АДМИНИСТРАЦИЯ ТАЗОВСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ

30 июля 2021 года № 297-р

п. Тазовский

О внесении изменений в распоряжение Администрации Тазовского района № 171-р от 22 июля 2020 года

В целях обеспечения безопасности персональных данных при их обработке в информационных системах обработки персональных данных, в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152 «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», руководствуясь статьей 44 Устава муниципального округа Тазовский район Ямало-Ненецкого автономного округа:

1. Утвердить прилагаемые изменения, которые вносятся в распоряжение Администрации Тазовского района № 171-р от 22 июля 2020 года «Об утверждении перечня мер по защите информации, содержащейся в информационных системах персональных данных Администрации Тазовского района» согласно приложению.

2. Контроль за исполнением настоящего распоряжения возложить на заместителя Главы Администрации Тазовского района по внутренней политике.

Управление делами

Глава Тазовского района В.П. Паршаков

УТВЕРЖДЕНЫ

распоряжением
Администрации Тазовского района
от 30 июля 2021 года № 297-р

ИЗМЕНЕНИЯ,
которые вносятся в распоряжение
Администрации Тазовского района № 171-р от 22 июля 2020 года

1. Приложения № 1, 2, 5, 6 признать утратившими силу.
2. Приложение № 3 изложить в следующей редакции:

«

Приложение № 3

УТВЕРЖДЕНО
распоряжением
Администрации Тазовского района
от 22 июля 2020 года № 171-р
(в редакции распоряжения
Администрации Тазовского района
от 30 июля 2021 года № 297-р)

ПЕРЕЧЕНЬ
администраторов безопасности и операторов
информационных систем персональных данных

№ п/п	Информационная система персональных данных (далее - ИСПДн)	Администратор безопасности системы	Оператор системы
1	2	3	4
1.	Сегмент СЭДД «Company Media 4.5» Обращение граждан ЯНАО	ведущий инженер-программист отдела информационных технологий Администрации Тазовского района	первый заместитель Главы Администрации Тазовского района; заместитель Главы Администрации Тазовского района по внутренней политике; заместитель Главы Администрации Тазовского района по социальным вопросам; заместитель Главы Администрации

1	2	3	4
			Тазовского района; начальник управления делами Администрации Тазовского района; начальник отдела делопроизводства управления делами Администрации Тазовского района; заведующий сектором по работе с обращениями граждан управления делами Администрации Тазовского района; секретарь руководителя отдела контроля и организационной работы управления делами Администрации Тазовского района; помощник руководителя отдела контроля и организационной работы управления делами Администрации Тазовского района
2.	«Бухгалтерия СМЕТА»	ведущий инженер-программист отдела информационных технологий Администрации Тазовского района	начальник отдела бухгалтерского учета и отчетности Администрации Тазовского района; главный специалист отдела бухгалтерского учета и отчетности Администрации Тазовского района; экономист отдела бухгалтерского учета и отчетности Администрации Тазовского района; бухгалтер отдела бухгалтерского учета и отчетности Администрации Тазовского района
3.	«Отдел кадров СМЕТА»	ведущий инженер-программист отдела информационных технологий Администрации Тазовского района	начальник отдела кадров Администрации Тазовского района; главный специалист отдела кадров Администрации Тазовского района; специалист по персоналу отдела кадров Администрации Тазовского района
4.	Региональный банк данных семей несовершеннолетних групп особого внимания ЯНАО	ведущий инженер-программист отдела информационных технологий Администрации Тазовского района	начальник отдела по обеспечению деятельности комиссии по делам несовершеннолетних Администрации азовского района; главный специалист отдела по обеспечению деятельности комиссии по делам

1	2	3	4
			несовершеннолетних Администрации Тазовского района; ведущий специалист отдела по обеспечению деятельности комиссии по делам несовершеннолетних Администрации Тазовского района; специалист отдела по обеспечению деятельности комиссии по делам несовершеннолетних Администрации Тазовского района
5.	Автоматизированная информационная система передачи данных службы по делам архивов система электронный архив Ямало-Ненецкого автономного округа отдел по делам архивов Администрации Тазовского района	ведущий инженер-программист отдела информационных технологий Администрации Тазовского района	начальник отдела по делам архивов (муниципального архива) Администрации Тазовского района; главный специалист отдела по делам архивов (муниципального архива) Администрации Тазовского района; специалист отдела по делам архивов (муниципального архива) Администрации Тазовского района
6.	Единое окно цифровой обратной связи Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функции)» ПОС	главный специалист отдела информационных технологий Администрации Тазовского района	специалист сектора по работе с обращениями граждан управления делами Администрации Тазовского района
7.	СМЭВ ЯНАО и Портал ЯНАО	главный специалист отдела информационных технологий Администрации Тазовского района	главный специалист отдела архитектуры и градостроительства Администрации Тазовского района; заведующий сектором информационной системы обеспечения градостроительной деятельности отдела архитектуры и градостроительства Администрации Тазовского района»; начальник отдела по делам архивов (муниципального архива) Администрации Тазовского района; главный специалист отдела по делам архивов (муниципального архива) Администрации Тазовского района;

1	2	3	4
			специалист отдела по делам архивов (муниципального архива) Администрации Тазовского района; главный специалист отдела бухгалтерского учета и отчетности Администрации Тазовского района; заведующий сектором содействия развитию предпринимательства управления социально-экономического развития Администрации Тазовского района
8.	Информационная система передачи данных в Пенсионный фонд Российской Федерации	главный специалист отдела информационных технологий Администрации Тазовского района	специалист по персоналу отдела кадров Администрации Тазовского района
9.	Официальный сайт tasu.ru	компания «СофтМажор» г. Екатеринбург	заведующий сектором по работе с обращениями граждан управления делами Администрации Тазовского района

».

3. Приложение № 4 изложить в следующей редакции:

«

Приложение № 4
УТВЕРЖДЕНО
распоряжением
Администрации Тазовского района
от 22 июля 2020 года № 171-р
(в редакции распоряжения
Администрации Тазовского района
от 30 июля 2021 года № 297-р)

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Тазовского района

I. Основные определения и сокращения

1.1. Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.2. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. Система защиты персональных данных (СЗПДн) – система обеспечения информационной безопасности ПДн.

1.4. Оператор - муниципальный орган, организующий и (или) осуществляющий обработку персональных данных, а также определяющий цели и содержание обработки ПДн.

1.5. Удаленная (дистанционная) работа - выполнение определенной трудовым договором трудовой функции вне места нахождения работодателя, его филиала, представительства, иного обособленного структурного подразделения (включая расположенные в другой местности), вне стационарного рабочего места, территории или объекта, прямо или косвенно находящихся под контролем работодателя, при условии использования для выполнения данной трудовой функции и для осуществления взаимодействия между работодателем и работником по вопросам, связанным с ее выполнением, информационно-телекоммуникационных сетей общего пользования, в том числе сети Интернет.

II. Общие положения

2.1. Настоящее Положение определяет порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн Администрации Тазовского района (далее – Администрация района) и содержит общие принципы защиты ПДн.

2.2. Данный документ направлен на достижение следующих целей:

– выполнение требований законодательства в области обеспечения безопасности ПДн;

– защита прав и свобод граждан Российской Федерации при обработке их ПДн в ИСПДн оператора;

– защита ПДн, обрабатываемых оператором, от НСД и от других несанкционированных действий.

2.3. Требования настоящего Положения распространяются на все отраслевые (функциональные) органы и структурные подразделения Администрации района, которые участвуют в обработке ПДн либо в организации обработки ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования ИСПДн.

2.4. Настоящий документ обязаны знать и использовать в работе все работники Администрации района, а также другие лица, допущенные к работе в ИСПДн.

2.5. Настоящее Положение разработано в соответствии со следующими нормативными актами:

– Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– методическими документами ФСБ России, ФСТЭК России, Роскомнадзора.

2.6. Принципы и требования по обеспечению безопасности ПДн распространяются:

– на все возможные формы существования информации, такие как: физические поля (электрические, акустические, электромагнитные, оптические и т.п.);

– носители на бумажной, магнитной, оптической и иной основе;

– на все возможные форматы представления ПДн.

2.7. Предотвращение несанкционированного и нелегитимного доступа к ИСПДн, технологиям и информационным ресурсам, результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных средств защиты информации (далее – СЗИ).

2.8. Настоящее Положение определяет:

– роли, полномочия, ответственность за обеспечение безопасности ПДн, подразделений оператора;

– порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

– мероприятия по обеспечению безопасности ПДн;

– требования по управлению процессом обеспечения безопасности ПДн.

2.9. Целью создания СЗПДн является исключение неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

2.10. В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

– конфиденциальности ПДн;

– целостности ПДн;

– доступности ПДн;

– неотказуемости.

2.11. К основным задачам в области обеспечения безопасности ПДн относится:

– определение новых ИСПДн;

– инвентаризация и управление изменениями в составе и структуре ИСПДн;

– сбор согласий на обработку ПДн с субъектов ПДн;

– разработка и актуализация Перечня сведений конфиденциального характера;

– уничтожение ПДн;

– управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;

– взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– классификация ИСПДн;

– разработка (актуализация) документации на СЗПДн;

– выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;

– эксплуатация СЗПДн в соответствии с документацией на нее;

– контроль уровня защищенности ПДн;

– обучение персонала по вопросам защиты ПДн;

– учет применяемых СЗИ, эксплуатационной и технической документации к ним, носителей ПДн;

– учет лиц, допущенных к обработке ПДн;

– взаимодействие с регуляторными органами по вопросам защиты ПДн;

– актуализация и подача уведомлений в уполномоченный орган по защите прав субъектов ПДн;

– аттестация (декларирование соответствия) по требованиям безопасности информации;

– получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн.

2.12. Обработка ПДн должна осуществляться в соответствии со следующими принципами:

– законности целей и способов обработки ПДн и добросовестности;

– соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;

– соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

– достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;

– недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

2.13. Оператор должен проводить регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

– создания новых ИСПДн;

– внесения изменений в технологические процессы существующие в ИСПДн;

– изменения нормативной базы затрагивающей принципы и (или) процессы обработки ПДн в ИСПДн оператора;

– проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

2.14. Отнесение сведений оператором к ПДн, безопасность которых должна обеспечиваться СЗПДн, представляет собой процесс обоснованного установления (документального оформления и утверждения) критериев их выделения из всей совокупности сведений, находящихся в обращении.

III. Организационная структура системы защиты персональных данных

3.1. СЗПДн является частью общей системы обеспечения информационной безопасности оператора.

3.2. Ответственным лицом за обработку ПДн в каждом подразделении Администрации района, обрабатывающим ПДН, является руководитель подразделения.

3.3. Основу организационной структуры СЗПДн составляют следующие организационные структуры:

– руководство;

– ответственные за обеспечение безопасности (администраторы безопасности) ПДн;

– сотрудники оператора, участвующие в процессах обработки ПДн.

3.4. Администраторы безопасности ПДн осуществляют следующие основные функции:

– участвуют в проведении классификации ИСПДн;

– распределяют ответственность по вопросам обработки и защиты ПДн;

– организуют подачу уведомлений в уполномоченный орган по защите прав субъектов ПДн;

– организуют работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;

– осуществляют организацию плановых и внеплановых проверочных мероприятий;

– организуют выполнение требований по защите ПДн у оператора;

– проводят разработку и актуализацию локальных нормативных документов, регламентирующих защиту ПДн у оператора;

– проводит ознакомление сотрудников с нормативными документами в области защиты ПДн;

– проводят оценку эффективности принятых мер и применяемых средств защиты ПДн;

– ПДн и технические задания на СЗПДн;

– контролируют выполнение сотрудниками требований по защите ПДн;

– организуют работы по сбору сведений об изменениях в составе и структуре ИСПДн;

– осуществляют контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов по защите ПДн, а также внутренних организационно распорядительных документов оператора;

– контролируют исполнение требований по уничтожению ПДн;

– разрабатывают рекомендации по оптимизации существующих и новых информационных процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;

– контролируют исполнение требований нормативных документов оператора в области обеспечения безопасности ПДн сотрудниками;

– организуют и осуществляют взаимодействие с регуляторами по вопросам защиты ПДн;

– участвуют в аттестации (декларировании соответствия) ИСПДн оператора по требованиям безопасности информации;

– контролируют ввод в действие, эксплуатацию СЗПДн;

– проводят расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных ситуаций;

– осуществляют сопровождение средств и систем защиты ПДн;

– проводят оперативный контроль функционирования средств и систем защиты ПДн;

– проводят резервирование ПДн;

– ведут учет носителей ПДн;

– осуществляют выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;

– контролируют соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и СЗПДн;

3.5. Сотрудники подразделений Администрации района, участвующие в процессах обработки ПДн, выполняют следующие основные функции:

– осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;

– осуществляют уведомление субъектов ПДн в случаях определенных нормативными актами;

– эксплуатируют СЗПДн в соответствии с документацией на нее;

– соблюдают требования нормативных документов по защите ПДн;

– осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

IV. Порядок организации и проведения работ по обеспечению безопасности персональных данных

4.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

4.2. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на оператора.

4.3. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.4. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

4.5. Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ, выполняемых в рамках жизненного цикла ИСПДн, на следующих этапах:

- инициация проекта ИСПДн;
- планирование проекта ИСПДн;
- реализация проекта ИСПДн, в составе:
- выбор технического решения - концепция реализации;
- проектирование ИСПДн;
- производство ИСПДн;
- приемка ИСПДн;
- внедрение ИСПДн;
- передача системы в эксплуатацию;
- документирование проекта.
- эксплуатация ИСПДн;
- модернизация ИСПДн;
- вывод из эксплуатации.

V. Допуск персонала к обработке персональных данных

5.1. При допуске к ПДн оператор руководствуется утвержденным списком лиц, допущенных к обработке ПДн.

5.2. Перечень лиц, допущенных к обработке ПДн, составляется и корректируется ответственными за обеспечение безопасности ПДн, на основании данных, подаваемых руководителями структурных подразделений оператора.

VI. Контроль изменений в составе и структуре информационных систем персональных данных

6.1. Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться администраторами безопасности ПДн.

6.2. Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

– изменение мест включения существующих компонент ИСПДн;

– удаление устройства из состава ИСПДн;

– изменение мест установки устройства из состава ИСПДн;

– прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

– создание новых и изменение существующих технологических процессов связанных с обработкой ПДн.

6.3. Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация СЗПДн.

VII. Защита от несанкционированного физического доступа к элементам информационных систем персональных данных

7.1. Мероприятия по физическому контролю доступа включают:

– мероприятия по контролю доступа на территорию;

– мероприятия по контролю доступа в помещения с оборудованием ИСПДн;

– мероприятия по контролю доступа к техническим средствам ИСПДн;

– мероприятия по контролю перемещений физических компонентов ИСПДн.

7.2. Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории оператора.

7.3. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными кодовыми замками или приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

7.4. Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

7.5. Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

7.6. Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не допущенных к обработке ПДн.

7.7. При выносе устройств, хранящих ПДн, за пределы КЗ для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

VIII. Резервирование персональных данных

8.1. Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

8.2. Резервированию должна подвергаться информация на серверах ИСПДн.

8.3. Резервирование должно осуществляться на различные носители информации с соответствующим уровнем надежности и долговечности.

8.4. Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

8.5. Доступ к резервным копиям должен быть строго регламентирован.

IX. Контроль за обеспечением необходимого уровня защищенности персональных данных

9.1. Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

– контроль за соблюдением требований по обработке и защите ПДн;

– контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;

– контроль эффективности средств защиты ПДн.

– Контрольные мероприятия могут быть:
– текущими;
– внезапными;
– плановыми внешними;
– плановыми внутренними.

9.2. Ответственность за текущий контроль эффективности обеспечения безопасности ПДн возлагается на администраторов безопасности ИСПДн.

9.3. Ответственность за плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственных за обеспечение безопасности ПДн.

9.4. Для планового контроля эффективности СЗПДн должны использоваться средства выявления уязвимостей информационной безопасности.

9.5. Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственных за обеспечение безопасности ПДн.

9.6. При проведении контроля эффективности в общем случае должно проверяться:

– наличие установленных СЗИ;
– корректность настроек СЗИ;
– выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;
– исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
– правильность организации работы с носителями ПДн;
– правильность обращения ключевой информации;
– соответствие СЗПДн реальному положению дел у оператора.

X. Обработка персональных данных удаленными (дистанционными) работниками

10.1. Удаленный (дистанционный) доступ к АРМ Администрации Тазовского района работника обрабатывающего персональные данные осуществляется исключительно с использованием технологий построения виртуальной частной сети (далее - VPN) и терминального доступа, определяемыми работниками отдела информационных технологий Администрации Тазовского района (далее - отдел информационных технологий).

10.2. Предоставление учетной записи или ключей шифрования (далее - ключевой набор) для удаленного доступа к АРМ работника осуществляется работниками отдела информационных технологий на основании распоряжения о переводе работника на удаленную (дистанционную) работу.

10.3. Работники отдела информационных технологий проводят проверку:

10.3.1. настройки средств защиты информации от несанкционированного доступа. Вход в операционную систему должен быть разрешен только одной доменной учетной записи работника, закрепленного за данным АРМ, заблокированы подключаемые съемные носители информации и мобильные устройства, установлены требования к сложности пароля и ограничения на возможность неверного ввода пароля не более 5 раз.

10.3.2. Настройки средства криптографической защиты информации и межсетевого экранирования уровня узла. В сетевых фильтрах открытой сети должны быть заблокированы все входящие подключения за исключением протоколов: RDP, ICMP, DHCP, NetBIOS, IGMP. Убедиться, что пользователь не может отключать защиту сетевого трафика и менять настройки сетевых пакетных фильтров.

10.3.3. на отсутствие установленного программного обеспечения (далее - ПО) не входящего в перечень разрешенного к установке.

10.4. Запрещается пересылать ПДн посредством почты и другими способами.

10.5. Работники Администрации на удаленной (дистанционной) работе обязаны соблюдать требования по информационной безопасности установленные в Администрации Тазовского района.

10.6. При обнаружении несанкционированного доступа к персональным данным при удаленной работе работник обязан сообщить об этом в отдел информационных технологий.

10.7. Сотрудники Администрации Тазовского района, которым предоставлен удаленный доступ к АРМ с персональными данными, несут персональную ответственность, предусмотренную трудовым, административным, уголовным законодательством Российской Федерации за нарушения требований информационной безопасности.

XI. Реагирование на нештатные ситуации

11.1. Оператор должен проводить расследования инцидентов, связанных с НСД и другими несанкционированными действиями, затрагивающими безопасность ПДн.

11.2. В рамках данного процесса должны решаться следующие задачи:

– расследование инцидентов, связанных с безопасностью ПДн;

– ликвидация последствий инцидентов, связанных с безопасностью ПДн;

– принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

XII. Заключительные положения

12.1. Требования настоящего Положения обязательны для всех сотрудников, допущенных к обработке персональных данных.».

4. Приложение № 14 изложить в следующей редакции:

«

Приложение № 14

УТВЕРЖДЕНА
распоряжением
Администрации Тазовского района
от 22 июля 2020 года № 171-р
(в редакции распоряжения
Администрации Тазовского района
от 30 июля 2021 года № 297-р)

ИНСТРУКЦИЯ
по порядку учета, хранения и уничтожения персональных данных в Администрации Тазовского района

I. Определения

1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.2. Администратор безопасности информации – работник отдела информационных технологий Администрации Тазовского района, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

1.3. Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

1.4. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.5. Доступность информации – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

1.6. Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

1.7. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.8. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.9. Информация – сведения (сообщения, данные) независимо от формы их представления.

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

1.11. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

1.12. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

1.13. 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 персональных данных.

1.14. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.15. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

1.16. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.17. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

1.18. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

II. Общие положения

2.1. Настоящая инструкция разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении перечня

сведений конфиденциального характера», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.2. Настоящая инструкция устанавливает порядок работы с документами – носителями конфиденциальной информации, содержащей персональные данные, в информационных системах персональных данных (далее – информационная система, ИС) Администрации Тазовского района (далее – Организация), в целях:

– предотвращения неконтролируемого распространения конфиденциальной информации, содержащей персональные данные в результате ее разглашения должностным лицом, имеющим доступ к информации, содержащей персональные данные, или получения несанкционированного доступа к конфиденциальной информации;

– предотвращения несанкционированного уничтожения, искажения, копирования, блокирования информации, содержащей персональные данные;

– предотвращения утраты, несанкционированного уничтожения или сбоев в процессе функционирования автоматизированных систем обработки информации, содержащей персональные данные, обеспечение полноты, целостности, достоверности такой информации;

– соблюдения правового режима использования информации, содержащей персональные данные;

– обеспечения возможности обработки и использования персональных данных Организации, его структурными подразделениями и должностными лицами, имеющими соответствующие полномочия.

III. Хранение и уничтожение персональных данных

3.1. Персональные данные субъекта ПДн хранятся в подразделениях организации, которые осуществляют их обработку и отвечает за взаимодействие с субъектом.

3.2. ПДн на бумажном носителе хранятся в папках в сейфе или в металлическом шкафу.

3.3. Персональные данные субъекта ПДн в электронном виде хранятся в локализованных электронных базах данных компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные субъекта, обеспечиваются системой защиты информации.

3.4. В нерабочее время помещение, где хранятся ПДн (хранилище ПДн), должно закрываться на ключ. В рабочее время, в случае ухода руководителя, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных руководителем подразделения.

3.5. Сотрудник организации, имеющий доступ к персональным данным субъектов ПДн, в связи с исполнением трудовых обязанностей, обеспечивает

хранение информации, содержащей персональные данные субъекта, исключающее доступ к ним третьих лиц.

3.6. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих персональные данные субъектов.

3.7. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные субъектов ПДн лицу, на которое приказом (распоряжением) будет возложено исполнение его трудовых обязанностей.

3.8. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные субъектов ПДн по указанию руководителя структурного подразделения, передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.

3.9. При увольнении сотрудника, имеющего доступ к персональным данным субъектов ПДн, документы и иные носители, содержащие персональные данные субъектов ПДн, по указанию руководителя структурного подразделения передаются другому сотруднику, имеющему доступ к персональным данным субъектов ПДн.

3.10. Повседневный контроль за выполнением требований по защите хранилищ ПДн осуществляют лица, ответственные за помещение (хранилище ПДн).

3.11. Периодический контроль эффективности мер защиты хранилищ ПДн осуществляется ответственным за организацию обработки и обеспечение защиты персональных данных.

3.12. Уничтожение персональных данных субъектов ПДн на бумажном носителе либо удаление электронных баз данных, содержащих персональные данные субъектов ПДн в электронном виде, осуществляется по истечении установленного срока обработки ПДн комиссией (Приложение № 1 данной инструкции).

3.13. После уничтожения ПДн формируется акт об уничтожении носителей персональных данных, согласно Приложению № 2 данной инструкции.

IV. Порядок предоставления доступа к персональным данным

4.1. Основанием для допуска сотрудника к работе с персональными данными является включение его в список лиц, допущенных к обработке персональных данных. Включение в список лиц, допущенных к работе с персональными данными, осуществляется указанием заместителя Главы Администрации Тазовского района по внутренней политике по представлению администратора безопасности информации. При допуске к работе с персональными данными определяется перечень информационных систем персональных данных, к работе в которых допущен специалист,

а также перечень обрабатываемых им персональных данных и разрешенный вид процедур обработки ПДн.

4.2. Доступ к персональным данным имеют сотрудники работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно распоряжению Администрации Тазовского района.

4.3. Пользователи допускаются к работе с ресурсами ИС только после прохождения инструктажа, проводимого администратором безопасности информации и ознакомлением с требованиями Политики в области организации обработки и обеспечения ПДн, должностной инструкции и иными локальными нормативными актами Организации в сфере обеспечения безопасности персональных данных.

4.4. Основанием для прекращения допуска сотрудника к работе с персональными данными или внесение изменений в его обязанности по работе в информационной системе, внесении изменений в перечень обрабатываемых ПДн и в перечень процедур обработки ПДн является распоряжение Администрации Тазовского района.

4.5. Внесение предложений на утверждение заместителю Главы Администрации Тазовского района по внутренней политике по изменению списка лиц, допущенных к работе с персональными данными, осуществляется администратором безопасности информации.

V. Порядок обеспечения безопасности персональных данных

5.1. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации, рассмотрен в Положении по организации работ по обеспечению информационной безопасности.

5.2. Порядок учёта, хранения и обращения со съёмными носителями персональных данных рассмотрен в Инструкции по порядку учёта, хранения и уничтожения машинных носителей информации.

VI. Ответственность

6.1. Работники, нарушившие требования настоящей инструкции, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами.

Приложение № 1

к Инструкции по порядку
учета, хранения и уничтожения
съёмных носителей
информации в Администрации
Тазовского района

С О С Т А В
Комиссии по уничтожению машинных носителей, содержащих персональные данные в Администрации Тазовского района

Председатель Комиссии:

заместитель Главы Администрации Тазовского района по внутренней политике.

Члены Комиссии:

начальник отдела информационных технологий Администрации Тазовского района;

главный специалист отдела информационных технологий Администрации Тазовского района;

ведущий инженер-программист отдела информационных технологий Администрации Тазовского района.

Приложение № 2

к инструкции по порядку
учета, хранения и уничтожения
съёмных носителей
информации в Администрации
Тазовского района

АКТ
об уничтожении носителей персональных данных

Комиссия по уничтожению персональных данных в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

В связи с достижением цели обработки персональных данных (ПДн) к уничтожению отобраны следующие носители персональных данных:

№ п/п	Тип носителя	Учетный номер носителя	Примечание
1.			
2.			
3.			

Уничтожение информации необходимо с _____ материальных носителей.

Проверка правильности включения материальных носителей ПДн в Акт проведена.

ПДн с материальных носителей уничтожены путем

_____

СОГЛАСОВАНО
Ответственный за организацию обработки
и обеспечение безопасности ПДн

_____ _____ _____
(ФИО) (подпись) (дата)

ОТМЕТКА О ВЫПОЛНЕНИИ
Ответственный за выполнение

_____ _____ _____
(ФИО, должность) (подпись) (дата)

».

5. Приложение № 17 изложить в следующей редакции:

«

Приложение № 17
УТВЕРЖДЕН
распоряжением
Администрации Тазовского
района от 22 июля 2020 года
№ 171-р (в редакции распоряжения
Администрации Тазовского района
от 30 июля 2021 года № 297-р)

СОСТАВ
комиссии для классификации информационных систем персональных данных Администрации Тазовского района

Председатель Комиссии:

Заместитель Главы Администрации Тазовского района по внутренней политике.

Члены комиссии:

начальник отдела информационных технологий Администрации Тазовского района;

главный специалист отдела информационных технологий Администрации Тазовского района.».