данных.
3. Письменно предупреждать об ответственности сотрудников, работающих с персональными данными других сотрудников, клиентов и иных лиц, в рамках деятельности организации.
4. Уничтожать хранящиеся в организации персональные данные после достижения целей сбора и обработки данных.

[54] Руководство по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

VIII. ПРАКТИЧЕСКИЕ ПРИМЕРЫ ЕВРОПЕЙСКОГО СУДА ПО ПРАВАМ ЧЕЛОВЕКА[55]

8.1 Л.Л. против Франции (№ 7508/02) - 10 октября 2006 г. *http://hudoc.echr.coe.int/eng?i=002-3113*

Заявитель жаловался на представление и использование при бракоразводном процессе документов из его медицинской карты без его согласия и без назначения медицинского эксперта. Суд постановил нарушение статьи 8 Конвенции, установив, что вмешательство в личную жизнь заявителя не было оправданным. Суд отметил, что французские суды только на вспомогательной основе ссылались на оспариваемые медицинские отчеты и они могли бы прийти к такому же выводу без них. Суд также отметил, что национальное законодательство не обеспечивало достаточных гарантий относительно использования данных о частной жизни в этом виде разбирательства.

8.2 Висс против Франции - 22 декабря 2005 г. *http://hudoc.echr.coe.int/eng?i=001-71735*

Два заявителя были арестованы по подозрению в совершении вооруженных ограблений и подвержены предварительному заключению. Согласно судебному ордеру разговоры по телефону между ними и их родственниками в тюремных комнатах были записаны. Заявители подали заявление о признании записи их разговоров недействительной. Суд постановил нарушение статьи 8 Конвенции, установив, что французское законодательство не указывает с достаточной ясностью, как и в какой степени власти могли вмешиваться в личную жизнь задержанных. Суд отметил, что систематическая запись для других целей, кроме тюремной безопасности, привели к утрате истинной идеи комнаты посещения -- позволить задержанным

[55] Практические кейсы выборочно приведены из Руководства по защите персональных данных, Общественный фонд “Гражданская инициатива интернет политики”, опубликовано при поддержке программного офиса ОБСЕ в г.Бишкек.

поддерживать некоторую степень частной жизни, в том числе конфиденциальность разговоров с членами семьи.

8.3 **Барбулеску против Румынии (Большая Палата) - 5 сентября 2017 г.** ***http://hudoc.echr.coe.int/eng-press?i=003-5825428-7419362***

Дело касалось решения частной компании уволить сотрудника после проверки его электронных сообщений и их содержания. Заявитель жаловался на то, что решение его работодателя нарушило его права на неприкосновенность частной жизни и что национальные суды не смогли защитить его права. Большая Палата постановила одиннадцатью голосами против шести, что имело место нарушение статьи 8 Конвенции, посчитав, что румынские власти неадекватно защищали право заявителя на уважение его личной жизни и переписки. Они не смогли найти справедливый баланс между различными интересами. Национальные суды не смогли определить, получил ли заявитель предварительное уведомление от работодателя о мониторинге его сообщений и о степени вторжение в частную жизнь. Кроме того, национальные суды не смогли определить, конкретные причины, оправдывающие введение мер мониторинга, мог ли работодатель использовать меры, влекущие за собой меньшее вмешательство в личную жизнь.

8.4 **Антович и Миркович против Черногории - 28 ноября 2017 г.** ***http://hudoc.echr.coe.int/eng-press?i=003-5927767-7571421***

Дело касалось двух профессоров и установленных в аудиториях систем видеонаблюдения. Профессоры заявили, что наблюдение было незаконным и они не имели эффективного контроля над собранными данными. Национальный суд отклонил их требование о компенсации, поскольку признал аудитории общественными местами. Суд постановил нарушение статьи 8 Конвенции. Суд отклонил аргумент правительства о том, что дело является

неприемлемым, отметив, что частная жизнь может включать профессиональную деятельность. Суд установил, что доказательства свидетельствовали о нарушении положений внутреннего законодательства, а национальный суд даже не обсудил правовые обоснования для видеонаблюдения, так как с самого начала решил, что дело не было связано с вторжением в частную жизнь.