



423740, Актаныш авылы, Ленин пр.,
17 нче йорт. Тел/факс 3-44-14.

423740, село Актаныш, пр. Ленина,
дом 17. Тел/факс 3-44-14.

ПОСТАНОВЛЕНИЕ

17.02.2020

КАРАР

ПР-23

**О порядке эксплуатации государственной
информационной системы Республики Татарстан «Бухгалтерский учет и
отчетность государственных органов Республики Татарстан и подведомственных
им учреждений»**

Во исполнение Постановления Кабинета Министров Республики Татарстан от 25.05.2019 года № 443 «Об утверждении Положения о государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений», Исполнительный комитет Актанышского муниципального района ПОСТАНОВЛЯЕТ:

1. Обеспечить использование государственной информационной системы «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» при ведении бухгалтерского учета, составлении отчетности, начислении заработной платы и осуществлении иных выплат физическим лицам в Исполнительном комитете Актанышского муниципального района и подведомственных ему учреждений».

2. Утвердить:

- Положение о порядке защиты персональных данных при работе в Государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (Приложение 1);

- Правила обеспечения безопасности персональных данных при их обработке в Государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (Приложение 2);

- Регламент выгрузки и передачи персональных данных в Государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (Приложение 3);

- Регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами при работе в Государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (Приложение 4).

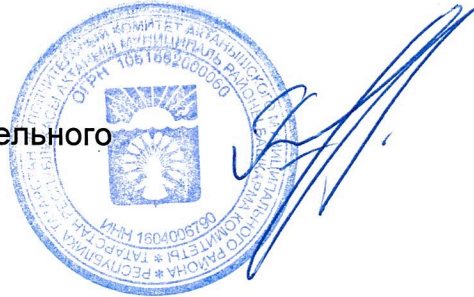
3. Рекомендовать руководителям муниципальных учреждений Актанышского муниципального района утвердить внутренние нормативные документы о порядке эксплуатации информационной системы «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (далее – Система) и назначить сотрудника, ответственного за эксплуатацию Системы.

4. Установить, что настоящее Постановление распространяется на правоотношения, возникшие с 9 января 2020 года.

5. Опубликовать настоящее постановление, на официальном портале правовой информации Республики Татарстан в информационно-телекоммуникационной сети "Интернет" по адресу: <http://pravo.tatarstan.ru> и на официальном сайте Актанышского муниципального района по адресу: <http://aktanysh.tatarstan.ru>.

6. Контроль за исполнением настоящего Постановления возложить на руководителя Финансово-бюджетной палаты Актанышского муниципального района Каюмову К.Р.

Руководитель Исполнительного
комитета



И.И. Габдулхаев



Приложение №1

УТВЕРЖДЕН

Постановлением Исполнительного комитета
Актамышского муниципального района от
«17» 02 2020г. № 17П-23

ПОЛОЖЕНИЕ

О порядке защиты персональных данных при работе в
Государственной информационной системе Республики Татарстан
«Бухгалтерский учет и отчетность государственных органов Республики
Татарстан и подведомственных
им учреждений»

СОДЕРЖАНИЕ

	Страница
Используемые сокращения	5
Термины и определения	6
1. Общие положения	7
2. Понятие и состав конфиденциальной информации	7
3. Порядок обработки конфиденциальной информации	8
4. Хранение и передача конфиденциальной информации	9
5. Ответственность за разглашение конфиденциальной информации	10
Приложение	11

Используемые сокращения

Сокращение	Полное наименование
Система	Государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
КИ	Конфиденциальная информация
ПО	Программное обеспечение
РД	Руководящий документ
РТ	Республика Татарстан
РФ	Российская Федерация
СрЗИ	Средство защиты информации
ФЗ	Федеральный закон

Термины и определения

В настоящем документе используются следующие термины и определения:

Автоматизированная информационная система – совокупность программно-аппаратных средств, предназначенных для автоматизации деятельности, связанной с хранением, передачей и обработкой информации;

Администратор безопасности Системы – сотрудник, работающий в Системе, в обязанности которого входит обеспечение штатного функционирования средств и системы защиты от несанкционированного доступа к защищаемой информации;

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

Информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации;

Оператор – Государственный заказчик, Функциональный оператор, Функциональный пользователь, организующий и осуществляющий обработку, а также определяющий цели и содержание обработки конфиденциальной информации в Системе;

Пользователь Системы – сотрудник, работающий в Системе, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты;

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты информации;

Орган – орган государственной власти Республики Татарстан, орган местного самоуправления Республики Татарстан.

1. Общие положения

1.1. Положение о защите персональных данных при работе в государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений» (далее – Положение) определяет порядок обработки и обеспечения защиты конфиденциальных данных при их обработке в Системе.

1.2. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
 - Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
 - Руководящим документом Государственной технической комиссии Российской Федерации от 30.03.1992г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
 - Постановлением Правительства Российской Федерации от 03.11.1994 №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в Федеральных органах исполнительной власти»;
- другими руководящими и нормативными документами по защите информации, действующими на территории Российской Федерации.

1.3. Настоящее Положение является обязательным для ознакомления и исполнения всеми пользователями, имеющими доступ к защищаемой информации, обрабатываемой в Системе. (Форма Листа ознакомления приведена в приложении к настоящему Положению).

2. ПОНЯТИЕ И СОСТАВ КОНФИДЕНЦИОНАЛЬНОЙ ИНФОРМАЦИИ

2.1. К информации конфиденциального характера относится несекретная информация, касающаяся деятельности ведения бухгалтерского учета и расчета заработной платы в Системе.

2.2. К конфиденциальной информации, обрабатываемой в Системе, относятся:

1) сведения по общим вопросам организационной деятельности Органов в Системе;

2) сведения по вопросам технической защиты информации;

3) сведения по бухгалтерским и кадровым вопросам;

4) сведения о персональных данных сотрудников Органа: фамилия, имя, отчество; прежние фамилия, имя отчество; дата и место рождения; пол; гражданство; владение иностранными языками и языками народов Российской Федерации; образование; ученая степень; ученое звание; дополнительное профессиональное образование; профессия (специальность); стаж работы; наличие классного чина (воинского или специального звания); наличие государственных наград и иных наград, знаков отличия (кем награжден и когда); сведения о приеме, перемещениях, назначениях и увольнении; сведения о командировках, отпусках, о временной нетрудоспособности; семейное положение (в том числе: состав семьи, степень родства, фамилия, имя, отчество, дата рождения близких родственников, их место работы или учебы); паспортные данные; свидетельство о государственной регистрации актов гражданского состояния; адрес места жительства и проживания; номер контактного телефона; номер страхового свидетельства государственного пенсионного страхования; сведения о воинском учете; идентификационный номер налогоплательщика; наличие (отсутствие) судимости; допуск к государственной тайне, оформленный за период работы; сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, о расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей; фотографическое изображение; заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, а также иные персональные данные, относящиеся к вопросам исполнения служебной деятельности и необходимые для выполнения работы в рамках Системы.

3. ПОРЯДОК ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

3.1. Под обработкой КИ пользователя Системы понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с КИ, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение КИ.

3.2. Обработка КИ может осуществляться с письменного согласия пользователя Системы либо без согласия в случаях, предусмотренных федеральным законодательством в сфере защиты конфиденциальной информации.

3.3. К обработке КИ в Системе допускаются лица на основании документа «Перечень лиц, допущенных к работе с Системой».

3.4. Пользователи Системы, получающие доступ к КИ, обязаны не раскрывать третьим лицам и не распространять КИ без согласия субъекта, если иное не предусмотрено федеральным законодательством в сфере защиты конфиденциальной информации.

3.5. Пользователи Системы при обработке КИ должны соблюдать следующие общие требования:

- обработка КИ может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

- при определении объема и содержания обрабатываемой КИ пользователь Системы должен руководствоваться Конституцией Российской Федерации и иными федеральными законами, в соответствии с утвержденным перечнем КИ;

- пользователи Системы должны быть ознакомлены под роспись с документами Системы, устанавливающими порядок обработки КИ.

4. ХРАНЕНИЕ И ПЕРЕДАЧА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Хранение КИ должно осуществляться не дольше, чем этого требуют цели обработки КИ, если срок хранения КИ не установлен федеральным законом.

4.2. КИ хранится в архиве базы данных Системы, к которому имеют доступ сотрудники, включенные в Перечень лиц, допущенных к работе с Системой.

4.3. На носителях информации, содержащих сведения конфиденциального характера, проставляется пометка «Для служебного пользования».

4.4. Передача документов и дел с пометкой «Для служебного пользования» от одного специалиста другому осуществляется с разрешения ответственного за информационную безопасность Системы.

4.5. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором по адресно проставляются номера экземпляров отправляемых

документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, готовившего документ.

4.6. Уничтожение дел, документов с пометкой «Для служебного пользования», утратившие свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

5. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5.1. Пользователь Системы, допущенный к работе с КИ, несет ответственность за сохранность носителя и конфиденциальность информации.

5.2. Ответственный за обеспечение безопасности информации в Системе, допускающий пользователей к работе с КИ, несет персональную ответственность за предоставленный допуск.

5.3. Нарушение норм, регулирующих получение, обработку и защиту КИ, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.



Приложение №2
УТВЕРЖДЕН

Постановлением
Исполнительного
комитета Актанышского муниципального
района от « 17 » 02 2020г.
№ 11Р-23

ПРАВИЛА

обеспечения безопасности персональных данных при их
обработке в Государственной информационной системе
Республики Татарстан
«Бухгалтерский учет и отчетность государственных органов
Республики Татарстан и подведомственных им учреждений»

СОДЕРЖАНИЕ

	Страница
Используемые сокращения	14
Термины и определения	15
1. Общие положения	16
2. Права и обязанности работников	16
3. Требования к получению персональных данных	16
4. Требования к организации работы с документами и другими материальными носителями, содержащими персональные данные	17
5. Требования к местам размещения оборудования и технических средств обработки, хранения и передачи персональных данных	19
6. Требования к условиям хранения персональных данных	19

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Полное наименование
Система	Государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»
ОГВ	Орган государственной власти Республики Татарстан
ОМС	Орган местного самоуправления Республики Татарстан
ПДн	Персональные данные
ТС	Техническое средство

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Закон - Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту ПДн;

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

ПДн - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных, и (или) в результате которых уничтожаются материальные носители персональных данных.

1. Общие положения

1.1. Данный документ содержит правила обеспечения безопасности ПДн при их обработке в Системе.

1.2. Данные Правила устанавливают следующие требования при обработке персональных данных:

- требования к получению ПДн;
- требования к организации работы с документами и другими материальными носителями, содержащими ПДн;
- требования к местам размещения оборудования и ТС обработки, хранения и передачи ПДн;
- требования к условиям хранения ПДн.

1.3. Требованиями данных Правил должны руководствоваться все пользователи Системы, которые осуществляют обработку ПДн.

2. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ

2.1. На пользователей Системы возлагаются обязанности по соблюдению положений организационно-распорядительной документации в части обеспечения защиты ПДн в рамках Системы в части их касающейся.

2.2. Дополнительные обязанности пользователей Системы, возникающие в связи с защитой и обработкой ими ПДн, включаются в их должностные инструкции.

2.3. Контроль за исполнением положений должностных инструкций, регулирующих обеспечение безопасности, производится в порядке, установленном ОГВ и ОМС.

2.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут ответственность в соответствии с федеральными законами.

3. ТРЕБОВАНИЯ К ПОЛУЧЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. При получении ПДн непосредственно у субъектов ПДн пользователи Системы должны обеспечить условия, не допускающие необоснованного раскрытия ПДн третьим лицам, в том числе:

- не произносить ПДн вслух при заполнении типовых форм, вводе данных в Систему, проверке достоверности предоставленных субъектом сведений на основании документов, удостоверяющих личность;

- не оставлять заполненные типовые формы на рабочих столах в свое отсутствие и при приеме третьих лиц.

3.2. При получении ПДн у третьих лиц пользователи Системы должны руководствоваться документом «Регламент обеспечения безопасности персональных данных при взаимодействии с контрагентами, третьими лицами».

4. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ РАБОТЫ С ДОКУМЕНТАМИ И ДРУГИМИ МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

4.1. Работа с документами и другими материальными носителями, содержащими ПДн, должна осуществляться пользователями Системы в соответствии с действующим порядком конфиденциального делопроизводства.

4.2. Дополнительно к действующему порядку конфиденциального делопроизводства законодательством¹ накладываются ограничения на оформление, ведение и использование документов и других материальных носителей, содержащих ПДн:

- правила учета материальных носителей ПДн;
- правила использования типовых форм документов;
- требования к фиксации ПДн на материальных носителях;
- порядок ведения журналов (реестров, книг), содержащих ПДн;
- правила уничтожения носителей ПДн.

4.3. При работе с материальными носителями ПДн пользователи Системы должны быть выполнены следующие условия:

4.3.1. Все машинные материальные носители, содержащие ПДн, должны быть учтены.

4.3.2. Учет машинных материальных носителей, содержащих ПДн, должны осуществлять руководители структурных подразделений Департамента казначейства Министерства финансов Республики Татарстан, ОГВ, ОМС в Журнале учета машинных носителей ПДн (далее - Журнал). Форма Журнала приведена в приложении к настоящим Правилам (приложение 1). Журнал может вестись в нескольких экземплярах.

4.3.3. Передача материальных носителей ПДн сторонним организациям должна осуществляться в соответствии с документом «Регламент обеспечения

¹ Постановление Правительства РФ от 15 сентября 2008 г. № 687 и Постановление Правительства РФ № 1119 от 1

информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами».

4.4. При фиксации ПДн на материальных носителях должны соблюдаться следующие условия:

4.4.1. ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

4.4.2. На одном материальном носителе не допускается фиксация ПДн, цели обработки которых заведомо не совместимы.

4.4.3. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

4.4.4. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению отдельной обработки ПДн.

4.5. При необходимости уничтожения ПДн и/или носителей ПДн должны соблюдаться следующие условия:

4.5.1. Внешние носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. При этом при необходимости предварительно осуществляется копирование сведений, не подлежащих уничтожению.

4.5.2. По истечении срока согласия субъекта на обработку его ПДн, персональные данные уничтожаются.

4.5.3. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.5.4. Уничтожение ПДн производится по акту комиссией не менее трех человек. Форма акта об уничтожении ПДн приведена в приложении к настоящим Правилам (приложение 2).

5. ТРЕБОВАНИЯ К МЕСТАМ РАЗМЕЩЕНИЯ ОБОРУДОВАНИЯ И ТЕХНИЧЕСКИХ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Доступ на территорию объекта должен осуществляться в соответствии с документами, регламентирующими организацию пропускного и внутриобъектного режима ОМС.

5.2. Места размещения оборудования и ТС обработки, хранения и передачи ПДн должны выбираться так, чтобы исключить или существенно уменьшить возможность несанкционированного доступа к ним и воздействия на них окружающей среды.

5.3. Оборудование, по возможности, должно размещаться в помещениях, имеющих достаточную площадь. При расположении оборудования на первом этаже окна данных помещений должны быть оборудованы решетками или другими устройствами, исключающими бесконтрольный доступ в помещения через окна.

5.4. Доступ лиц в помещения с оборудованием, предназначенным для обработки ПДн, должен быть ограничен и обеспечиваться в соответствии со служебной необходимостью.

6. ТРЕБОВАНИЯ К УСЛОВИЯМ ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок хранения носителей ПДн определяется ответственным лицом за организацию обработки ПДн в соответствии с законодательством Российской Федерации.

Приложение № 2 к Правилам обеспечения безопасности персональных данных при их обработке в Государственной информационной Системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»

УТВЕРЖДАЮ
Руководитель подразделения

(должность)

(фамилия и инициалы)

« ____ » _____ 20__ г.

**Акт
об уничтожении персональных данных**

(место составления)

(дата)

Нами,

(должность, ФИО работников, проводивших уничтожение)

в присутствии

(должность, ФИО работников, присутствовавших при уничтожении)

составлен акт о нижеследующем:

« ____ » _____ 20__ г. нами было произведено уничтожение персональных данных следующих документов(дел):

№ п/п	Название (краткое содержание) документа	№ по журнал у учета	Кол-во листов	Способ уничтожения	Причина уничтожения	Примечание
1	2	3	4	5	6	7
1.	Дело (наименование)	11	150	Путем сожжения	Утрата актуальности	Дело (наименование)
2.						
3.						

носителей персональных данных:

п/п	носителя	по журналу учета		уничтожения	ие
1	2	3	4	5	6
1.	Дискета	22	Путем сожжения (излома)	Выход из строя	Дискета
2.					
3.					

(При необходимости указать дальнейшие действия с не уничтоженными документами, носителями, например, передача в архив на хранение).

Всего документов, носителей _____

(цифрами и прописью)

Документы уничтожены _____

(дата)

ФИО работников, проводивших уничтожение

(подпись, инициалы и фамилия)

ФИО работников, проводивших уничтожение

(подпись, инициалы и фамилия)

ФИО работников, проводивших уничтожение

(подпись, инициалы и фамилия)

ФИО работников, проводивших уничтожение

(подпись, инициалы и фамилия)

Дата подписания « ____ » _____ 20 ____ г.



Приложение №3

УТВЕРЖДЕН
Постановлением
комитета
муниципального

Исполнительного
Актанышского
района от

« 17 » 02 2020г. № ПР-23

РЕГЛАМЕНТ
выгрузки и передачи персональных данных в
Государственной информационной системе Республики Татарстан «Бухгалтерский
учет и отчетность государственных органов Республики Татарстан и
подведомственных им учреждений»

СОДЕРЖАНИЕ

	Страница
Используемые сокращения	25
Термины и определения	26
1. Общие положения	27
2. Права и обязанности работников	27
3. Обеспечение безопасности персональных данных при их выгрузке на носители и последующей передаче	28

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Полное наименование
Система	Государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»
ИБ	Информационная безопасность
Орган	Органы государственной власти / Органы местного самоуправления
ПДн	Персональные данные

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Закон - Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

Информационная система персональных данных - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту ПДн;

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

Ответственный за обеспечение безопасности ПДн - структурное подразделение Органа, ответственное за обеспечение безопасности ПДн;

Передача персональных данных - доведение ПДн до уполномоченного представителя контрагента или третьего лица каким-либо образом (передача, пересылка, ознакомление, осуществление доступа);

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту ПДн);

Распространение персональных данных - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Уточнение персональных данных - корректировка ПДн, обрабатываемых в организации, которая производится в случае недостоверности обрабатываемых данных или в случае их изменения.

1. Общие положения

1.1. Настоящий документ устанавливает порядок обеспечения безопасности ПДн и выполнение положений Закона при осуществлении выгрузки ПДн из Системы.

1.2. Требования настоящего Регламента распространяются на Органы, в которых работают пользователи Системы.

1.3. При осуществлении выгрузки ПДн с целью обмена (передачи) ПДн между Органами и контрагентами/третьими лицами следует руководствоваться документом «Регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами».

1.4. Данный Регламент охватывает случаи осуществления выгрузки ПДн на бумажные носители.

1.5. Вывод ПДн на машинные носители (например, USB-флэш диски, DVD/CD диски) запрещен.

2. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ

2.1. В рамках обеспечения ИБ при выгрузке и передаче ПДн выделяются следующие роли:

– руководители структурных подразделений, в которых работают пользователи;

– пользователи.

2.2. На руководителей структурных подразделений органов, осуществляющих обработку ПДн, возлагаются следующие обязанности:

1) проведение инструктажа пользователей Системы (под роспись в «Журнале проведения инструктажа»), для ознакомления со следующими документами:

– регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;

– правила обеспечения безопасности персональных данных при их обработке;

– политика подсистемы разграничения доступа;

– настоящий Регламент;

2) ознакомление пользователей Системы с перечнем обрабатываемых ими ПДн на основании документа «Перечень персональных данных подлежащих защите»;

3) учет работников своего подразделения, допущенных к обработке ПДн Системы;

4) обеспечение выполнения пользователями Системы требований документов:

- регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;
- правила обеспечения безопасности персональных данных при их обработке;
- политика подсистемы разграничения доступа;
- настоящий Регламент.

2.3. На пользователей, обрабатывающих ПДн в рамках Системы, возлагаются обязанности по соблюдению положений организационно-распорядительной документации для обеспечения защиты ПДн в рамках Системы в части их касающейся.

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ВЫГРУЗКЕ НА НОСИТЕЛИ И ПОСЛЕДУЮЩЕЙ ПЕРЕДАЧЕ

3.1. Обеспечение безопасности ПДн при их выгрузке на материальные носители достигается за счет реализации описанного ниже порядка.

3.2. Пользователь Системы осуществляет выгрузку ПДн на материальный носитель и передает полученные материальные носители на согласование руководителю соответствующего структурного подразделения Органа.

3.3. На передаваемых материальных носителях проставляется отметка «Конфиденциально», либо «Для служебного пользования» согласно действующим в Органе порядком конфиденциального делопроизводства.

3.4. При работе с материальными носителями ПДн пользователями Системы должны быть выполнены следующие условия:

3.4.1. Передача материальных носителей ПДн между пользователями одного структурного подразделения Органа осуществляется в соответствии с действующим в Органе порядком конфиденциального делопроизводства.

3.4.2. Передача материальных носителей ПДн вручную (почтой, курьером или лично уполномоченным представителям контрагентов и третьих лиц), контрагентам или третьим лицам осуществляется только по поручению руководителя Органа в соответствии с документом «Регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами».

3.5. При необходимости уничтожения материальных носителей ПДн должны

3.5.1. Материальные носители ПДн, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

3.5.2. По истечении срока согласия субъекта на обработку его ПДн, ПДн уничтожаются.

3.5.3. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.6. Все материальные носители, содержащие ПДн, должны храниться в специально выделенных служебных помещениях или в запираемых и опечатываемых шкафах (хранилищах). При этом должны быть созданы необходимые условия, обеспечивающие их физическую сохранность.

3.7. При выходе пользователя из служебного помещения материальные носители должны быть убраны в хранилища.

3.8. Хранение материальных носителей ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки. По достижении целей обработки или в случае утраты необходимости в их достижении ПДн подлежат уничтожению, за исключением случаев, предусмотренных законодательством Российской Федерации.

3.9. Все ПДн (материальные носители), обработка которых осуществляется в различных целях, должны храниться отдельно.

3.10. Хранение и выдачу носителей ПДн организуют руководители структурных подразделений Органов, в которых работают пользователи.

3.11. Документы, содержащие ПДн субъектов ПДн, должны храниться в течение срока, определенного в согласии субъектов на обработку его ПДн.

Приложение №4

УТВЕРЖДЕН

Постановлением Исполнительного
комитета Актамышского

муниципального района от

« ____ » _____ 2020г. № ____

РЕГЛАМЕНТ

обеспечения информационной безопасности персональных данных при
взаимодействии с контрагентами и третьими лицами при работе
в Государственной информационной системе Республики Татарстан
«Бухгалтерский учет и отчетность государственных органов Республики Татарстан и
подведомственных им учреждений»

СОДЕРЖАНИЕ

	Страница
Используемые сокращения	32
Термины и определения	33
1. Общие положения	34
2. Обязанности и ответственность работников	34
3. Обеспечение безопасности персональных данных при их предоставлении в случаях угрозы жизни и здоровью	36
4. Обеспечение безопасности персональных данных при обмене в случаях, установленных федеральными законами	36
5. Обеспечение безопасности персональных данных при обмене персональными данными в рамках заключенных договоров	37
6. Обеспечение безопасности персональных данных при передаче персональных данных	38
7. Обеспечение безопасности персональных данных при получении персональных данных	39
8. Предоставление контрагентам доступа к информационной системе персональных данных	40
9. Контроль за поддержанием информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами	42
Приложение 1	44
Приложение 2	45
Приложение 3	46
Приложение 4	47

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Полное наименование
Департамент	Департамент казначейства Министерства финансов Республики Татарстан
Система	Государственная информационная система Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»
ИБ	Информационная безопасность
МЦР ГУ ИТС РТ	Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан
Орган	Органы государственной власти/Органы местного самоуправления/Подведомственные учреждения
ПДн	Персональные данные
ППО	Прикладное программное обеспечение

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Закон - Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;

Информационная система персональных данных - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств;

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту ПДн;

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

ПДн - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

Ответственный за обеспечение безопасности ПДн - структурное подразделение Департамента, структурное подразделение Органа, специалист, ответственный за обеспечение безопасности ПДн;

Передача ПДн - доведение ПДн до уполномоченного представителя контрагента или третьего лица каким-либо образом (передача, пересылка, ознакомление, осуществление доступа);

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных, и (или) в результате которых уничтожаются материальные носители персональных данных;

Распространение персональных данных - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

Сервисная организация - организация, осуществляющая на договорной основе оказание услуг по предоставлению ИТ-сервисов, обслуживанию ИТ-инфраструктуры, обеспечению информационной безопасности Системы и имеющая

Уточнение ПДн - корректировка ПДн, обрабатываемых в организации, которая производится в случае недостоверности обрабатываемых данных или в случае их изменения.

1. Общие положения

1.1. Настоящий документ устанавливает порядок обеспечения ИБ ПДн в Системе и выполнения положений Закона при взаимодействии с контрагентами и третьими лицами.

1.2. Данный Регламент охватывает следующие случаи взаимодействия с контрагентами и третьими лицами в процессе обработки ПДн:

- обмен ПДн с контрагентами и третьими лицами;
- предоставление доступа к Системе контрагентам и третьим лицам.

1.3. Обмен ПДн между Департаментом, Органом и контрагентами и третьими лицами может происходить в случаях, установленных законодательством Российской Федерации, с соблюдением установленных норм защиты ПДн.

2. ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ

2.1. В рамках обеспечения ИБ ПДн при взаимодействии с контрагентами и третьими лицами выделяются следующие роли:

руководители структурных подразделений, в которых работают пользователи Системы;

ответственный за обеспечение безопасности ПДн;

администратор ППО (администратор пользователей учреждения);

администратор безопасности (СИС админ);

пользователи.

2.2. На ответственных за обеспечение безопасности ПДн в Органах, осуществляющих обработку ПДн, возлагаются следующие обязанности:

1) проведение инструктажа пользователей Системы (под роспись в «Журнале проведения инструктажа») для ознакомления со следующими документами:

- правила обеспечения безопасности персональных данных при их обработке;
- регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;
- регламент выгрузки и передачи персональных данных;

2) учет работников своего подразделения, допущенных к обработке ПДн Системы;

3) обеспечение выполнения пользователями Системы требований документов:

- правила обеспечения безопасности персональных данных при их обработке;
- регламент обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами;
- регламент выгрузки и передачи персональных данных.

2.3. На ответственного за обеспечение безопасности ПДн Системы возлагаются следующие обязанности:

- планирование и координация работ по обеспечению безопасности ПДн Системы;
- контроль за реализацией организационных и технических мер обеспечения информационной безопасности ПДн Системы;
- контроль за выполнением пользователями, обрабатывающими ПДн в рамках Системы, установленных правил по их защите ПДн при обработке;
- организация технической реализации требований по защите ПДн Системы.

2.4. В рамках деятельности по обеспечению безопасности ПДн на администраторов ППО возлагаются обязанности по обеспечению сопровождения и системного администрирования ППО, а также по предоставлению доступа пользователям к Системе.

2.5. В рамках деятельности, обязанность по контролю за соблюдением мер по защите ПДн при их обработке возлагается на ответственного за обеспечение безопасности ПДн Системы.

2.6. На пользователей, обрабатывающих ПДн в рамках Системы, возлагаются обязанности по соблюдению положений организационно-распорядительной документации в части обеспечения защиты ПДн в рамках Системы в части их касающейся.

2.7. Обязанности пользователей Системы, возникающие в связи с защитой и обработкой ими ПДн, включаются в их должностные регламенты, инструкции.

2.8. Контроль за исполнением положений должностных регламентов, инструкций, регулирующих обеспечение безопасности, производится в порядке, определённом Органом.

2.9. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, несут ответственность в соответствии с законодательством.

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ПРЕДОСТАВЛЕНИИ В СЛУЧАЯХ УГРОЗЫ ЖИЗНИ И ЗДОРОВЬЮ

3.1. В случае если передача ПДн контрагентам и третьим лицами необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно, руководители Органов могут принять решение о передаче ПДн².

3.2. Ответственный за обеспечение безопасности ПДн производит идентификацию лица, получающего ПДн, по документу, удостоверяющему личность, и служебному удостоверению (при наличии), а также записывает контактную информацию данного лица.

3.3. Ответственный за обеспечение безопасности ПДн получает расписку в получении данных. В расписке указываются ФИО, состав полученных ПДн, дата получения, сведения о документе, удостоверяющем личность.

3.4. После получения расписки предоставление ПДн осуществляется в произвольной форме.

3.5. В течение суток после предоставления ПДн пользователем Системы, предоставившим данные, совместно с руководителем своего структурного подразделения вносится запись в Журнал. Типовая форма Журнала приведена в приложении 4 к настоящему Регламенту.

При этом в поле «Основание для передачи ПДн» указывается причина передачи «угроза жизни или здоровью», а в поле «Дата и подпись лица, получившего данные/отметка о подтверждении получения» указывается «Расписка прилагается». Расписка в получении данных хранится в Органе, в которых работают пользователи Системы.

3.6. Руководитель структурного подразделения пользователя Системы, предоставившего персональные данные, уведомляет ответственного за обеспечение безопасности ПДн Системы о факте передачи ПДн.

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБМЕНЕ В СЛУЧАЯХ, УСТАНОВЛЕННЫХ ФЕДЕРАЛЬНЫМИ ЗАКОНАМИ

4.1. В случае если необходимость обмена ПДн установлена законодательством Российской Федерации, необходимый порядок обмена определяется соответствующим Органом.

4.2. Обмен ПДн с Органами, в указанном в п.4.1. настоящего раздела случае, осуществляют соответствующие структурные подразделения Департамента, Органа, в которых работают пользователи Системы.

4.3. В случае если в соответствии с законодательством Российской Федерации ПДн не подлежат ежегодному или ежемесячному предоставлению, но запрашивающий орган обладает в соответствии с законодательством необходимыми полномочиями для запроса и получения ПДн, указанный орган направляет письменный запрос на получение данных сведений руководству Департамента, Органу.

4.4. Запрос должен быть оформлен на официальных бланках с подписью руководителей запрашивающих Органов и должен содержать указание цели и правовое основание требования ПДн, если иное не установлено Федеральными законами. Запрос также может содержать описание порядка (формы, сроки и способы) передачи ПДн.

4.5. При принятии решения об удовлетворении запроса руководителем Органа осуществляется предоставление ПДн в соответствии с разделами 7, 8 настоящего Регламента.

4.6. Руководитель структурного подразделения, в котором работают пользователи Системы, уведомляет ответственного за обеспечение безопасности ПДн Системы о факте передачи ПДн.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБМЕНЕ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В РАМКАХ ЗАКЛЮЧЕННЫХ ДОГОВОРОВ

5.1. При возникновении необходимости заключения договора об обмене ПДн с контрагентами в Системе обязательным является согласование вопроса с Департаментом и с МЦР ГУ ИТС РТ.

5.2. Обмен ПДн с контрагентами в рамках заключенных договоров через структурные подразделения Органов запрещен.

5.3. В случае если обмен ПДн субъектов ПДн с контрагентами осуществляется на основании договора между Департаментом и контрагентом, условия предоставления ПДн определяются в данном договоре.

5.4. При заключении договора с контрагентом в договор вносятся условия предоставления ПДн и обязательства контрагента по обеспечению безопасности ПДн (в том числе в случае реорганизации или ликвидации организации-

контрагента), а также заключается Соглашение о конфиденциальности с контрагентами, которым передаются ПДн.

5.5. Условия предоставления ПДн и обязательства контрагента по обеспечению безопасности ПДн, включаемые в состав договора, согласовываются с ответственным за обеспечение безопасности ПДн Системы.

5.6. Передача (получение) ПДн осуществляется в соответствии с разделами 7, 8 настоящего Регламента.

6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Передача ПДн осуществляется на материальном носителе или в электронном виде по каналам связи ответственным за работу с ПДн в Органе по решению руководителя Органа.

6.2. Передача ПДн на материальном носителе осуществляется в следующем порядке:

6.2.1. Департамент, Орган, в котором работают пользователи Системы, проставляют на передаваемых документах, содержащих ПДн, отметку «конфиденциально», либо «Для служебного пользования». Передача документов осуществляется сопроводительным письмом с уведомлением контрагента или третьего лица о конфиденциальности передаваемых данных, а также с запросом на подтверждение получения передаваемых данных. (Рекомендуемая форма сопроводительного письма приведена в приложении 1 к настоящему Регламенту);

6.2.2. Сопроводительное письмо подписывается руководителем Органа либо его заместителем и прикладывается к передаваемому материальному носителю;

6.2.3. Материальный носитель запаковывается в соответствии с действующим порядком конфиденциального делопроизводства;

6.2.4. Передача материальных носителей, содержащих ПДн, осуществляется почтовой связью (пересылка заказными либо ценными почтовыми отправлениями), курьерской связью или передается лично уполномоченным представителям контрагентов и третьих лиц;

6.2.5. При передаче материальных носителей, содержащих ПДн, уполномоченным представителям контрагентов и третьих лиц Орган, в котором работают пользователи Системы, предварительно производят идентификацию уполномоченного представителя по документу, удостоверяющему личность;

6.2.6. После передачи материального носителя Орган, в котором работают пользователи Системы, вносят запись в Журнал. Форма Журнала приведена в приложении 4 к настоящему Регламенту;

6.2.7. После получения подтверждения о получении ПДн в Журнал (Приложение 4 к настоящему Регламенту) вносится запись о подтверждении (при передаче материального носителя на территории Органа запись о подтверждении вносится непосредственно при передаче).

6.3. Передача ПДн в электронном виде по каналам связи осуществляется в следующем порядке:

6.3.1. Передача информации в электронном виде по каналам связи осуществляется в соответствии с принятым порядком защищенного информационного обмена между организациями, которые должны обеспечивать защиту ПДн от несанкционированного доступа;

6.3.2. При передаче ПДн в электронном виде по каналам связи Департамента, Орган, в котором работают пользователи Системы, направляет сопроводительное письмо, уведомляющее контрагента или третье лицо о конфиденциальности передаваемых данных, а также содержащее запрос на подтверждение получения передаваемых данных. Рекомендуемая форма сопроводительного письма приведена в приложении 1 к настоящему Регламенту;

6.3.3. Передача ПДн в электронном виде пользователями Системы осуществляется через защищенные каналы связи;

6.3.4. После отправки и получения подтверждения о получении ПДн Орган, в котором работают пользователи Системы, вносят соответствующую запись в Журнал. Типовая форма Журнала приведена в приложении 4 к настоящему Регламенту.

7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПОЛУЧЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Получение ПДн от контрагентов и третьих лиц осуществляется через структурное подразделение, ответственное за конфиденциальное делопроизводство в Органе. Получение ПДн от контрагентов и третьих лиц через иные структурные подразделения Органа запрещено.

7.2. Получение материальных носителей ПДн производится в соответствии с действующим порядком конфиденциального делопроизводства Органа.

7.3. При получении от контрагентов или третьих лиц файловых массивов, содержащих ПДн, ответственный за обеспечение безопасности ПДн принимает решение о сроках, месте и способах обработки полученных данных (в том числе о необходимости обработки ПДн в Системе).

7.4. В случае если ответственный за обеспечение безопасности ПДн принял решение о необходимости обработки полученных ПДн в Системе, и категории и объем полученных данных соответствуют уровням защищенности системы, ПДн загружаются в Систему.

7.5. В случае если ответственный за обеспечение безопасности ПДн от учреждения принял решение о необходимости обработки полученных ПДн в Системе, но категории и объем полученных данных не соответствуют уровню защищенности системы, ответственный за обеспечение безопасности ПДн также принимает решение о принятии мер по приведению их в соответствие, в том числе:

- меры по повышению уровня защищенности Системы и соответствующей ее защите;

- меры по снижению категории или объема ПДн путем редактирования, обезличивания или сегментирования полученных файловых массивов.

7.6. Применяемые меры и средства защиты информации должны обеспечивать соответствие Системы требованиям норм и стандартов в области обеспечения ИБ. Соответствие нормам и стандартам ИБ должно быть подтверждено оценкой соответствия в форме аттестации на соответствие требованиям ИБ.

7.7. Ответственный за обеспечение безопасности ПДн от учреждения определяет ответственных за реализацию данных мер, в том числе в рамках действующих договоров с сервисными организациями.

7.8. Загрузку ПДн в Систему осуществляют администраторы Системы в соответствии с эксплуатационной документацией на систему.

8. ПРЕДОСТАВЛЕНИЕ КОНТРАГЕНТАМ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Предоставление доступа к Системе осуществляется на основании договора, заключенного между Департаментом, МЦР ГУ ИТС РТ и контрагентом, в котором определяются условия предоставления доступа к ПДн.

8.2. При заключении договора с контрагентом в договор вносятся условия предоставления доступа к Системе и обязательства контрагента по обеспечению безопасности ПДн (в том числе в случае реорганизации или ликвидации

организации-контрагента), а также заключается Соглашение о конфиденциальности с контрагентами, которые могут получить доступ к ПДн.

8.3. Предоставление представителям контрагентов доступа к Системе осуществляется на основании письма контрагента, которому необходимо предоставить доступ. В письме указываются координаты ответственного лица контрагента.

8.4. На основании заключенного договора, указанного в п.8.1. настоящего раздела, ответственный за обеспечение безопасности ПДн вносит данные о контрагенте в Список контрагентов и третьих лиц, имеющих доступ к Системе (далее - Список) (форма Списка представлена в приложении 2 к настоящему Регламенту).

8.5. Список контрагентов и третьих лиц, имеющих доступ к Системе, хранится у ответственного за обеспечение безопасности ПДн от учреждения или назначенного им ответственного лица. Данный список передается системному администратору, отвечающему за техническую эксплуатацию Системы.

8.6. Предоставление доступа к Системе контрагентам и третьим лицам осуществляется в следующем порядке:

8.6.1. Администратор ППО проверяет, существует ли техническая возможность предоставления доступа;

8.6.2. В случае если такая возможность существует, администратор ППО формирует технические условия и требования, при которых возможно предоставление прав доступа. Данные условия и требования должны распространяться на Стороны заключенного договора;

8.6.3. Требования и технические условия определяются для каждого конкретного случая, но в общем случае должны включать:

- необходимые технические условия (требования к параметрам соединений, необходимая конфигурация и настройки оборудования, требования к средствам защиты информации, требование отсутствия подключения к другим сетям или меры по защите, применяемые при подключении и т.д.);

- требования по защите информации, которые должны соблюдаться организацией-контрагентом;

- разграничение ответственности между организациями;

8.6.4. Определенные требования и технические условия согласовываются с ответственным за обеспечение безопасности ПДн от учреждения в Системе;

8.6.5. Администратор ППО направляет в письменном или электронном виде контрагенту письмо с подтверждением положительного решения о предоставлении

доступа. Письмо также должно включать сформированные требования и технические условия, координаты ответственного лица от Департамента;

8.6.6. Реализацию технических условий внутри Системы обеспечивает администратор ППО в рамках своих полномочий;

8.6.7. После выполнения всех необходимых действий, определенных в требованиях и технических условиях, администратор ППО предоставляет контрагенту все необходимые права доступа;

8.6.8. При необходимости администратор ППО представляет контрагенту реквизиты, необходимые для доступа.

9. КОНТРОЛЬ ЗА ПОДДЕРЖАНИЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВЗАИМОДЕЙСТВИИ С КОНТРАГЕНТАМИ И ТРЕТЬИМИ ЛИЦАМИ

9.1. Контроль за поддержанием ИБ при взаимодействии с контрагентами и третьими лицами осуществляет ответственный за обеспечение безопасности ПДн от учреждения. На него при взаимодействии с контрагентами и третьими лицами возложена ответственность по контролю за:

- организацией учета всех передаваемых и получаемых ПДн (п.9.2. настоящего раздела);

- включением в договоры с контрагентами и третьими лицами обязательств по защите ПДн (п.9.3. настоящего раздела);

- соблюдением порядка предоставления доступа к Системе (п.9.4. настоящего раздела).

9.2. Контроль за организацией учета всех передаваемых и получаемых ПДн осуществляется на плановой основе:

9.2.1. Ответственный за обеспечение безопасности ПДн ежегодно выполняет анализ Журналов на предмет проверки правильности и полноты их заполнения;

9.2.2. В случае выявления некорректности заполнения Журналов ответственным за обеспечение безопасности ПДн вносится запись об этом в Журнал учета нарушений. Форма Журнала учета нарушений приведена в приложении 3 к настоящему Регламенту.

9.3. Контроль за включением в договоры с контрагентами и третьими лицами обязательств по защите ПДн:

9.3.1. Ответственный за обеспечение безопасности ПДн при заключении договоров контролирует внесение в них обязательств контрагента по обеспечению безопасности ПДн, а также заключение Соглашения о конфиденциальности.

9.4.1. Администраторы безопасности ежедневно просматривают журналы регистрации событий Системы с целью выявления записей, свидетельствующих о несанкционированном предоставлении (изменении) прав доступа контрагентам;

9.4.2. В случае обнаружения несанкционированных изменений администратор безопасности вносит запись в Журнал учета нарушений, сообщает Ответственному за обеспечение безопасности ПДн о нарушениях и принимает необходимые меры по их устранению;

9.4.3. В случае обнаружения фактов несанкционированного предоставления (изменения) прав доступа контрагентам администратор безопасности информирует ответственного за обеспечение безопасности ПДн.

Приложение 1

к Регламенту обеспечения
информационной безопасности
персональных данных при
взаимодействии с контрагентами и
третьими лицами при работе в
Государственной информационной
системе Республики Татарстан
«Бухгалтерский учет и отчетность
государственных органов Республики
Татарстан и подведомственных им
учреждений»

Сопроводительное письмо.

В ответ на Ваш запрос от _____ 20__ г. (на основании Договора №
___ от _____ в Ваш адрес направляю персональные данные о

(прилагаются).

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О
персональных данных» передаваемая Вам информация является
конфиденциальной.

В соответствии с действующим законодательством Российской Федерации
на Вас возлагаются обязательства по обеспечению безопасности персональных
данных (в том числе по недопущению их незаконного распространения) с даты
предоставления их Вам.

Просим подтвердить получение Вами переданных сведений в письменной
форме.

(наименование должности
Органа)

(подпись)

(ФИО) должностного лица

Приложение 2
к Регламенту обеспечения информационной безопасности персональных данных при взаимодействии с контрагентами и третьими лицами при работе в Государственной информационной системе Республики Татарстан «Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений»

Список
контрагентов и третьих лиц, имеющих доступ к Государственной информационной системе
Республики Татарстан «Бухгалтерский учет и отчетность государственных органов
Республики Татарстан и подведомственных им учреждений»

№ п/п	Наименование Органа	Цель доступа в Систему	Перечень модулей (информации) Системы, к которым предоставляется доступ	Примечание	Дата и подпись Должностного лица

Приложение 3
к Регламенту обеспечения
информационной безопасности
персональных данных при
взаимодействии с контрагентами и
третьими лицами при работе в
Государственной информационной
системе Республики Татарстан
«Бухгалтерский учет и отчетность
государственных органов
Республики Татарстан и
подведомственных им учреждений»

**ЖУРНАЛ УЧЕТА
НАРУШЕНИЙ ПОРЯДКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «БУХГАЛТЕРСКИЙ УЧЕТ И
ОТЧЕТНОСТЬ ГОСУДАРСТВЕННЫХ ОРГАНОВ РЕСПУБЛИКИ ТАТАРТАН И
ПОДВЕДОМСТВЕННЫХ
ИМ УЧРЕЖДЕНИЙ»**

Начат «__» _____ 20__ г.

Окончен «__» _____ 20__ г.

№ п/п	Дата выявления нарушения	ФИО и подпись работника, выявившего нарушение	Описание нарушения	Предпринятые действия	Примечание

