ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ
АЛЕКСЕЕВСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
АЛЕКСЕЕВСК
МУНИЦИПАЛЬ РАЙОНЫНЫҢ
БАШКАРМА КОМИТЕТЫ

ПОСТАНОВЛЕНИЕ **КАРАР**

23.07.2020 п.г.т.Алексеевское № 290

Об утверждении
положения об обеспечении
безопасности персональных данных

Во исполнение требований Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», приказа 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» и приказа ФСТЭК России от 11 февраля 2013 года №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», и прочих нормативных документов по защите информации,

постановляю:

1. Утвердить и ввести в действие Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан (далее – Положение) (Приложение к настоящему Постановлению).
2. Ответственному за обеспечение безопасности персональных данных в информационных системах обеспечить выполнение требований Положения.
3. Требования Положения довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.
4. Контроль за исполнением настоящего постановления оставляю за собой.

И.о. руководителя
Исполнительного комитета **А.Д. Васильев**

Приложение
к постановлению
Исполнительного комитета
Алексеевского муниципального
района Республики Татарстан
от 23.07.2020 № 290

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан

1. Основные термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

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

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;

Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных;

Оператор – 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;

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

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;

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.

2. Общие положения

2.1. Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

2.3. Положение обязательно для исполнения всеми работниками Исполнительного комитета Алексеевского муниципального района Республики Татарстан (далее – Комитета), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.

3. Цели и задачи обеспечения безопасности персональных данных

3.1. Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3.2. Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в

соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3.3. СЗПДн в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.

4. Основные принципы построения системы защиты информации

4.1. СЗПДн основывается на следующих принципах:

- системности;
- комплексности;
- непрерывности защиты;
- разумной достаточности;
- гибкости;
- простоты применения средств защиты информации (далее – СЗИ).

4.2. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

4.3. Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

4.4. Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Комитета, и каждый работник должен принимать участие в этом процессе.

4.5. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.6. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.

4.7. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не

должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.

5. Основные мероприятия по обеспечению безопасности персональных данных

5.1.Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:

- определение ответственных лиц за обеспечение защиты ПДн;
- определение уровня защищенности ПДн;
- реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
- ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
- учет и хранение съемных машинных носителей ПДн;
- организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
- организация парольной защиты;
- организация антивирусной защиты;
- организация обновления программного обеспечения и СЗИ;
- использование СЗИ;
- использование средств шифровальной (криптографической) защиты информации (далее – СКЗИ);
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн.

5.2.Определение ответственных лиц за обеспечение безопасности ПДн

5.2.1. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:

- Руководитель Комитета.
- Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.
- Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.

– Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.

5.3.Определение уровня защищенности ПДн

5.3.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется, в соответствии с постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных», форма которого приведена в Приложении №1 к настоящему Положению.

5.4.Определение класса защищенности ИСПДн

5.4.1. Класс защищенности ИСПДн определяется в соответствии с требованиями приказа ФСТЭК России от 11 февраля 2013 года №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5.5.Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн

5.5.1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПЛн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан», утвержденным приказом Руководителя Комитета.

5.5.2. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом Руководителя Комитета, с максимальным удалением от её границ.

5.5.3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденными приказом Руководителя Комитета.

5.6.Учет и хранение съемных машинных носителей ПДн

5.6.1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Инструкцией по обращению со съемными машинными носителями персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденной постановлением Руководителя Комитета.

5.7.Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ

5.7.1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан», утвержденной постановлением Руководителя Комитета.

5.8.Организация парольной защиты

5.8.1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденной постановлением Руководителя Комитета.

5.9.Организация антивирусной защиты

5.9.1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты информации в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденным постановлением Руководителя.

5.10. Организация обновления программного обеспечения и СЗИ

5.10.1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан» и «Инструкцией администратора информационных систем персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан», утвержденным постановлением Руководителя Комитета.

5.11. Применение СЗИ

5.11.1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 года №184-ФЗ «О техническом регулировании».

5.11.2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.

5.12. Использование СКЗИ

5.12.1. Для обеспечения защиты ПДн, обрабатываемых в ИСНДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению с шифровальными (криптографическими) средствами защиты информации в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденным постановлением Руководителя Комитета.

5.13. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн

5.13.1. На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:

- предварительные испытания СЗПДн;
- опытную эксплуатацию СЗПДн;
- анализ уязвимостей ИСПДн и принятие мер по их устранению;
- приемочные испытания СЗПДн.

5.14. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер

5.14.1. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
- факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
- факты сбоя или некорректной работы систем обработки ПДн;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн, обрабатываемых в ИСПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.

5.14.2. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных Исполнительного комитета Алексеевского муниципального района Республики Татарстан», утвержденным постановлением Руководителя Комитета.

5.15.Контроль за принимаемыми мерами по обеспечению безопасности ПДн

5.15.1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в Исполнительном комитете Алексеевского муниципального района Республики Татарстан», утвержденным постановлением Руководителя Комитета.

6. Ответственность

6.1. Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.

6.2. Ответственность за доведение требований настоящего Положения до работников Комитета и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

Управляющий делами
Исполнительного комитета **Г.А. Юсупова**

Приложение № 1
к Положению об
обеспечении безопасности
персональных данных,
обрабатываемых в
информационных системах
персональных данных

ФОРМА

АКТ

«___» _____ 20__ г. № _____

Алексеевское

Определения уровня защищенности
персональных данных
в информационной системе
персональных данных
«_____»
(наименование информационной системы)

Комиссия в составе:
Председатель:
_____ _____
Члены комиссии:
1. _____ _____
2. _____ _____
3. _____ _____

на основании исходных данных об информационной системе персональных данных «_____»
(наименование информационной системы)
(далее – ИСПДн) определила:

1. В ИСПДн обрабатываются _____ категории
(биометрические, специальные, иные, общедоступные)
персональных данных _____ субъектов персональных данных
(менее 100 000, более 100 000)
_____ Исполнительного комитета Алексеевского
муниципального района Республики Татарстан;
((не) являющимися работниками)

2. ИСПДн располагается в пределах Российской Федерации;

3. Для ИСПДн актуальны угрозы 3 типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

в соответствии с постановлением Правительства РФ от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их

обработке в информационных системах персональных данных», установила необходимость обеспечения _____ уровня
(первого, второго, третьего, четвертого)
защищенности персональных данных.

Председатель:

_____ _____ _____

Члены комиссии:

_____ _____ _____

_____ _____ _____

_____ _____ _____

ЛИСТ ОЗНАКОМЛЕНИЯ

с постановлением Исполнительного комитета Алексеевского муниципального района Республики Татарстан от «___» _____ 2020 г. № _____ «Об утверждении положения об обеспечении безопасности персональных данных»

№ п/п	Фамилия имя отчество	Должность	Дата ознакомления	Подпись
1			«___» ___ 20__ г.	
2			«___» ___ 20__ г.	
3			«___» ___ 20__ г.	
4			«___» ___ 20__ г.	
5			«___» ___ 20__ г.	
6			«___» ___ 20__ г.	
7			«___» ___ 20__ г.	
8			«___» ___ 20__ г.	
9			«___» ___ 20__ г.	
10			«___» ___ 20__ г.	
11			«___» ___ 20__ г.	
12			«___» ___ 20__ г.	
13			«___» ___ 20__ г.	
14			«___» ___ 20__ г.	
15			«___» ___ 20__ г.	
16			«___» ___ 20__ г.	
17			«___» ___ 20__ г.	
18			«___» ___ 20__ г.	
19			«___» ___ 20__ г.	
20			«___» ___ 20__ г.	