АДМИНИСТРАЦИЯ ТЕМРЮКСКОГО ГОРОДСКОГО ПОСЕЛЕНИЯ ТЕМРЮКСКОГО РАЙОНА

РАСПОРЯЖЕНИЕ

от 30.08.2019 № 184-р

город Темрюк

Об утверждении внутренних нормативно-правовых актов по защите персональных данных в администрации Темрюкского городского поселения Темрюкского района

Для обеспечения безопасности персональных данных при их обработке в администрации Темрюкского городского поселения Темрюкского района во исполнение требований Федерального закона от 27 июля 2006 года № 152 «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,

1. Утвердить следующий перечень нормативно-правовых актов:

1.1. Инструкцию системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Темрюкского городского поселения Темрюкского района, (Приложение № 1);

1.2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 2);

1.3. Инструкцию ответственного за обработку персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 3);

1.4. Инструкцию по организации антивирусной защиты в администрации Темрюкского городского поселения Темрюкского района (Приложение № 4);

1.5. Инструкцию по порядку учета и хранению документов, содержащих персональные данные, в администрации Темрюкского городского поселения Темрюкского района (Приложение № 5);

1.6. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации Темрюкского городского поселения Темрюкского района (Приложение № 6);

1.7. Инструкцию по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных) в администрации Темрюкского городского поселения Темрюкского района (Приложение № 7);

1.8. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 8)

1.9. Положение об обработке персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 9);

1.10. Порядок доступа сотрудников администрации Темрюкского городского поселения Темрюкского района в помещения, где ведётся обработка персональных данных (Приложение №10);

1.11. Правила работы с обезличенными персональными данными в администрации Темрюкского городского поселения Темрюкского района (Приложение № 11);

1.12. Регламент порядка действий сотрудников администрации Темрюкского городского поселения Темрюкского района, при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных (Приложение № 12);

1.13. Инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 13).

1.14. Политика обработки персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 14).

1.15. Инструкцию администратора безопасности информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 15).

1.16. Инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в администрации Темрюкского городского поселения Темрюкского района (Приложение № 16).

1.17. Концепцию информационной безопасности информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 17).

1.18. Политику информационной безопасности в администрации Темрюкского городского поселения Темрюкского района (Приложение № 18).

1.19. Инструкцию по организации парольной защиты информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 19).

1.20. Инструкцию по организации защиты информации о событиях безопасности в информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 20).

1.21. Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 21).

1.22. Инструкцию по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в администрации Темрюкского городского поселения Темрюкского района (Приложение № 22).

1.23. Порядок уничтожения и блокирования персональных данных в администрации Темрюкского городского поселения Темрюкского района (Приложение № 23).

2. Ведущему специалисту (по организационным вопросам и взаимодействию со средствами массовой информации (СМИ)) (Семикиной) разместить настоящее постановление на официальном сайте администрации Темрюкского городского поселения Темрюкского района в информационно-телекоммуникационной сети «Интернет».

3. Контроль за выполнением настоящего распоряжения оставляю за собой.

4. Распоряжение вступает в силу со дня его подписания.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

АДМИНИСТРАЦИЯ ТЕМРЮКСКОГО ГОРОДСКОГО ПОСЕЛЕНИЯ ТЕМРЮКСКОГО РАЙОНА
ОБЩИЙ ОТДЕЛ

ПРИЛОЖЕНИЕ № 1
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности, полномочия и ответственность системного администратора информационных систем персональных данных (ИСПДн) по обеспечению безопасности персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Администратор ИСПДн (далее – Администратор) назначается распоряжением главы администрации Темрюкского городского поселения Темрюкского района.

1.3. Администратор ИСПДн подчиняется главе Темрюкского городского поселения Темрюкского района.

1.4. Администратор ИСПДн в своей работе руководствуется настоящей Инструкцией и Положением о защите персональных данных, руководящими и нормативными документами ФСТЭК России и внутренними регламентирующими документами по защите информации в администрации.

1.5. Администратор ИСПДн отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

2. Обязанности по обеспечению безопасности информации

Администратор ИСПДн обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Ознакомить всех пользователей ИСПДн с внутренними нормативно-правовыми актами по обеспечению безопасности персональных данных (под роспись).

2.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

программного обеспечения автоматизированных рабочих мест (далее – АРМ) и серверов (операционные системы, прикладное и специальное ПО);

аппаратных средств;

аппаратных и программных средств защиты.

2.4. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.5. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов (если не назначен другой ответственный).

2.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.7. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Осуществлять регистрацию пользователей, выдачу временных паролей пользователей, осуществлять контроль за правильностью использования пароля пользователем ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.12. Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и Компаниями.

2.13. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Ответственность

3.1. В случае нарушения положений настоящей Инструкции администратор несёт ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 2
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ

о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных в администрации Темрюкского городского поселения Темрюкского района

1. Назначение и область действия

1.1. Данная Инструкция определяет действия, связанные с мерами и средствами поддержания непрерывной работы и восстановления работоспособности информационных систем в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Настоящая Инструкция регламентирует:

меры защиты от потери информации;

действия по восстановлению в случае потери информации.

1.3. Действие настоящей Инструкции распространяется на администраторов информационных систем, ответственных за резервное копирование информации.

2. Меры обеспечения надежной работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры.

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

системы обеспечения отказоустойчивости;

системы резервного копирования и хранения данных;

системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

пожарные сигнализации и системы пожаротушения;

системы вентиляции и кондиционирования;

системы резервного питания.

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

резервные линии электропитания в пределах комплекса зданий;

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры.

2.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых персональных данных – не реже раза в неделю или по требованию пользователя ИСПДн;

для системной информации – не реже раза в месяц;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн каждый раз при внесении изменений в эталонные копии (выход новых версий).

2.2.2. Данные о проведение процедуры резервного копирования должны отражаться в специально созданном Журнале учета.

2.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя; датой проведения резервного копирования.

2.2.4. Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

2.2.5. Носители и резервные копии данных должны храниться не менее года для возможности восстановления данных.

3. Порядок проведения резервирования информации

3.1. Перед проведением процедуры резервного копирования необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

3.2. Резервирование информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

3.3. Все файлы, входящие в состав резервной копии, должны архивироваться в один архив с присвоением имени архива в формате время дата (например, 18.00 21.11.2011).

3.4. Архивация может производиться как штатными средствами, поставляемыми в составе специализированного программного обеспечения для построения информационной системы, так и сторонним программным обеспечением (например, 7zip, WinRar).

3.5. Резервные копии должны сохраняться на носители, не входящие в состав технических средств информационной системы персональных данных (внешние жесткие диски, CD/DVD диски, flash диски).

3.6. После завершения процедуры резервного копирования информации и записи резервной копии на носитель, необходимо поместить носитель с резервной копией в специально отведённое для хранения место и проставить соответствующую отметку в Журнале.

4. Порядок проведения восстановления информации

4.1. Перед проведением процедуры восстановления информации необходимо убедиться в том, что все пользователи информационной системы завершили свою работу с информационной системой.

4.2. Восстановление информации следует проводить из наиболее актуальной резервной копии.

4.3. В случае, если специализированное программное обеспечение для построения информационной системы не позволяет работать с заархивированными резервными копиями, то перед восстановлением информации необходимо разархивировать файлы резервной копии при помощи стороннего программного обеспечения (например 7zip, WinRar).

4.4. Восстановление информации в информационных системах персональных данных проводится при помощи штатных средств, поставляемых в составе специализированного программного обеспечения для построения информационной системы, либо, в случае отсутствия таковых, штатными средствами операционной системы или системы управления базами данных (при использовании таковой).

4.5. После завершения процедуры восстановления необходимо убедиться в работоспособности информационной системы персональных данных.

4.6. В случае успешного восстановления оповестить пользователей информационной системы о возможности продолжения работы. В противном случае необходимо изучить документацию, прилагаемую к программному обеспечению либо обратиться в службу технической поддержки.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 3
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии со ст. 22.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность лиц, ответственных за организацию обработки персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Ответственный за организацию обработки персональных данных назначается распоряжением главы администрации Темрюкского городского поселения Темрюкского района из числа сотрудников администрации.

1.3. Ответственный за организацию обработки персональных данных подчиняется главе Темрюкского городского поселения Темрюкского района.

1.4. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей Инструкцией, ФЗ-№ 152 от 27 июля 2006 года. «О персональных данных», ФЗ-№ 149 от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использовании средств автоматизации», Приказом федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К) и внутренними документами администрации по защите информации.

1.5. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности

персональных данных и не исключает обязательного выполнения их требований.

2. Обязанности

2.1. Осуществлять внутренний контроль за соблюдением сотрудниками администрации требований законодательства РФ при обработке персональных данных, внутренних положений, инструкций и других нормативно-правовых документов в области защиты информации.

2.2. Доводить до сведения работников администрации (структурного подразделения) содержание положений законодательства РФ о персональных данных, внутренних нормативно-правовых актов администрации по вопросам обработки персональных данных, требований по защите персональных данных.

2.3. Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов:

в соответствии с ФЗ-152 «О персональных данных» субъект персональных данных или его представитель имеет право на получение информации, касающейся обработки его персональных данных на основании обращения либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации;

такие обращения и запросы субъектов персональных данных подлежат обязательному учету;

ответственный за организацию обработки обязан фиксировать все обращения и запросы в журнале учета обращений граждан (субъектов персональных данных).

2.4. Организовать прием и обработку обращений и запросов пользователей информационной системы на получение персональных данных, включая лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, а также факты предоставления персональных данных по этим запросам регистрировать в Журнале обращений.

2.5. Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации пользователями информационной системы персональных.

3. Ответственность

3.1. В случае нарушения положений настоящей Инструкции ответственные за организацию обработки персональных данных лица несут ответственность в соответствии с действующим законодательством.

4. С настоящей Инструкцией ознакомлены:

№	Фамилия, имя, отчество	Должность сотрудника	Подпись
1	Ермолаев Максим Викторович	Глава Темрюкского городского поселения Темрюкского района	
2	Румянцева анна Владимировна	Заместитель главы Темрюкского городского поселения Темрюкского района	
3	Сокиркин Алексей Викторович	Заместитель главы Темрюкского городского поселения Темрюкского района	
ОБЩИЙ ОТДЕЛ			
4	Отставная Любовь Валерьевна	Начальник общего отдела	
5	Чепель Галина Георгиевна	Главный специалист общего отдела	
6	Лихтаревская Светлана Михайловна	Заведующий приемной	
7	Семикина Ольга Анатольевна	Ведущий специалист (по организационным вопросам и взаимодействии со (СМИ))	
8	Рогова Любовь Витальевна	Ведущий специалист (по вопросам потребительского рынка)	
ОТДЕЛ ПО ВОПРОСАМ ЗЕМЕЛЬНЫХ ОТНОШЕНИЙ И АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА			
9	Пчелкина Марина Александровна	Начальник отдела	
10	Борисёнок Максим Вячеславович	Ведущий специалист (по земельному контролю) отдела по вопросам земельных отношений и агропромышленного комплекса	
ОТДЕЛ ПО КАПИТАЛЬНОМУ СТРОИТЕЛЬСТВУ			
11	Казакова Марина Викторовна	Начальник отдела по капитальному строительству	

12	Давлетшина Анжела Хаметьяновна	Ведущий специалист отдела по капитальному строительству	
ОТДЕЛ ПО ВОПРОСАМ ЖИЛИЩНО-КОММУНАЛЬНОГО ХОЗЯЙСТВА			
13	Ковальчук Евгений Владимирович	Ведущий специалист отдела по вопросам жилищно-коммунального хозяйства	
14	Сергиенко Сергей Сергиенко	Ведущий специалист отдела по вопросам жилищно-коммунального хозяйства	
15	Куриная Ольга Викторовна	Ведущий специалист отдела по вопросам жилищно-коммунального хозяйства	
ОТДЕЛ ПО ВОПРОСАМ ПЕРСПЕКТИВНОГО РАЗВИТИЯ, АРХИТЕКТУРУ И ГРАДОСТРОИТЕЛЬСТВА			
16	Лукина Светлана Геннадьевна	Главный специалист отдела по вопросам перспективного развития, архитектуры и градостроительства	
17	Кайнова Людмила Ивановна	Ведущий специалист отдела по вопросам перспективного развития, архитектуры и градостроительства	
ОТДЕЛ ПО ФИНАНСАМ И БЮДЖЕТУ			
18	Мухаммадиева Светлана Викторовна	Начальник отдела по финансам и бюджету	
19	Богданец Оксана Владимировна	Ведущий специалист отдела по финансам и бюджету	
20	Падалко (Власова) Яна Александровна	Ведущий специалист отдела по финансам и бюджету	
21	Жевака Ольга Борисовна	Главный специалист (по вопросам имущественных отношений)	
ОТДЕЛ КАДРОВ			
22	Рафикова Светлана Викторовна	Начальник отдела кадров	
23	Кушнарёва Алла Михайловна	Ведущий специалист отдела кадров	
ЮРИДИЧЕСКИЙ ОТДЕЛ			
24	Масёхина Марина Ивановна	Начальник юридического отдела	
25	Вишнякова Татьяна Владимировна	Ведущий специалист (по правовым вопросам) юридического отдела	
ОТДЕЛ ПО МУНИЦИПАЛЬНЫМ ЗАКУПКАМ			
26	Заводовская Елена Ивановна	Начальник отдела по муниципальным закупкам	
27	Журман Наталья Сергеевна	Ведущий специалист отдела по муниципальным закупкам	
28	Чечин Виталий Сергеевич	Ведущий специалист (по взаимодействию с правоохранительными органами, казачеством, общественными объединениями, ГО и ЧС)	

ПРИЛОЖЕНИЕ № 4
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по организации антивирусной защиты в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.

1.2. Данная Инструкция распространяется на всех пользователей и администраторов информационных систем персональных данных (далее – ИСПДн) в администрации.

2. Установка и обновление антивирусных средств

2.1. Установка и настройка антивирусных средств осуществляются только администратором информационной системы персональных данных.

2.2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

3.2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.

3.3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

3.4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно

допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.

3.5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.

3.6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.

3.7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационной системы персональных данных;

провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса пользователь или Администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

5. Ответственность при организации антивирусной защиты

5.1. Ответственность за организацию антивирусной защиты возлагается на Администратора информационной системы персональных данных.

5.2. Ответственность за выполнение требований данной Инструкции возлагается на Пользователей и администратора информационной системы персональных данных.

5.3. Периодический контроль за соблюдением положений данной Инструкции возлагается на администратора информационной системы персональных данных.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 5
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Темрюкского городского поселения Темрюкского района (далее – администрация), допущенных к обработке персональных данных.

2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

2.1. Все находящиеся на хранении и в обращении документы с персональными данными в администрации подлежат учёту.

2.2. Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

2.3. Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

2.4. При работе с документами, которые содержат персональные данные необходимо:

2.4.1. Соблюдать требования настоящей Инструкции.

2.4.2. Использовать полученные документы исключительно для выполнения своих служебных обязанностей.

2.4.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

2.4.4. Бережно относится к документам, содержащим персональные данные.

2.4.5. Обеспечивать физическую безопасность документов всеми разумными способами.

2.4.6. Обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях

2.4.7. Извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные.

2.4.8. Осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения руководителя.

2.4.9. При передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

2.4.10. В случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность главу Темрюкского городского поселения Темрюкского района. Отметки об утрате вносятся в журнал учета документов с персональными данными.

2.4.11. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы с персональными данными информации изымаются.

3. Запрещается

3.1. Использовать документы с персональными данными в личных целях.

3.2. Передавать документы с персональными данными третьим лицам без соответствующего разрешения руководителя Темрюкского городского поселения Темрюкского района

3.3. Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

3.4. Выносить документы с персональными данными из служебных помещений для работы с ними на дому и т. д.

3.5. Оставлять документы с персональными данными без присмотра.

3.6. Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

4. Ответственность

4.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 6
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ) в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в администрации Темрюкского городского поселения Темрюкского района (далее – администрация).

1.2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.

2. Обязанности Пользователя

2.1. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

2.2. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

2.3. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

2.4. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.5. Пользователь обязан немедленно уведомлять ответственного за обработку персональных данных о компрометации криптографических ключей.

2.6. Пользователь обязан немедленно уведомлять ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

3. Порядок обращения со средствами криптографической защиты информации

3.1. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

3.3. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

3.4. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

3.5. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.6. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

3.7. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Порядок обращения с ключами ЭЦП

4.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

4.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

4.3. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

4.4. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа; защиты электронного документа от подделки и обеспечения конфиденциальности документа.

4.5. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

4.6. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

5. Запрещается

5.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

5.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

5.3. Передавать НКИ третьим лицам.

5.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

5.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

5.6. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;

– Передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;

– Нарушение правил хранения криптографических ключей;

– Вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– Отрицательный результат при проверке наложенной ЭЦП;

– Несанкционированное или без учётное копирование ключевой информации;

– Все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

6.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

6.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

6.4. Для восстановления конфиденциальной связи после компрометации

действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

7. Ответственность Пользователя

7.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

7.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 7
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ

по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных) в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при их хранении на машинных носителях.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Темрюкского городского поселения Темрюкского района (далее – Администрация), допущенных к обработке персональных данных.

2. Основные термины, сокращения и определения

2.1. Администратор информационной системы персональных данных – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.

2.2. АРМ – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.

2.3. ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

2.4. ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

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

2.6. ПК – персональный компьютер.

2.7. ПО – программное обеспечение вычислительной техники.

2.8. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

2.9. Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработке

персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Администрации и подвергаются регулярной ревизии и контролю.

3.3. Носители конфиденциальной информации предоставляются сотрудникам Администрации на основании письменного разрешения руководителя Администрации при:

необходимости выполнения вновь принятым работником своих должностных обязанностей;

возникновения у сотрудника Администрации производственной необходимости.

4. Порядок учета, хранения и обращения с машинными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении машинные носители с конфиденциальной информацией (персональными данными) в Администрации подлежат учёту.

4.2. Каждый машинный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Факт выдачи машинного носителя фиксируется в журнале учета машинных носителей конфиденциальной информации.

5. При использовании сотрудниками носителей конфиденциальной информации необходимо

5.1. Соблюдать требования настоящей Инструкции.

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей.

5.3. Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.

5.4. Бережно относится к носителям конфиденциальной информации (персональных данных).

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.6. Извещать ответственного за обработку персональных данных о фактах утраты (кражи) носителей конфиденциальной информации.

5.7. Перед работой проверять носители конфиденциальной информации на наличие вредоносного ПО.

5.8. Осуществлять вынос машинных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату только с письменного разрешения руководителя.

5.9. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на машинные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на машинных носителях осуществляется в порядке, установленном для документов данного типа.

5.10. В случае утраты или уничтожения машинных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель Администрации. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета машинных носителей конфиденциальной информации (персональных данных).

5.11. Машинные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт.

5.12. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются.

6. Запрещается

6.1. Использовать носители конфиденциальной информации в личных целях.

6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

6.3. Хранить машинные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4. Выносить машинные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

7. Ответственность

7.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 8
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Пользователем является каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно-правовыми документами Администрации по защите информации.

2. Обязанности пользователя

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних нормативно-правовых документов, по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (Раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет (Раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в Администрации, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору информационной системы персональных данных или ответственном за обработку персональных данных.

2.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к Администратору информационной системы персональных данных.

2.9. Пользователям запрещается:

Разглашать защищаемую информацию третьим лицам;

Копировать защищаемую информацию на внешние носители без письменного разрешения руководителя структурного подразделения или Администрации;

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

Несанкционированно открывать общий доступ к ресурсам;

Запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

Отключать (блокировать) средства защиты информации;

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системе персональных данных;

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с Администратором информационной системы персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

3. Организация парольной защиты

3.1. Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационной системы персональных данных.

3.2. Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

3.6. Лица, использующие паролирование, обязаны:

Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

Своевременно сообщать Администратору информационной системы персональных данных об утере, компрометации, несанкционированном

изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и международного обмена (сети Интернет) (далее – Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других);

Передавать по Сети защищаемую информацию без использования средств шифрования;

Запрещается скачивать из Сети программное обеспечение и исполняемые файлы (файлы с расширением exe, dll, msi);

Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие);

Запрещается нецелевое использование подключения к Сети.

5. Ответственность

5.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 9
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ПОЛОЖЕНИЕ
об обработке персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) в администрации Запорожского сельского поселения Темрюкского района (далее – Администрация) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных».

1.2. Цель разработки Положения — определение порядка обработки персональных данных в Администрации, обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных, а также установление ответственности работников, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его подписания и действует в течение трёх лет, после чего должно быть пересмотрено.

1.3.2. Все изменения в Положение вносятся Распоряжением.

1.4. Все работники Администрации, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается только в случаях их обезличивания.

2. Основные понятия и состав персональных данных

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации субъекту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и прочая дополнительная информация;

обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

конфиденциальность персональных данных — обязательное требование для работника, получившего доступ к персональным данным, не допускать их распространения без согласия субъекта персональных данных или иного законного основания;

распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

использование персональных данных — действия (операции) с персональными данными, совершаемые работниками в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

информация — сведения (сообщения, данные) независимо от формы их представления;

документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных входят сведения, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья и другая информация, позволяющая идентифицировать субъекта персональных данных и получить о нём дополнительную информацию.

3. Цели обработки персональных данных, их состав и сроки обработки

3.1. Обработка персональных данных сотрудников осуществляется в целях обеспечения кадровой работы, в том числе в целях содействия сотруднику в прохождении гражданской службы, обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей, ведения кадрового и бухгалтерского учета, и выполнения функций, возложенных законодательством Российской Федерации.

3.2. Персональные данные сотрудников обрабатываются до момента увольнения. Документы по личному составу, законченные делопроизводством до 1 января 2003 года, хранятся 75 лет, а документы по личному составу, законченные делопроизводством после 1 января 2003 года, хранятся 50 лет, после чего передаются на постоянное хранение в государственные архивные фонды в соответствии со ст. 22.1 Федерального закона от 22 октября 2004 года № 125-ФЗ "Об архивном деле в Российской Федерации".

3.3. Обработка персональных данных жителей муниципального образования осуществляется в целях предоставления муниципальных услуг и исполнения муниципальных функций в соответствии с порядком работы с обращениями граждан в Администрации, утвержденными постановлениями Администрации.

3.4. Персональные данные граждан, обратившихся в Администрацию лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений с последующим уведомлением заявителей о результатах рассмотрения.

3.5. Персональные данные субъектов, не являющимися сотрудниками, в том числе персональные данные, полученные с формы обратной связи сайта Администрации, обрабатываются и хранятся до момента достижения цели обработки персональных данных, после чего уничтожаются.

3.6. Состав обрабатываемых персональных данных определяется в соответствии с перечнем персональных данных, обрабатываемых в Администрации Темрюкского городского поселения Темрюкского района (Приложение № 1 к данному Положению).

4. Сбор, обработка и защита персональных данных

4.1. Порядок получения персональных данных

4.1.1. Доступ к персональным данным разрешен сотрудникам, указанным в перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо, осуществление доступа к персональным данным, в Администрации Темрюкского городского поселения Темрюкского района. (Приложение № 2 к данному Положению).

4.1.2. Перед допуском к работе с персональными данными, предоставлением персональных данных для выполнения служебных обязанностей с работника необходимо взять письменное обязательство о неразглашении персональных данных (Приложение № 3 к данному Положению).

4.1.3. Все персональные данные следует получать у субъекта персональных данных. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудник Администрации должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.2. Порядок обработки персональных данных.

4.2.1. Субъект персональных данных предоставляет сотруднику Администрации достоверные сведения о себе. Сотрудник Администрации проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами, удостоверяющими личность и иными документами подтверждающие достоверность сведений о субъекте персональных данных.

4.2.2. В соответствии со ст. 6 ФЗ-152 «О Персональных данных» сотрудники Администрации при обработке персональных данных должны соблюдать следующие общие требования:

4.2.2.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. (Приложение № 4 к данному Положению).

4.2.2.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

4.2.2.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг.

4.2.2.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по

которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

4.2.2.5. Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

4.2.2.6. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.2.2.7. Защита персональных данных от неправомерного их использования или утраты обеспечивается Администрацией за счет средств Администрации в порядке, установленном законодательством.

4.2.2.8. Отказ гражданина от своих прав на сохранение и защиту тайны недействителен.

4.2.3. Автоматизированная обработка персональных данных разрешается в информационных системах персональных данных перечисленных в перечне информационных систем персональных данных, принадлежащих Администрации Запорожского сельского поселения Темрюкского района (Приложение № 5 к данному Положению).

5. Передача и хранение персональных данных

5.1. При передаче персональных данных необходимо соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, установленных федеральным законодательством.

5.1.2. Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц письменное подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

5.1.3. Осуществлять передачу персональных данных субъектов в пределах Администрации в соответствии с настоящим Положением и другими внутренними нормативно-правовыми актами по защите информации.

5.1.4. При передаче персональных данных за пределы Администрации в другие организации в целях выполнения производственных функций (аутсорсинг, аутстаффинг и т.п.) заключать договоры с указанием в них о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены.

5.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

5.2. Персональные данные субъектов могут обрабатываться и храниться, как на бумажных носителях, так и в электронном виде.

6. Уничтожение персональных данных

6.1. Уничтожение документов, содержащих персональные данные, в том числе черновиков, бракованных листов и испорченных копий, должно производиться комиссией.

6.2. Порядок уничтожения документов, черновиков, испорченных листов, неподписанных проектов документов, содержащих персональные данные:

документы, черновики документов, испорченные листы, варианты и неподписанные проекты документов разрываются таким образом, чтобы было невозможно дальнейшее восстановление информации. В учетных данных документа (карточке, журнале) делается отметка об уничтожении черновика с указанием количества листов и проставлением подписи сотрудника и даты;

уничтожение документов, содержащих персональные данные, производится в строгом соответствии со сроками хранения.

6.3. Уничтожение персональных данных в электронном виде осуществляется путём удаления информации со всех носителей и резервных копий без возможности дальнейшего восстановления.

7. Доступ к персональным данным

7.1. Доступ сотрудников к персональным данным осуществляется на основании разрешительной системы доступа.

7.2. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях.

7.3. Передача персональных данных третьей стороне возможна только при письменном согласии субъекта персональных данных, либо на основании законодательства Российской Федерации.

7.4. Передача персональных данных третьей стороне в случаях, не предусмотренных законодательством Российской Федерации осуществляется на договорной основе с указанием в договоре о том, что переданные персональные данные могут быть использованы только в целях, для которых они сообщены.

8. Правила работы с обезличенными данными

8.1. Обезличиванием персональных данных называются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (например, статистические данные).

8.2. Обезличивание персональных данных в Администрации при обработке персональных данных с использованием средств автоматизации осуществляется с помощью специализированного программного обеспечения на основании нормативно правовых актов, правил, инструкций, руководств, регламентов, инструкций на такое программное обеспечение и иных документов для достижения заранее определенных и заявленных целей.

8.3. Допускается обезличивание персональных данных при обработке персональных данных без использования средств автоматизации - производить способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8.4. Работа с обезличенными данными осуществляется в порядке установленным законодательством Российской Федерации и внутренними нормативно-правовыми актами, регулирующими работу с персональными данными.

9. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

9.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Администрации организуется проведение периодических проверок условий обработки персональных данных. Проверки осуществляются ответственным за организацию обработки персональных данных в Администрации либо комиссией, образуемой руководителем Администрации не реже одного раза в 3 года.

9.2. При осуществлении внутреннего контроля соответствия обработки персональных данных установленным требованиям в Администрации производится проверка:

соблюдения принципов обработки персональных данных в Администрации;

соответствия локальных актов в области персональных данных Администрации действующему законодательству Российской Федерации;

выполнения сотрудниками Администрации требований и правил (в том числе особых) обработки персональных данных в информационных системах персональных данных Администрации;

перечней персональных данных, используемых для решения задач и функций структурными подразделениями Администрации и необходимости

обработки персональных данных в информационных системах персональных данных Администрации;

правильность осуществления сбора, систематизации, сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных в каждой информационной системе персональных данных Администрации;

актуальность перечня должностей сотрудников Администрации, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

актуальность перечня должностей сотрудников Администрации, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;

соблюдение прав субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

соблюдение обязанностей Администрацией, предусмотренных действующим законодательством в области персональных данных;

порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

наличие необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в информационных системах персональных данных Администрации;

актуальность сведений, содержащихся в уведомлении Администрации об обработке персональных данных;

актуальность перечня информационных систем персональных данных в Администрации;

наличие и актуальность сведений, содержащихся в Правилах обработки персональных данных для каждой информационной системы персональных данных Администрации;

знания и соблюдение сотрудниками Администрации положений действующего законодательства Российской Федерации в области персональных данных;

знания и соблюдение сотрудниками Администрации положений локальных актов Администрации в области обработки и обеспечения безопасности персональных данных;

знания и соблюдение сотрудниками Администрации инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

соблюдение сотрудниками Администрации конфиденциальности персональных данных;

актуальность локальных актов Администрации в области обеспечения безопасности персональных данных, в том числе в Технических паспортах информационных систем персональных данных;

соблюдение сотрудниками Администрации требований по обеспечению безопасности персональных данных;

наличие локальных актов Администрации, технической и эксплуатационной документации технических и программных средств информационных систем персональных данных Администрации;

иных вопросов.

9.3. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Администрации докладывает ответственный за организацию обработки персональных данных, либо председатель комиссии.

10. Права субъекта персональных данных

10.1. Субъект персональных данных имеет право получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей его персональные данные.

10.2. Субъект персональных данных имеет право требовать от сотрудников Администрации уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для работы Администрации персональных данных.

10.3. Субъект персональных данных имеет право получать информацию, которая касается обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;

наименование и место нахождения Администрации, сведения о лицах (за исключением работников Администрации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения,

если иной порядок представления таких данных не предусмотрен федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ-№152 «О персональных данных»;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные ФЗ-№152 «О персональных данных» или другими федеральными законами.

10.4. Субъект персональных данных имеет право требовать извещения сотрудниками Администрации всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

11.1. Работники Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 1
к Положению об обработке
персональных данных в администрации
Запорожского сельского поселения
Темрюкского района

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в администрации Темрюкского городского поселения Темрюкского района

В администрации Темрюкского городского поселения Темрюкского района обрабатывается следующий перечень персональных данных:

Персональные данные сотрудников:

1. Фамилия, Имя, Отчество
2. Тип документа, удостоверяющего личность, серия и номер, дата выдачи
3. Дата рождения
4. Место рождения
5. Адрес места жительства/прописки
6. Идентификационный номер налогоплательщика (ИНН)
7. Страховой номер индивидуального лицевого счета (СНИЛС)
8. Гражданство
9. Номер телефона
10. Адрес электронной почты
11. Семейное положение
12. Состав семьи, сведения о детях
13. Социальное положение
14. Образование
15. Профессия
16. Должность
17. Стаж
18. Сведения о доходах
19. Сведения о воинской обязанности и военной службе
20. Сведения об имуществе
21. Сведения об отсутствии судимости
22. Номера лицевых счетов, банковских карт

Персональные данные субъектов, не являющихся сотрудниками:

1. Фамилия, Имя, Отчество
2. Тип документа, удостоверяющего личность, серия и номер, дата выдачи
3. Дата рождения
4. Место рождения

5. Адрес места жительства/прописки
6. Идентификационный номер налогоплательщика (ИНН)
7. Страховой номер индивидуального лицевого счета (СНИЛС)
8. Гражданство
9. Номер телефона
10. Адрес электронной почты
11. Семейное положение
12. Состав семьи, сведения о детях
13. Социальное положение
14. Образование
15. Профессия
16. Должность
17. Стаж
18. Сведения о воинской обязанности и военной службе
19. Сведения об имуществе

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 2
к Положению об обработке
персональных данных в администрации
Темрюкского городского поселения
Темрюкского района

ПЕРЕЧЕНЬ
должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в администрации Темрюкского городского поселения Темрюкского района

Для обеспечения безопасности персональных данных при их обработке, хранении и передаче утверждаю следующий перечень должностей, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо, осуществление доступа к персональным данным:

1. Ермолаев Максим Викторович - глава Темрюкского городского поселения Темрюкского района;
2. Румянцева Анна Владимировна - заместитель главы Темрюкского городского поселения Темрюкского района;
3. Сокиркин Алексей Викторович - заместитель главы Темрюкского городского поселения Темрюкского района;
4. Отставная Любовь Валерьевна - начальник общего отдела;
5. Чепель Галина Георгиевна - главный специалист общего отдела;
6. Лихтаревская Светлана Михайловна - заведующий приемной;
7. Семикина Ольга Анатольевна - ведущий специалист (по организационным вопросам и взаимодействии со (СМИ));
8. Рогова Любовь Витальевна - ведущий специалист (по вопросам потребительского рынка);
9. Пчелкина Марина Александровна - начальник отдела по вопросам земельных отношений и агропромышленного комплекса;
10. Борисёнок Максим Вячеславович - ведущий специалист (по земельному контролю) отдела по вопросам земельных отношений и агропромышленного комплекса;
11. Казакова Марина Викторовна - начальник отдела по капитальному строительству;
12. Давлетшина Анжела Хаметьяновна - ведущий специалист отдела по капитальному строительству;
13. Ковальчук Евгений Владимирович - ведущий специалист отдела по вопросам жилищно-коммунального хозяйства;

14. Сергиенко Сергей Сергиенко - ведущий специалист отдела по вопросам жилищно-коммунального хозяйства;
15. Куриная Ольга Викторовна - ведущий специалист отдела по вопросам жилищно-коммунального хозяйства;
16. Лукина Светлана Геннадьевна - главный специалист отдела по вопросам перспективного развития, архитектуры и градостроительства;
17. Кайнова Людмила Ивановна - ведущий специалист отдела по вопросам перспективного развития, архитектуры и градостроительства;
18. Мухаммадиева Светлана Викторовна - начальник отдела по финансам и бюджету;
19. Богданец Оксана Владимировна - ведущий специалист отдела по финансам и бюджету;
20. Падалко Яна Александровна - ведущий специалист отдела по финансам и бюджету;
21. Жевака Ольга Борисовна - главный специалист (по вопросам имущественных отношений);
22. Рафикова Светлана Викторовна - начальник отдела кадров;
23. Кушнарёва Алла Михайловна - ведущий специалист отдела кадров;
24. Масёхина Марина Ивановна - начальник юридического отдела;
25. Вишнякова Татьяна Владимировна - ведущий специалист (по правовым вопросам) юридического отдела;
26. Заводовская Елена Ивановна - начальник отдела по муниципальным закупкам;
27. Журман Наталья Сергеевна - ведущий специалист отдела по муниципальным закупкам;
28. Чечин Виталий Сергеевич - ведущий специалист (по взаимодействию с правоохранительными органами, казачеством, общественными объединениями, ГО и ЧС).

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 3
к Положению об обработке
персональных данных в администрации
Темрюкского городского поселения
Темрюкского района

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных в администрации Темрюкского городского поселения Темрюкского района

Я, _____
(ФИО сотрудника)

Паспорт серия _____ номер _____ выдан _____

_____

исполняющий(ая) должностные обязанности _____
(должность)

предупрежден(а), что на период исполнения должностных обязанностей мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю.

3. Не использовать персональные данные с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к персональным данным не разглашать и не передавать третьим лицам известные мне персональные данные.

Я предупрежден (а), что в случае нарушения данного обязательства буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____
(Фамилия, Имя, Отчество) (Дата) (Подпись)

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 4
к Положению об обработке
персональных данных в администрации
Темрюкского городского поселения
Темрюкского района

Типовая форма
согласия на обработку персональных данных работника
администрации Темрюкского городского поселения
Темрюкского района

Я, _____
(Ф.И.О. полностью)

зарегистрированный(-ая) по адресу: _____
_____,

паспорт серии _____№_____ выдан_____
_____,
(орган, выдавший паспорт и дата выдачи)

с целью исполнения определенных сторонами условий трудового договора (трудоустройства) даю согласие администрации Темрюкского городского поселения Темрюкского района, расположенной по адресу: 353500, Краснодарский край, г. Темрюк, ул. Ленина, д. 48, на обработку нижеследующих персональных данных:

Фамилия, имя, отчество;

Вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;

Число, месяц, год рождения;

Место рождения;

Адрес места жительства/прописки;

Информация о гражданстве;

Идентификационный номер налогоплательщика (ИНН);

Страховой номер индивидуального лицевого счета (СНИЛС);

Номер контактного телефона или сведения о других способах связи;

Семейное положение, состав семьи и сведения о близких родственниках;

Сведения о трудовой деятельности;

Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании), о профессиональной переподготовке и повышении квалификации;

Профессия;

Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

Должность;
Стаж;
Сведения о воинском учете и реквизиты документов воинского учета;
Национальность;
Сведения об имуществе;
Информация о наличии или отсутствии судимости;
Номер расчетного счета, банковской карты.

Разрешаю сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, а также передачу третьим лицам, а именно в

_____

_____.

(указать, в какие организации будут передаваться персональные данные)

Настоящее согласие вступает в силу с момента его подписания и действительно до моего увольнения.

Данное согласие может быть отозвано по моему письменному заявлению.

_____ _____

(число, месяц, год) (подпись)

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 5
к Положению об обработке
персональных данных в администрации
Темрюкского городского поселения
Темрюкского района

ПЕРЕЧЕНЬ
информационных систем персональных данных, принадлежащих администрации Темрюкского городского поселения Темрюкского района

В администрации Темрюкского городского поселения Темрюкского района функционируют следующие информационные системы персональных данных (ИСПДн):

1. «АРМ главы»
2. «АРМ заместителя главы»
3. «АРМ начальника общего отдела»
3. «АРМ начальника отдела по финансам и бюджету»
4. «АРМ начальника отдела по вопросам земельных отношений и агропромышленного комплекса»
5. «АРМ начальника отдела по капитальному строительству»
6. «АРМ начальника отдела кадров»
7. «АРМ начальника юридического отдела»
8. «АРМ заведующего приёмной»
9. «АРМ ведущего специалиста»
10. «АРМ главного специалиста»

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ №10

к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ПОРЯДОК
доступа сотрудников администрации Темрюкского городского поселения Темрюкского района в помещения, где ведётся обработка персональных данных

1. Общие положения

1.1. Настоящий Порядок доступа сотрудников в помещения, где ведётся обработка персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация), разработано в соответствии с Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», постановлением Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Целью настоящего Порядка является исключение несанкционированного доступа в помещения, где ведётся обработка персональных данных и предотвращение нарушения конфиденциальности персональных данных.

2. Порядок доступа в помещения, где ведётся обработка персональных данных

2.1. Доступ сотрудников Администрации в помещения, в которых ведется обработка персональных данных, осуществляется по перечню должностей сотрудников Администрации в помещения, где ведется обработка персональных данных. Перечень готовится и уточняется лицом, ответственным за организацию обработки персональных данных в Администрации и утверждается руководителем Администрации.

2.2. Допуск в помещения, в которых ведется обработка персональных данных, иных лиц, осуществляется сотрудниками, указанными в Разрешительной системе доступа сотрудников Администрации в помещения, в которых ведется обработка персональных данных. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных,

допускается только в присутствии сотрудников, указанных в Разрешительной системе доступа сотрудников Администрации в помещения, в которых ведется обработка персональных данных.

3. Запрещается

3.1. Запрещается оставлять помещения, где ведётся обработка персональных данных, без присмотра сотрудников, имеющих допуск в помещения, где ведётся обработка персональных данных.

3.2. Запрещается оставлять без присмотра находящихся в помещении, где ведётся обработка персональных данных, посторонних лиц, а также, сотрудников, не имеющих допуск в помещения, где ведётся обработка персональных данных.

4. Внутренний контроль

4.1. Внутренний контроль за соблюдением порядка доступа в помещения, где ведётся обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

5. Ответственность

5.1. Сотрудники, нарушившие нормы настоящего Порядка, несут ответственность в соответствии с действующим законодательством

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 11

к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ПРАВИЛА
работы с обезличенными персональными данными в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в Администрации.

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

2.2. 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.

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

2.4. Обезличивание персональных данных проводится с целью ведения статистических данных и снижения ущерба от разглашения защищаемых персональных данных.

3. Способы обезличивания персональных данных

3.1. Уменьшение перечня обрабатываемых сведений (например, исключить место жительства субъекта персональных данных).

3.2. Замена части сведений идентификаторами (например, заменить Фамилию, Имя, Отчество порядковым номером по табелю).

3.3. Обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.4. Деление сведений на части и обработка в разных информационных системах.

3.5. Возможны другие способы обезличивания, исключающие возможность определения принадлежности персональных данных определённому субъекту персональных данных.

4. Порядок работы с обезличенными персональными данными

4.1. Мероприятия по обезличиванию персональных данных проводят сотрудники, ответственные за обработку персональных данных.

4.2. Обезличенные персональные данные могут обрабатываться как автоматизированным, так и не автоматизированным способами.

4.3. Обработка обезличенных персональных данных осуществляется с соблюдением конфиденциальности.

4.4. При работе с обезличенными персональными данными в автоматизированном и не автоматизированном режимах необходимо соблюдать правила и требования по обеспечению безопасности персональных данных, действующие в Администрации.

4.5. Передача обезличенных персональных данных третьим лицам разрешается с письменного разрешения руководителя Администрации, либо без такового в случаях, предусмотренных действующим законодательством.

5. Ответственность

5.1. Лица, нарушившие настоящие Правила, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 11

к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.209 № 184-р

ПРАВИЛА
работы с обезличенными персональными данными в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящие Правила работы с обезличенными персональными данными в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в Администрации.

2. Термины и определения

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

2.2. 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.

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

2.4. Обезличивание персональных данных проводится с целью ведения статистических данных и снижения ущерба от разглашения защищаемых персональных данных.

3. Способы обезличивания персональных данных

3.1. Уменьшение перечня обрабатываемых сведений (например, исключить место жительства субъекта персональных данных).

3.2. Замена части сведений идентификаторами (например, заменить Фамилию, Имя, Отчество порядковым номером по табелю).

3.3. Обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город).

3.4. Деление сведений на части и обработка в разных информационных системах.

3.5. Возможны другие способы обезличивания, исключающие возможность определения принадлежности персональных данных определённому субъекту персональных данных.

4. Порядок работы с обезличенными персональными данными

4.1. Мероприятия по обезличиванию персональных данных проводят сотрудники, ответственные за обработку персональных данных.

4.2. Обезличенные персональные данные могут обрабатываться как автоматизированным, так и не автоматизированным способами.

4.3. Обработка обезличенных персональных данных осуществляется с соблюдением конфиденциальности.

4.4. При работе с обезличенными персональными данными в автоматизированном и не автоматизированном режимах необходимо соблюдать правила и требования по обеспечению безопасности персональных данных, действующие в Администрации.

4.5. Передача обезличенных персональных данных третьим лицам разрешается с письменного разрешения руководителя Администрации, либо без такового в случаях, предусмотренных действующим законодательством.

5. Ответственность

5.1. Лица, нарушившие настоящие Правила, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 12
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

РЕГЛАМЕНТ

порядка действий сотрудников администрации Темрюкского городского поселения Темрюкского района при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Настоящий Регламент разработан на основании и во исполнение Федерального закона РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

Целью настоящего Регламента является:

обеспечение прав субъектов персональных данных на доступ к их персональным данным, которые обрабатываются в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация);

обеспечение прав уполномоченного органа по защите прав субъектов персональных данных на получение информации, необходимой ему для реализации полномочий по защите прав субъектов персональных данных;

упорядочение действий сотрудников Администрации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

Настоящий Регламент распространяется на сотрудников Администрации, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, а также уполномоченного органа по защите прав субъектов персональных данных, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

Настоящий Регламент подлежит применению исключительно в случаях обращений либо при получении запросов субъектов персональных данных или их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в рамках Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ.

1. Общие положения

1.1. Настоящий Регламент использует следующие сокращения:

ПДн – персональные данные;

ИСПДн – информационная система персональных данных.

1.2. Субъект ПДн – это физическое лицо, определенное или определяемое на основании любой относящейся к нему информации.

1.3. Законный представитель субъекта ПДн – это гражданин, который в силу закона выступает во всех учреждениях и организациях от имени и в защиту личных и имущественных прав и законных интересов недееспособных, ограниченно дееспособных граждан, либо дееспособных, но в силу своего физического состояния (по старости, болезни и т. п.) не могущих лично осуществлять свои права и выполнять свои обязанности. В качестве законных представителей выступают родители, усыновители, опекуны и попечители.

1.4. Далее по тексту настоящего Регламента под субъектом ПДн будет подразумеваться также законный представитель субъекта ПДн.

1.5. В соответствии со ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ субъект ПДн имеет право:

на получение сведений о Администрации, как операторе ПДн, в т.ч. о месте его нахождения;

на получение сведений о наличии у Администрации ПДн, относящихся к соответствующему субъекту персональных данных;

на ознакомление с такими ПДн;

требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

на получение при обращении или при получении запроса информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки персональных данных Администрацией, а также цель такой обработки;

способы обработки персональных данных, применяемые Администрацией;

сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

перечень обрабатываемых персональных данных и источник их получения;

сроки обработки персональных данных, в том числе сроки их хранения;

сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

1.6. В соответствии со ст. 9 Федерального закона РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ субъект ПДн имеет право отозвать свое согласие на обработку ПДн.

1.7. В соответствии со ст.ст. 14, 20, 21 Федерального закона РФ «О

персональных данных» от 27 июля 2006 г. № 152-ФЗ Администрация, как оператор ПДн, в случае поступления соответствующего запроса от субъекта ПД обязан:

предоставить субъекту ПДн в доступной форме сведения о наличии его ПДн (при этом указанные сведения не должны содержать ПДн, относящиеся к другим субъектам ПДн);

сообщить субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, и другие сведения, право на получение которых субъектом ПДн предусмотрено ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ;

предоставить возможность ознакомления с ПДн без взимания платы за это;

внести в ПДн необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

прекратить обработку ПДн и уничтожить их в случае отзыва субъектом ПДн согласия на обработку своих ПДн;

о внесенных изменениях и предпринятых мерах уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы;

уведомить субъекта ПДн об уничтожении ПДн;

1.8. В соответствии с п. 3 ч. 5 ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ право субъекта ПДн на доступ к своим ПДн ограничивается в случае, если предоставление ПДн нарушает конституционные права и свободы других лиц.

2. Действия сотрудников администрации при получении запроса субъекта ПДн

2.1. В соответствии с ч. 3 ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя.

2.2. В целях регистрации запросов субъектов ПДн и ответов на такие запросы в Администрации осуществляется ведение журнала регистрации запросов субъектов ПДн.

2.3. Ответственный за организацию обработки ПДн осуществляет прием и регистрацию запросов субъектов ПДн, а также рассмотрение, подготовку, регистрацию и направление ответов на такие запросы.

2.4. При получении запроса (обращения) физического лица, сотрудник Администрации, ответственный за прием и регистрацию входящей корреспонденции в Администрации, непосредственно в день получения устанавливает:

2.4.1. Содержит ли запрос фамилию, имя, отчество (последнее при его наличии) гражданина или его законного представителя, номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

2.4.2. Содержит ли почтовый адрес, по которому должны быть направлены ответ;

2.4.3. Имеется ли собственноручная подпись, а если запрос направлен в электронной форме, то имеется ли электронная цифровая подпись;

2.4.4. Сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

2.4.5. Отвечает ли такой запрос (обращение) требованиям, установленным ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ, к запросу субъекта ПДн.

2.5. В случае если при приеме запроса (обращения) физического лица будет установлено, что он содержит в себе все сведения, перечисленные в п. 2.4. настоящего то такой запрос подлежит приему и регистрации в журнале регистрации запросов субъектов ПДн в тот же день.

2.6. В случае, если при приеме запроса (обращения) физического лица будет установлено, что он не содержит в себе сведений, перечисленных в п. 2.4. настоящего Регламента, то такой запрос подлежит приему и регистрации в порядке, предусмотренном Администрацией для приема и регистрации прочей входящей корреспонденции.

2.7. Запросы субъектов ПДн, зарегистрированные в соответствии с п. 2.5. настоящего Регламента, в день регистрации подлежат передаче сотруднику (сотрудникам) Администрации, указанному (-ным) в п. 2.3. настоящего Регламента.

2.8. Сотрудники Администрации, ответственные за рассмотрение запросов субъектов персональных данных, обязаны рассмотреть запрос субъекта ПДн и подготовить ответ на него в письменной форме в течение десяти рабочих дней с даты получения Администрацией указанного запроса.

2.9. В случае если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение десяти рабочих дней с даты получения Администрацией указанного запроса.

2.10. Письменный ответ на запрос субъекта ПДн должен быть направлен в его адрес заказным письмом с уведомлением о вручении в течение десяти рабочих дней с даты получения Администрацией указанного запроса.

2.11. Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает конституционные права и свободы других лиц, Администрация сообщает ему об отказе в предоставлении информации о ПДн либо таких ПДн, о чем в срок, не превышающий семи рабочих дней со дня получения запроса субъекта ПДн в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение п. 4 ч. 8 ст. 14 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ.

2.12. Для обработки персональных данных, содержащихся в обращении в письменной форме субъекта ПД, дополнительного согласия не требуется.

3. Действия сотрудников Администрации при получении запроса уполномоченного органа по защите прав субъектов персональных данных

3.1. Прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн осуществляется Администрацией в порядке, установленном для приема и регистрации входящей корреспонденции.

3.2. При получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудники Администрации, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса и передают его сотрудникам указанным в п. 2.3

3.3. Администрация, в лице сотрудников, указанных в п. 2.3. настоящего Регламента, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет истребуемые им документы в течение семи рабочих дней с даты получения такого запроса.

3.4. В случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные п. 4 настоящего Регламента для соответствующих действий (операций) в отношении ПДн.

4. Действия сотрудников Администрации при получении требования субъекта ПДн об уточнении своих ПДн, их блокировании или уничтожении; в случае выявления при обращении или по запросу субъекта ПДн фактов недостоверности ПДн или неправомерных действий с ними; в случае отзыва субъектом ПДн согласия на их обработку

4.1. При получении требований субъектов ПДн об уточнении своих ПДн, их блокировании, уничтожении прием и регистрация таких требований осуществляется в порядке, предусмотренном п. 2 настоящего Регламента.

4.2. Требования субъектов ПДн в тот же день передаются сотрудникам Администрации, указанным в п. 2.3.

4.3. Полномочные сотрудники Администрации вносят в ПДн субъекта

необходимые изменения, уничтожают или блокируют соответствующие ПДн по предоставлении субъектом ПДн сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Администрация, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.4. О внесенных изменениях и предпринятых мерах Администрация обязана уведомить субъекта ПДн и третьих лиц, которым ПДн этого субъекта были переданы.

4.5. В случае если факт недостоверности ПДн или неправомерных действий с ними будет выявлен при обращении или по запросу субъекта ПДн Администрация обязана осуществить блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения такого запроса на период проверки.

4.6. В случае подтверждения факта недостоверности ПДн Администрация на основании документов, представленных субъектом ПДн, или иных необходимых документов обязана уточнить ПДн и снять их блокирование.

4.7. В случае выявления неправомерных действий с ПДн Администрация в срок, не превышающий трех рабочих дней с даты такого выявления, обязана устранить допущенные нарушения.

4.8. В случае невозможности устранения допущенных нарушений Администрация в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязана уничтожить ПДн.

4.9. Об устранении допущенных нарушений или об уничтожении ПДн Администрация обязана уведомить субъекта ПДн.

4.10. В случае отзыва субъектом ПДн согласия на обработку своих ПДн Администрация обязана прекратить обработку ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено федеральным законодательством. Об уничтожении ПДн Администрация обязана уведомить субъекта ПДн.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 1 к Регламенту
Форма 1 «Запрос субъекта ПДн»

Главе Темрюкского городского поселения Темрюкского района

от

Паспорт серия номер

(Когда и кем выдан)

Проживающий по адресу:

Контактный номер телефона

Руководствуясь ст. 14 Федерального закона «О персональных данных», прошу Вас предоставить мне следующую информацию:

1. Какова цель обработки моих персональных данных в Администрации Темрюкского городского поселения Темрюкского района;
2. Каковы способы обработки моих персональных данных, применяемые в Администрации Темрюкского городского поселения Темрюкского района, как оператором персональных данных;
3. Какие лица имеют доступ к моим персональным данным и каким лицам может быть предоставлен такой доступ;
4. Каков перечень обрабатываемых в Администрации Темрюкского городского поселения Темрюкского района принадлежащих мне персональных данных и каков источник их получения;
5. Каковы сроки обработки моих персональных данных и каковы сроки их хранения;
6. Какие юридические последствия для меня, как для субъекта персональных данных, может повлечь за собой обработка моих персональных данных.

Фамилия И.О. (Подпись) (Дата)

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 2 к Регламенту
Форма 2 «Ответ на запрос субъекта ПДн»

Исх №	От

Фамилия Имя Отчество
Адрес

Уважаемый _____!

Руководствуясь положениями ст. ст. 14, 20 Федерального закона РФ «О персональных данных» от 27 июля 2006 года № 152-ФЗ сообщаем Вам, что администрация Темрюкского городского поселения Темрюкского района обрабатывает Ваши персональные данные

1.Цель обработки Ваших персональных –

_____
(указать цель, заранее определенную до начала обработки)

2.Способы обработки Ваших персональных данных – автоматизированная обработка, неавтоматизированная обработка, смешанная обработка.

3.Лица, имеющие доступ к Вашим персональным данным:

- Должность1;
- Должность2;
- Должность3;

4.Доступ к Вашим персональным данным может быть предоставлен: *(тут указать тех лиц, которым МОЖЕТ быть предоставлен доступ).* Также, по основаниям, предусмотренным действующим законодательством, доступ к Вашим персональным данным может быть предоставлен органам, осуществляющим оперативно-розыскную деятельность, органам дознания, следствия, суда.

5.Перечень обрабатываемых персональных данных: (*Перечислить перечень)* Источник получения персональных данных – *(Указать источник получения).*

6.Срок обработки Ваших персональных данных – *(указать срок)*

7.Обработка Ваших персональных данных может повлечь следующие юридические последствия – *указать какие. (В теории права под юридическими последствиями понимают возникновение, изменение и прекращение в результате наступления какого-либо юридического факта тех или иных прав и обязанностей. По смыслу п.6 ч.4 ст.14 ФЗ 152 под таким юридическим фактом в Законе понимается именно сам факт*

обработки ПДн, т.е. факт совершения каких-либо действий с ПДн. Очевидно, что для человека факт совершения с его ПДн каких-либо операций (т.е. факт обработки ПДн) порождает возникновение у него комплекса прав, присущих субъекту ПДн и прямо предусмотренных ФЗ-152, а именно: право на доступ к своим ПДн, право на получение сведений об операторе, право требовать уточнения, блокирования или уничтожения ПДн, право отозвать согласие на обработку ПДн и т.п. Таким образом, юридически корректным было бы указание в ответе на запрос следующего: обработка Ваших ПДн влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту ПДн и предусмотренных ст.14 ФЗ «О персональных данных»).

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 3 к Регламенту
Пример ответа на запрос субъекта ПДн

Исх. № 1 от 01.03.2019 г.

Иванову Ивану Ивановичу
Адрес: 353551 Краснодарский край Темрюкский район ст. Запорожская, ул. Таманской дивизии, дом 35

Уважаемый Иван Иванович!

Руководствуясь положениями ст. ст. 14, 20 Федерального закона РФ «О персональных данных» от 27 июля 2006 г. № 152-ФЗ сообщаем Вам, что Администрация Темрюкского городского поселения Темрюкского района обрабатывает Ваши персональные данные

1. Цель обработки Ваших персональных – *бухгалтерский и кадровый учет, регистрация сведений, необходимых для оказания муниципальных услуг*

2. Способы обработки Ваших персональных данных – смешанная обработка.

3. Лица, имеющие доступ к Вашим персональным данным:
   - *Главный специалист*
   - *Ведущий специалист*

4. Доступ к Вашим персональным данным может быть предоставлен *заместителю главы Темрюкского городского поселения Темрюкского района.* Также, по основаниям, предусмотренным действующим законодательством, доступ к Вашим персональным данным может быть предоставлен органам, осуществляющим оперативно-розыскную деятельность, органам дознания, следствия, суда.

5. Перечень обрабатываемых персональных данных: фамилия, имя, отчество, серия и номер паспорта, дата рождения, адрес места рождения, адрес места жительства/прописки, ИНН, СНИЛС, номер телефона, семейное положение, состав семьи, образование, профессия, должность, стаж, сведения о воинской обязанности, сведения об имуществе. Источник получения персональных данных – *документы, предъявляемые Вами при устройстве на работу.*

6. Срок обработки Ваших персональных данных – *до момента Вашего увольнения, до момента прекращения оказания Вам муниципальных услуг.*

7. Обработка Ваших персональных данных влечет для Вас в качестве юридических последствий возникновение у Вас прав, присущих субъекту ПДн и предусмотренных ст. 14 ФЗ «О персональных данных», а именно: право на

доступ к своим ПДн, право на получение сведений об операторе, право требовать уточнения, блокирования или уничтожения ПДн, право отозвать согласие на обработку ПДн и т.п.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 13
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) разработана с учетом Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним внутренними нормативными правовыми актами.

1.2. Настоящая Инструкция определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Тематика внутреннего контроля

2.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

Соответствие полномочий пользователя разрешительной системе доступа;

Соблюдение пользователями информационных систем персональных данных парольной политики;

Соблюдение пользователями информационных систем персональных данных антивирусной политики;

Соблюдение пользователями информационных систем персональных данных правил работы с машинными носителями персональных данных;

Соблюдение правил работы с средствами криптографической защиты;

Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

Соблюдение порядка резервирования баз данных и хранения резервных копий;

Соблюдение порядка работы со средствами защиты информации.

2.2. Соблюдение правил хранения и работы с бумажными носителями персональных данных.

3. Порядок проведения внутренних проверок

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Администрация организует проведение периодических проверок условий обработки персональных данных.

3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее – Ответственный) либо комиссией, образуемой руководством Администрации.

3.3. Внутренние проверки проводятся в соответствии с Планом внутренних проверок, составленным Ответственным либо Председателем комиссии и утвержденным руководством Администрации. Форма Плана приведена в Приложении №1 к настоящей Инструкции. При необходимости План может быть изменен.

3.4. План внутренних проверок составляется в декабре текущего года на следующий год и включает в себя все тематики проверок, равномерно распределенные на весь год.

3.5. Очередность и объем проверок определяется Ответственным либо Председателем комиссии самостоятельно.

3.6. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.7. Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении №2 к настоящей Инструкции.

3.8. При выявлении нарушений в ходе проверки Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.9. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным либо комиссией самостоятельно в январе следующего за проверочным годом.

3.10. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю докладывает Ответственный либо Председатель комиссии.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение №1
к инструкции осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Темрюкского городского поселения Темрюкского района

План
внутренних проверок условий обработки персональных данных

№	Тема проверки	Нормативный документ предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя разрешительной системе доступа	Разрешительная система доступа		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Инструкция пользователя		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики	Инструкция по антивирусной защите		
4.	Соблюдение пользователями информационных систем персональных данных правил работы с машинными носителями персональных данных	Инструкция по работе со съёмными носителями		
5.	Соблюдение правил работы с средствами криптографической защиты	Инструкция по работе с средствами криптографической защиты		

№	Тема проверки	Нормативный документ предъявляющий требования	Срок проведения	Исполнитель
6.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Порядок доступа сотрудников в помещения где ведётся обработка персональных данных		
7.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Инструкция о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных		
8.	Соблюдение порядка работы со средствами защиты информации	Инструкция пользователя информационных систем персональных данных, инструкция администратора информационных систем персональных данных по обеспечению безопасности персональных данных		
9.	Соблюдение правил хранения и работы с бумажными носителями персональных данных.	Инструкция по порядку учета и хранению документов, содержащих персональные данные		

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение №2
к инструкции осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации Темрюкского городского поселения Темрюкского района

Протокол
проведения внутренней проверки условий обработки персональных данных

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка

_____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями

_____
_____.
(название документа)

В ходе проверки проверено:

_____
_____
_____
_____.

Выявленные нарушения:

_____
_____
_____.

Меры по устранению нарушений:

_____
_____
_____
_____.

Срок устранения нарушений: _____.

Должность Ответственного _____И.О. Фамилия
либо
Председатель комиссии _____И.О. Фамилия
Члены комиссии:
Должность _____И.О. Фамилия
Должность _____И.О. Фамилия

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 14
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ПОЛИТИКА
обработки персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Политика обработки персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в Администрации персональных данных, функции Администрации при обработке персональных данных, права субъектов персональных данных, а также реализуемые Администрацией требования к защите персональных данных.

1.2. Политика разработана с учетом требований Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

1.3. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих в Администрации вопросы обработки персональных данных Администрации и других субъектов персональных данных.

2. Законодательные и иные нормативные правовые акты Российской Федерации, в соответствии с которыми определяется Политика обработки персональных данных в администрации

2.1. Политика обработки персональных данных в Администрации определяется в соответствии со следующими нормативными правовыми актами:

Трудовой кодекс Российской Федерации;

Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 06 марта 1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»;

постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

постановление Правительства Российской Федерации от 6 июля 2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ Роскомнадзора от 05 сентября 2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти.

2.2. В целях реализации положений Политики в Администрации разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

Положение об обработке персональных данных в Администрации;

Порядок доступа Администрации в помещения, где ведётся обработка персональных данных;

Правила работы с обезличенными персональными данными в Администрации;

Регламент порядка действий Администрации при обращении либо при получении запроса субъекта персональных данных или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных;

Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Администрации;

Иные локальные нормативные акты и документы, регламентирующие в Администрации вопросы обработки персональных данных.

3. Основные термины и определения, используемые в локальных нормативных актах администрации, регламентирующие вопросы обработки персональных данных

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

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

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных

данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемые 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.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

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

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

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

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

4. Принципы и цели обработки персональных данных

4.1. Администрация, являясь оператором персональных данных, осуществляет обработку персональных данных Администрации и других субъектов персональных данных, не состоящих с Администрацией в трудовых отношениях.

4.2. Обработка персональных данных в Администрации осуществляется с учетом необходимости обеспечения защиты прав и свобод Администрации и других субъектов персональных данных, в том числе защиты права на

неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

обработка персональных данных осуществляется в Администрации на законной и справедливой основе;

обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

обработке подлежат только персональные данные, которые отвечают целям их обработки;

содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Администрацией принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Персональные данные обрабатываются в Администрации в целях:

обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Администрации;

осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Администрацию, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

регулирования трудовых отношений с сотрудниками Администрации (содействие в трудоустройстве, обучение и продвижение по службе,

обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);

защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

подготовки, заключения, исполнения и прекращения договоров с контрагентами;

обеспечения пропускного режима в Администрации;

осуществления прав и законных интересов Администрации в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Администрации, или третьих лиц либо достижения общественно значимых целей;

в иных законных целях.

5. Перечень субъектов, персональные данные которых обрабатываются в администрации

5.1. В администрации обрабатываются персональные данные следующих категорий субъектов:

сотрудников;

жителей муниципального образования.

6. Перечень персональных данных, обрабатываемых в Администрации

6.1. Перечень персональных данных, обрабатываемых в Администрации, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Администрации с учетом целей обработки персональных данных, указанных в разделе 4 Политики.

6.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Администрации не осуществляется.

7. Функции Администрации при осуществлении обработки персональных данных

7.1. Администрация при осуществлении обработки персональных данных:

принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных;

принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

назначает лицо, ответственное за организацию обработки персональных данных в Администрации;

издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Администрации;

осуществляет ознакомление Администрации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных сотрудников;

публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8. Условия обработки персональных данных в Администрации

8.1. Обработка персональных данных в Администрации осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

8.2. Администрация без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

8.3. Администрация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

8.4. В целях внутреннего информационного обеспечения Администрация может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия,

имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

8.5. Доступ к обрабатываемым в Администрации персональным данным разрешается только сотрудникам Администрации, согласно перечня должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Администрации.

9. Перечень действий с персональными данными и способы их обработки

9.1. Администрация осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

9.2. Обработка персональных данных в Администрации осуществляется следующими способами:

неавтоматизированная обработка персональных данных;

автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

смешанная обработка персональных данных.

10. Права субъектов персональных данных

10.1. Субъекты персональных данных имеют право на:

полную информацию об их персональных данных, обрабатываемых в Администрации;

доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

отзыв согласия на обработку персональных данных;

принятие предусмотренных законом мер по защите своих прав;

обжалование действия или бездействия Администрации, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

осуществление иных прав, предусмотренных законодательством Российской Федерации.

11. Меры, принимаемые Администрацией для обеспечения выполнения обязанностей оператора при обработке персональных данных

11.1. Меры, необходимые и достаточные для обеспечения выполнения Администрацией обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

наличие ответственного за обработку персональных данных;

наличие администратора информационных систем персональных данных;

наличие утвержденных инструкций, регламентирующих работу с персональными данными и информационными системами персональных данных;

осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

ознакомление всех сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных под роспись;

учет машинных носителей персональных данных;

обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

наличие правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных;

определён перечень сотрудников, осуществляющих обработку персональных данных;

сведения на бумажных носителях хранятся в сейфах или выделенных помещениях;

определены места хранения персональных данных;

ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);

обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Администрации, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Администрации.

12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов администрации в области персональных данных, в том числе требований к защите персональных данных

12.1. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в Администрации и локальным нормативным актам Администрации в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

12.2. Внутренний контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов Администрации в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных в Администрации.

12.3. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Администрации осуществляет Ответственный за организацию обработки персональных данных.

12.4. Работники Администрации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 15
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
администратора безопасности при использовании ресурсов объекта вычислительной техники администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Администратор безопасности ИСПДн (далее – Администратор безопасности) назначается распоряжением главы Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Администратор безопасности подчиняется главе Администрации.

1.3. Администратор безопасности в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Администрации.

1.4. Администратор безопасности отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.5. Администратор безопасности является ответственным должностным лицом Администрации, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.6. Администратор безопасности должен иметь специальное рабочее место, размещенное в здании Администрации так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключением к ИСПДн, а также средствами контроля за техническими средствами защиты.

1.8. Администратор безопасности осуществляет методическое руководство Операторов и Администраторов ИСПДн, в вопросах обеспечения безопасности персональных данных.

1.9. Требования администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.10. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. Должностные обязанности

Администратор безопасности обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Осуществлять установку, настройку и сопровождение технических средств защиты.

2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.4. Участвовать в приемке новых программных средств.

2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8. Осуществлять контроль над выполнением Плана мероприятий по защите персональных данных.

2.9. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.10. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.11. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.12. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.13. Контролировать исполнение пользователями парольной политики.

2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.

2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.17. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.18. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.19. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.20. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.21. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.22. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Ответственность

3.1. В случае нарушения положений настоящей Инструкции Администратор безопасности несёт ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 16
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций в администрации Темрюкского городского поселения Темрюкского района

1. Назначение и область действия

1.1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей данной Инструкции является:

– определение мер защиты от прерывания;

– определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей Администрации, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

– системы жизнеобеспечения;

– системы обеспечения отказоустойчивости;

– системы резервного копирования и хранения данных;

– системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных в Приложении 1.

Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Администрации сотрудниками (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

– Уровень 1 – **Незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

– Уровень 2 – **Авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

- Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

- сбоя системы кондиционирования.

- Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу;

- сбоев общественного транспорта;

- эпидемии;

- массового отравления персонала;

- сильного снегопада;

- торнадо;

- сильных морозов.

– Уровень 3 – **Катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

– пожар в здании;

– взрыв;
– просадка грунта с частичным обрушением здания;
– массовые беспорядки в непосредственной близости от Объекта.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

– системы жизнеобеспечения;
– системы обеспечения отказоустойчивости;
– системы резервного копирования и хранения данных;
– системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

– пожарные сигнализации и системы пожаротушения;
– системы вентиляции и кондиционирования;
– системы резервного питания.

Все критичные помещения Администрации (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Инструкции о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных.

3.2. Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Администрации, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу.

По окончанию ознакомления сотрудник расписывается в инструкции.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение к инструкции
пользователя по обеспечению
безопасности обработки персональных
данных при возникновении
внештатных ситуаций в администрации
Темрюкского городского поселения
Темрюкского района

ИСТОЧНИКИ УГРОЗ

Технологические угрозы	
1	Пожар в здании
2	Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения)
3	Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением)
4	Химический выброс в атмосферу
Внешние угрозы	
5	Массовые беспорядки
6	Сбои общественного транспорта
7	Эпидемия
8	Массовое отравление персонала
Стихийные бедствия	
9	Удар молнии
10	Сильный снегопад
11	Сильные морозы
12	Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания
13	Затопление водой в период паводка
14	Наводнение, вызванное проливным дождем
15	Торнадо
16	Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод)
Телеком и ИТ угрозы	

17	Сбой системы кондиционирования
18	Сбой ИТ – систем
Угроза, связанная с человеческим фактором	
19	Ошибка персонала, имеющего доступ к серверной
20	Нарушение конфиденциальности, целостности и доступности конфиденциальной информации
Угрозы, связанные с внешними поставщиками	
21	Отключение электроэнергии
22	Сбой в работе интернет-провайдера
23	Физически разрыв внешних каналов связи

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 17
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

КОНЦЕПЦИЯ
информационной безопасности информационных систем персональных данных

1. Определения

1.1. В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

3. Введение

3.1. Настоящая Концепция информационной безопасности ИСПДн Администрации Новотаманского сельского поселения Темрюкского района (далее – Администрация) является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности Администрации.

3.2. Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов при обработке информации вообще, и персональных данных в частности.

3.3. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Администрации. Концепция определяет основные требования и базовые

подходы к их реализации, для достижения требуемого уровня безопасности информации.

3.4. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

3.5. Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

3.6. Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Администрации, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

3.7. Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Администрации;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

– координации деятельности структурных подразделений Администрации при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Администрации.

3.8. Область применения Концепции распространяется на все подразделения Администрации, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

3.9. Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных (ПДн).

4. Общие положения

4.1. Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Администрации, в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

4.2. СЗПДн представляет собой совокупность 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.

4.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.4. 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. Эти меры призваны обеспечить:

– **конфиденциальность** информации (защита от несанкционированного ознакомления);

– **целостность** информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

4.6. Стадии создания СЗПДн включают:

– предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;

– стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

– стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

4.7. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие)

предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

– инструкцию администратора информационных систем персональных данных по обеспечению безопасности персональных данных;

– инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных;

– инструкцию ответственного за обработку персональных данных;

– инструкцию по организации антивирусной защиты;

– инструкцию по порядку учета и хранению документов, содержащих персональные данные;

– инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ);

– инструкцию по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных);

– инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных;

– инструкцию осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

– инструкцию пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций.

4.8. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

4.9. Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Администрации.

5. Задачи СЗПДн

5.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

5.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

– защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

– к информации, циркулирующей в ИСПДн;

– средствам вычислительной техники ИСПДн;

– аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

– регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

– контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

– защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

– защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

– защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

– обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

– своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

6. Объекты защиты

6.1. Перечень информационных систем.

В Администрации Темрюкского городского поселения Темрюкского района производится обработка персональных данных в информационных система обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании внутреннего обследования.

6.2. Перечень объектов защиты.

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, обрабатываемых в Администрации Темрюкского городского поселения Темрюкского района.

Объекты защиты включают:

– обрабатываемая информация;

– технологическая информация;

– программно-технические средства обработки;

– средства защиты ПДн;

– каналы информационного обмена и телекоммуникации;

– объекты и помещения, в которых размещены компоненты ИСПДн.

7. Классификация пользователей ИСПДн

7.1. Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник Администрации, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

7.2. Пользователи ИСПДн делятся на три основные категории:

7.2.1. Администратор ИСПДн. Сотрудники Администрации, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

– обладает полной информацией о технических средствах и конфигурации ИСПДн;

– имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

– обладает правами конфигурирования и административной настройки технических средств ИСПДн.

7.2.2. Программист-разработчик ИСПДн. Сотрудники Администрации или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИСПДн обладает следующим уровнем доступа:

– обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

– обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

7.2.3. Оператор ИСПДн. Сотрудники подразделений Администрации участвующих в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

7.3. Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

7.4. Все выявленные группы пользователей отражаются в Перечне должностей работников, допущенных к работе с персональными данными и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в Администрации Темрюкского городского поселения Темрюкского района. На основании обследования определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих Администрации Темрюкского городского поселения Темрюкского района.

8. Основные принципы построения системы комплексной защиты информации

8.1. Построение системы обеспечения безопасности ПДн ИСПДн Администрации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;
– системность;
– комплексность;
– непрерывность;
– своевременность;
– преемственность и непрерывность совершенствования;
– персональная ответственность;
– минимизация полномочий;
– взаимодействие и сотрудничество;
– гибкость системы защиты;
– открытость алгоритмов и механизмов защиты;
– простота применения средств защиты;
– научная обоснованность и техническая реализуемость;
– специализация и профессионализм;
– обязательность контроля.

8.2. Законность.

8.2.1. Предполагает осуществление защитных мероприятий и разработку СЗПДн Администрации в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

8.2.2. Пользователи и обслуживающий персонал ПДн ИСПДн Администрации должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

8.3. Системность.

8.3.1. Системный подход к построению СЗПДн Администрации предполагает учет всех взаимосвязанных, взаимодействующих и

изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Администрации.

8.3.2. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

8.4. Комплексность.

8.4.1. Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

8.4.2. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

8.4.3. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

8.5. Непрерывность защиты ПДн.

8.5.1. Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

8.5.2. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

8.5.3. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных

программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

8.6. Своевременность.

8.6.1. Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации, в частности.

8.6.2. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

8.7. Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

8.8. Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

8.9. Принцип минимизации полномочий.

8.9.1. Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

8.9.2. Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

8.10. Взаимодействие и сотрудничество.

8.10.1. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Администрации, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

8.10.2. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

8.11. Гибкость системы защиты ПДн.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной

гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

8.12. Открытость алгоритмов и механизмов защиты.

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

8.13. Простота применения средств защиты.

8.13.1. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

8.13.2. Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

8.14. Научная обоснованность и техническая реализуемость.

8.14.1. Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

8.14.2. СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

8.15. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Администрации.

8.16. Обязательность контроля.

8.16.1. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

8.16.2. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен

осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

9. Меры, методы и средства обеспечения требуемого уровня защищенности

9.1. Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

– законодательные (правовые);
– морально-этические;
– организационные (административные);
– физические;
– технические (аппаратные и программные).

9.2. Законодательные (правовые) меры защиты.

9.2.1. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

9.2.2. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

9.3. Морально-этические меры защиты.

9.3.1. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

9.3.2. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

9.4. Организационные (административные) меры защиты.

9.4.1. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего

персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

9.4.2. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

9.4.3. Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

9.4.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;

– формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

– принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Администрации в целом;

– обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

9.4.5. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

9.4.6. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

– какова область применения политики безопасности ПДн;

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн, а также их установить ответственность;

– кто имеет права доступа к ПДн;

– какими мерами и средствами обеспечивается защита ПДн;

– какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

9.4.7. Организационные меры должны:

– предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

– определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

– организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

9.4.8. Организационные меры должны состоять из:

– регламента доступа в помещения ИСПДн;

– порядок допуска сотрудников к использованию ресурсов ИСПДн Администрации;

– регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

– регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

– инструкций пользователей ИСПДн (администратора ИСПДн, пользователя ИСПДн);

– инструкция пользователя при возникновении внештатных ситуаций.

9.5. Физические меры защиты.

9.5.1. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

9.5.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

9.6. Аппаратно-программные средства защиты ПДн.

9.6.1. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

9.6.2. С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

– средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Администрации;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства защиты ПДн.

9.6.3. Успешное применение технических средств защиты на основании принципов (раздел 8) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

– обеспечена физическая целостность всех компонент ИСПДн;

– каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании приказов руководства Администрации;

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

– специалистами Администрации осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10. Контроль эффективности системы защиты

10.1. Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

10.2. Контроль может проводиться как администраторами ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

10.3. Контроль может осуществляться администратором ИСПДн как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

10.4. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

11. Сферы ответственности за безопасность ПДн

11.1. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является глава Темрюкского городского поселения Темрюкского района. Глава Темрюкского городского поселения Темрюкского района может делегировать часть полномочий по обеспечению безопасности персональных данных.

11.2. Сфера ответственности руководителя учреждения включает следующие направления обеспечения безопасности ПДн:

– планирование и реализация мер по обеспечению безопасности ПДн;

– анализ угроз безопасности ПДн;

– разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

– контроль защищенности ИТ инфраструктуры Администрации от угроз ИБ путем;

– обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

– предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

11.3. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 6), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

12. Модель нарушителя безопасности

12.1. Под нарушителем в Администрации понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 6).

12.2. Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

– внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

– внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

12.3. Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

13. Модель угроз безопасности

13.1. Для ИСПДн Администрации выделяются следующие основные категории угроз безопасности персональных данных:

13.1.1. Угрозы от утечки по техническим каналам.

13.1.2. Угрозы несанкционированного доступа к информации:

– угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

– угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

– угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

– угрозы преднамеренных действий внутренних нарушителей;

– угрозы несанкционированного доступа по каналам связи;

– описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн.

14. Механизм реализации Концепции

14.1. Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

– федеральных законов в области обеспечения информационной безопасности и защиты информации;

– постановлений Правительства Российской Федерации;

– руководящих, организационно-распорядительных и методических документов ФСТЭК России;

– потребностей ИСПДн в средствах обеспечения безопасности информации.

15. Ожидаемый эффект от реализации Концепции

15.1. Реализация Концепции безопасности ПДн в ИСПДн позволит:

– оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности,

определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

– разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

– провести классификацию и сертификацию ИСПДн;

– провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

– обеспечить необходимый уровень безопасности объектов защиты.

15.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.

16. Список использованных источников

16.1. Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

– Федеральный Закон от 27.07.2006 .г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012 г. № 1119.

– «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

– «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

16.2. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее – ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

– Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 18
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.19 № 184-р

ПОЛИТИКА
информационной безопасности информационных систем персональных данных

1. Определения

1.1. В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения

персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые пользователем ИСПДн в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения пользователем ИСПДн или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

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

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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение

(в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Пользователь ИСПДн – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение

информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных пользователем ИСПДн через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

3. Введение

3.1. Настоящая Политика информационной безопасности Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) является официальным документом.

3.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПД Администрации.

3.3. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11.11.2007 г. № 781 «Об утверждении

Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

– «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008г.;

– «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

3.4. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Администрации.

4. Общие положения

4.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Администрации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

4.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

4.4. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

4.5. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

4.6. Состав ИСПДн, подлежащих защите, представлен в Перечене ИСПДн.

5. Область действия

5.1. Требования настоящей Политики распространяются на всех сотрудников Администрации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

6. Система защиты персональных данных

6.1. Система защиты персональных данных (СЗПДн), строится на основании:

– перечня персональных данных, подлежащих защите;

– акта классификации информационной системы персональных данных;

– модели угроз безопасности персональных данных;

– положения о разграничении прав доступа к обрабатываемым персональным данным;

– руководящих документов ФСТЭК и ФСБ России.

6.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Администрации. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Пляне мероприятий по обеспечению защиты ПДн.

6.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

– АРМ пользователей;

– сервера приложений;

– СУБД;

– граница ЛВС;

– каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

6.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

– антивирусные средства для рабочих станций пользователей и серверов;

– средства межсетевого экранирования;

– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

6.5. Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

– управление и разграничение доступа пользователей;

– регистрацию и учет действий с информацией;

– обеспечение целостности данных;

– обнаружение вторжений.

6.6. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и

утверждены директором Администрации или лицом, ответственным за обеспечение защиты ПДн.

7. Требования к подсистемам СЗПДн

7.1. СЗПДн включает в себя следующие подсистемы:

– управления доступом, регистрации и учета;

– обеспечения целостности и доступности;

– антивирусной защиты;

– межсетевого экранирования;

– анализа защищенности;

– обнаружения вторжений;

– криптографической защиты.

7.2. Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в Акте классификации информационной системы персональных данных.

7.3. Подсистемы управления доступом, регистрации и учета.

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

– идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

– идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

– идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

– регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

– регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

7.4. Подсистема обеспечения целостности и доступности.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных

средств ИСПДн Администрации, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

7.5. Подсистема антивирусной защиты.

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Администрации.

Средства антивирусной защиты предназначены для реализации следующих функций:

– резидентный антивирусный мониторинг;

– антивирусное сканирование;

– скрипт-блокирование;

– централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

7.6. Подсистема межсетевого экранирования.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

– фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;

– фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

– идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;

– регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

– контроля целостности своей программной и информационной части;

– фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

– регистрации и учета запрашиваемых сервисов прикладного уровня;

– блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

– контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

7.7. Подсистема анализа защищенности.

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.8. Подсистема обнаружения вторжений.

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

7.9. Подсистема криптографической защиты.

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Администрации, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

8. Пользователи ИСПДн

8.1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

8.2. В ИСПДн Администрации можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

– Администратор ИСПДн;

– Пользователь ИСПДн.

8.3. Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Разрешительной системе доступа сотрудников к ресурсам информационных систем персональных данных, принадлежащих Администрации Темрюкского городского поселения Темрюкского района.

8.4. Администратор ИСПДн.

Администратор ИСПДн, сотрудник Администрации, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного Пользователя ИСПДн к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

– обладает полной информацией о технических средствах и конфигурации ИСПДн;

– имеет доступ ко всем техническим средствам обработки информаций и данным ИСПДн;

– обладает правами конфигурирования и административной настройки технических средств ИСПДн.

8.5. Пользователь ИСПДн.

Пользователь ИСПДн – сотрудник Администрации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь ИСПДн не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

– располагает конфиденциальными данными, к которым имеет доступ.

9. Требования к персоналу по обеспечению защиты ПДн

9.1. Все сотрудники Администрации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

9.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.4. Сотрудники Администрации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.5. Сотрудники Администрации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

9.6. Сотрудники Администрации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях,

когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

9.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Администрации, третьим лицам.

9.9. При работе с ПДн в ИСПДн сотрудники Администрации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

9.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

9.11. Сотрудники Администрации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

9.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

10. Должностные обязанности пользователей ИСПДн

10.1. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

– инструкция администратора ИСПДн;
– инструкция пользователя ИСПДн;
– инструкция о порядке резервирования и восстановления;
– инструкция по антивирусной защите;
– инструкция пользователя СКЗИ;
– инструкция по работе с документами с ПДн;
– инструкция по учету машинных носителей;
– регламент реагирования на запрос субъекта ПДн;
– инструкция пользователя при возникновении внештатных ситуаций;
– инструкция по организации парольной защиты;
– инструкция по организации защиты информации о событиях безопасности в ИСПДн;

– инструкция по установке и модификации по;

– инструкция по обеспечению защиты информации при выводе ИСПДн из эксплуатации.

11. Ответственность сотрудников

11.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

11.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

11.3. Администратор ИСПДн несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

11.4. При нарушениях сотрудниками Администрации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

11.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Администрации.

11.6. Необходимо внести в Положения о подразделениях Администрации, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

12. Список использованных источников

12.1. Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

– Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 01.11.2012 г. № 1119.

– «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

– «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

12.2. Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

– Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 19
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.19 № 184-р

ИНСТРУКЦИЯ
по организации парольной защиты информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации парольной защиты информационных систем персональных данных в Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на всех пользователей информационных систем персональных данных (далее – Пользователь).

1.3. Пользователем является каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

2. Организация парольной защиты

2.1. Пароли доступа к элементам информационной системы персональных данных создаются Администратором безопасности информационной системы персональных данных.

2.2. Правила смены личных паролей:

Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.

Внеплановая смена (удаление) личного пароля любого пользователя информационных систем персональных данных в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри банка) должна производится немедленно после окончания последнего сеанса работы данного пользователя системы.

Внеплановая полная смена всех паролей должна производится в случае прекращения полномочий (увольнение, переход на другую должность и другие обстоятельства) администраторов информационных систем персональных данных и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо

полномочия по управлению подсистемой защиты информации данной системы, а значит, кроме личного пароля им могут быть известны пароли других пользователей системы.

Администратор безопасности информационной системы персональных данных оказывает необходимую помощь пользователям в процессе смены пароля.

2.3. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

Запрещается выбирать пароли, которые уже использовались ранее.

2.4. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан и с учётом текущей раскладки клавиатуры.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

2.5. Правила хранения пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

2.6. Действия в случае утери и компрометации пароля:

В случае утери пароля сотрудник получает у Администратора безопасности информационной системы персональных данных новый пароль.

В случае компрометации пароля (подсматривание кем-либо, разглашение пароля и др.) пароль необходимо сменить в соответствии с вышеуказанными требованиями.

2.7. Лица, использующие паролирование, обязаны:

Четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию. .

Своевременно сообщать Администратору безопасности информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

По первому требованию Администратора безопасности информационной системы персональных данных предъявлять значения действующего личного пароля для контроля соответствия установленным требованиям, а после проверки провести немедленную его смену

3. Ответственность

3.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

3.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.

3.3. Владельцы паролей должны под расписку быть ознакомлены с данной инструкцией.

3.4. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 20
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по организации защиты информации о событиях безопасности в информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации защиты информации о событиях безопасности в информационных систем персональных данных в администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных (далее – Администратор).

2. События безопасности

2.1. К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, принадлежащих Администрации, должны быть отнесены любые проявления состояния информационных систем персональных данных и системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационных систем персональных данных, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.

2.2. В информационных системах персональных данных Администрации подлежат регистрации следующие события:

– вход/выход, а также попытки входа пользователей в информационные системы персональных данных и загрузки/останова операционной системы;

– подключение машинных носителей информации и вывод информации на носители информации;

– запуск/завершение программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

– попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам,

записям, полям записей) и иным объектам доступа;

– попытки удаленного доступа.

2.3. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечивать возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

2.3.1. При регистрации входа/выхода пользователей в информационные системы персональных данных и загрузки/останова операционной системы состав и содержание информации должны, как минимум, включать дату и время входа/выхода в систему/из системы или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки/останова операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.3.2. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.3.3. При регистрации запуска/завершения программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.3.4. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.3.5. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.3.6. При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3. Защита информации о событиях безопасности

3.1. В информационных системах персональных данных Администрации должна обеспечиваться защита информации о событиях безопасности.

3.2. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.3. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

3.4. Требования к защите информации о событиях безопасности:

– в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита);

– в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (не перезаписываемые носители информации);

– в информационных системах персональных данных для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы;

– оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу сотрудников.

4. Ответственность

4.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

4.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 21
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.19 № 184-р

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации Темрюкского городского поселения Темрюкского района (далее – Администрация), включает в себя описание комплекса организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников Администрации, использующих в работе информационные систем персональных данных, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

1.3. Должностные лица Администрации, задействованные в обеспечении функционирования информационных систем персональных данных Администрации, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.4. Ознакомление с требованиями Инструкции пользователей информационных систем персональных данных осуществляет Администратор безопасности информационных систем персональных данных под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

1.5. Непосредственное исполнение настоящей Инструкции определяется Администратором безопасности информационных систем персональных данных по согласованию с ответственным за организацию обработки безопасности персональных данных Администрации.

2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств рабочих станций Администрации должны производиться только на основании заявок, согласованных с Администратором безопасности информационных систем персональных данных.

2.2. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности информационных систем персональных данных Администрации, должны производиться только на основании заявок, согласованных с руководством Администрации и Администратором безопасности информационных систем персональных данных. При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

2.3. Все изменения конфигурации технических и программных средств, входящих в состав аттестованных по требованиям безопасности информационных систем персональных данных Администрации, отражаются в Техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации, без уведомления об предполагаемых изменениях организацию, производившую аттестацию.

2.4. В заявке указываются наименование компьютера и ответственный за него сотрудник. После чего заявка передается Администратору безопасности информационных систем персональных данных для исполнения работ по внесению изменений в конфигурацию программного обеспечения и аппаратных средств информационных систем персональных данных Администрации.

2.5. Право внесения изменений в конфигурацию аппаратно-программных средств информационных систем персональных данных Администрации предоставляется Администратору безопасности информационных систем персональных данных, Администратору информационных систем персональных данных, а также ответственному за организацию обработки персональных данных. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо без согласования с Администратором безопасности информационных систем персональных данных и/или ответственным за организацию обработки персональных данных запрещено.

2.6. Установка и настройка программного средства осуществляются Администратором безопасности информационных систем персональных данных и/или Администратором информационных систем персональных данных согласно эксплуатационной документации.

2.7. Запрещается установка и использование на персональных электронных вычислительных машинах (серверах) программного обеспечения, не входящего в Перечень программного обеспечения, разрешенного к

использованию в информационных систем персональных данных Администрации Темрюкского городского поселения Темрюкского района (Приложение № 1).

2.8. Администратор безопасности информационных систем персональных данных Администрации осуществляет контроль за отсутствием на компьютерах сотрудников программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.9. Установка (обновление) программного обеспечения (системного, тестового и т.п.) на средствах вычислительной техники производится с эталонных копий программных средств, хранящихся у Администратора информационных систем персональных данных. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

2.10. После установки (обновления) программного обеспечения Администратор информационных систем персональных данных должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и совместно с пользователем компьютера проверить правильность настройки средств защиты.

2.11. После завершения работ по внесению изменений в состав аппаратных средств рабочей станции ее системный блок должен закрываться Администратором безопасности информационных систем персональных данных на ключ (при наличии штатных механических замков) и опечатываться (пломбироваться, защищаться специальной наклейкой).

2.12. Администратор безопасности информационных систем персональных данных должен произвести соответствующую запись в «Журнале фактов вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств на элементах в ИСПДн» (Приложение № 2).

2.13. В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают Администратору безопасности информационных систем персональных данных. Использование программного средства до получения специальных указаний запрещается.

2.14. Оригиналы заявок (документов) или приказы, на основании которых производились изменения в составе технических или программных средств персональных электронных вычислительных машин с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у Администратора безопасности информационных систем персональных данных Администрации.

3. Порядок пересмотра инструкции

3.1. Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств информационных систем персональных данных Администрации, приводящих к существенным изменениям технологии обработки информации.

3.2. Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным организацию обработки персональных данных в Администрации.

3.3. Полный пересмотр данного документа проводится ответственным за организацию обработки персональных данных Администрации с целью проверки соответствия положений данного документа реальным условиям применения их в информационных систем персональных данных Администрации.

3.4. Вносимые изменения не должны противоречить другим положениям Инструкции.

4. Ответственные за организацию и контроль выполнения инструкции

4.1. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на Администратора безопасности информационных систем персональных данных.

4.2. Ответственность за общий контроль информационной безопасности возлагается на ответственного за организацию обработки персональных данных Администрации.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 1
к инструкции по установке, модификации
и техническому обслуживанию
программного обеспечения и аппаратных
средств информационной системы
персональных данных администрации
Темрюкского городского поселения
Темрюкского района

Перечень программного обеспечения, разрешенного к использованию в информационных систем персональных данных администрации Темрюкского городского поселения Темрюкского района

- Microsoft Office (OpenOffice) – набор программ для работы с текстовыми документами, электронными таблицами, презентациями;
- Adobe Acrobat Reader – программа просмотра PDF-документов;
- 7-ZIP – программа для работы с электронными архивами;
- KES – антивирусный пакет;
- правовые системы (Гарант, Консультант-плюс);
- дополнительное программное обеспечение, требуемое для выполнения специализированных задач – данное программное обеспечение устанавливается сотрудниками Администрации по предварительной заявке пользователя с учётом наличия официально приобретённой или бесплатно распространяемой версии данной программы и рассмотрения возможности установки её на компьютер пользователя.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 2
к инструкции по установке, модификации и
техническому обслуживанию программного
обеспечения и аппаратных средств
информационной системы персональных данных
администрации Темрюкского городского
поселения Темрюкского района

Журнал фактов вскрытия и опечатывания рабочих станций и серверов, выполнения профилактических работ, установки и модификации программных средств на элементах в ИСПДн

№ п.п	Дата	Описание выполненной работы	ФИО исполнителей и их подписи	ФИО пользователя, подпись
1	2	3	4	5
1.				
2.				

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 22
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в администрации Темрюкского городского поселения Темрюкского района

1.Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных Администрации (далее – Администратор).

2. Порядок защиты информации

2.1. Обеспечение защиты информации при выводе из эксплуатации информационных систем персональных данных или после принятия решения об окончании обработки информации осуществляется Администратором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности Администрации.

2.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы персональных данных или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

2.4. Факт уничтожения данных, находившихся на машинных носителях информации оформляется актом за подписью Администратора. Форма Акта приведена в Приложении № 1.

2.5. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

3. Ответственность

3.1. Ответственность за обеспечение защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации возлагается на Администратора.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 1
к инструкции по обеспечению защиты
информации при выводе
информационных систем персональных
данных из эксплуатации или после
принятия решения об окончании
обработки информации в администрации
Темрюкского городского поселения
Темрюкского района

АКТ
затирания остаточной информации, хранившейся
на машинных носителях

Все файлы, содержащие подлежащую защите информацию, находившиеся на машинном носителе

_____,
(модель, серийный номер машинного носителя)

выводимого их эксплуатации / передаваемого
(нужное подчеркнуть)

_____, (с
какой целью)

_____,
(кому: должность, Ф.И.О.)

уничтожены (затерты) посредством программы

_____.
(указать наименование программы)

Администратор безопасности информационных систем персональных данных

«___» _____ 20__ г. _____ _____
(подпись) (фамилия, инициалы)

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 22
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.2019 № 184-р

ИНСТРУКЦИЯ
по обеспечению защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в администрации Темрюкского городского поселения Темрюкского района

1.Общие положения

1.1. Настоящая Инструкция разработана с целью обеспечения защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации Темрюкского городского поселения Темрюкского района (далее – Администрация).

1.2. Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных Администрации (далее – Администратор).

2. Порядок защиты информации

2.1. Обеспечение защиты информации при выводе из эксплуатации информационных систем персональных данных или после принятия решения об окончании обработки информации осуществляется Администратором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности Администрации.

2.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы персональных данных или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

2.4. Факт уничтожения данных, находившихся на машинных носителях информации оформляется актом за подписью Администратора. Форма Акта приведена в Приложении № 1.

2.5. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

3. Ответственность

3.1. Ответственность за обеспечение защиты информации при выводе информационных систем персональных данных из эксплуатации или после принятия решения об окончании обработки информации в Администрации возлагается на Администратора.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

Приложение № 1
к инструкции по обеспечению защиты
информации при выводе
информационных систем персональных
данных из эксплуатации или после
принятия решения об окончании
обработки информации в администрации
Темрюкского городского поселения
Темрюкского района

АКТ
затирания остаточной информации, хранившейся
на машинных носителях

Все файлы, содержащие подлежащую защите информацию, находившиеся на машинном носителе

_____,
(модель, серийный номер машинного носителя)

выводимого их эксплуатации / передаваемого
(нужное подчеркнуть)

_____, (с
какой целью)

_____,
(кому: должность, Ф.И.О.)

уничтожены (затерты) посредством программы

_____.
(указать наименование программы)

Администратор безопасности информационных систем персональных данных

«___» _____ 20__ г. _____ _____
(подпись) (фамилия, инициалы)

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев

ПРИЛОЖЕНИЕ № 23
к распоряжению администрации
Темрюкского городского поселения
Темрюкского района
от 30.08.19 № 184-р

ПОРЯДОК
уничтожения и блокирования персональных данных в администрации Темрюкского городского поселения Темрюкского района

1. Общие положения

1.1. Настоящий Порядок уничтожения и блокирования персональных данных (далее – Порядок) администрации Темрюкского городского поселения Темрюкского района (далее – Администрация) определяет условия и способы уничтожения:

- бумажных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных;
- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

2. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

2.1. Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.

2.2. В случае подтверждения факта недостоверности персональных данных работник, ответственный за организацию обработки персональных данных (далее – Ответственный), на основании документов, представленных субъектом персональных данных, обязан уточнить персональные данные и принять меры к их блокированию.

2.3. В случае выявления неправомерных действий с персональными данными Ответственный обязан устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

2.4. Об устранении допущенных нарушений или об уничтожении персональных данных Ответственный обязан уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также уведомить указанный орган.

2.5. Ответственный обязан уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных;
- отзыва субъектом персональных данных согласия на обработку своих персональных данных;
- в случае, указанном в п.2.3. настоящего Порядка.

2.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с момента наступления таких случаев.

2.7. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

3. Работа с бумажными носителями (документами)

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1.

Таблица 1

Виды и периоды уничтожения бумажных носителей, содержащих персональные данные

№ п/п	Документ	Срок хранения	Действия по окончании срока хранения
1.	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника	75 лет	Сдача в архив
2.	Документы, сведения, содержащие персональные данные субъектов персональных данных при предоставлении им муниципальных услуг	Установленные для данных документов сроки хранения	Уничтожение
3.	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учёта, списки доступа, иная документация и т.п.)	Хранятся до замены на новые, если не указан конкретный срок хранения	Уничтожение

3.2. По окончании срока хранения документы, указанные в п. 3.1. Порядка передаются в архив либо уничтожаются путём измельчения на мелкие

части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

4. Работа с машинными носителями информации

4.1. Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), дискетах 3,5“ 1.4 Mb (далее – FDD), FLASH-накопителях.

4.2. Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2.

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информационной системы Оператора Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД
2.	База данных автоматизированной информационной системы «1С Предприятие- Кадры»	Носитель: файлы на НЖМД сервера	До создания более актуальной копии Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД

4.3. Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. Порядка должны находиться в сейфе, опечатываемом печатью (кроме формируемых или обрабатываемых в данный момент на рабочем месте).

4.4. По окончании сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего их использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

4.5. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».

4.6. В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, FLASH применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

5. Порядок оформления документов об уничтожении носителей

5.1. Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая распоряжением главы.

5.2. В ходе процедуры уничтожения носителей персональных данных необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

5.3. Комиссия составляет и подписывает Акт об уничтожении носителей.

Глава Темрюкского городского поселения
Темрюкского района М.В. Ермолаев