

**Управление социальной защиты населения администрации
Юргинского муниципального округа**

УТВЕРЖДАЮ

Начальник управления социальной защиты
населения администрации Юргинского
муниципального округа



Кибе Л.С.

« 07 » _____ 2020г.

**Правила осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных**

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в управлении социальной защиты администрации Юргинского муниципального округа, определяющие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных в органе исполнительной власти и их подведомственных учреждениях.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник администрации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.4. Контрольные мероприятия по обеспечению уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн управления проводятся в следующих целях:

1.4.1 проверка выполнения требований организационно-распорядительной документации по защите информации в администрации действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.4.2 оценка уровня осведомленности и знаний работников администрации в области обработки и защиты персональных данных;

1.4.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в управлении разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в администрации.

2.3. Плановые контрольные мероприятия проводятся в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения

мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулируемыми органами;

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируются в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение руководству администрации.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных администрации.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных

мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.
- Соблюдение Порядка доступа в помещения администрации, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных
требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	
Контроль обновления ПО и единообразия применяемого ПО	Еженедельно	Ежемесячно	
Контроль обеспечения резервного копирования		Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	

ПРОТОКОЛ № _____
проведения внутренних проверок контроля соответствия обработки персональных данных
требованиям к защите персональных данных в _____

Настоящий Протокол составлен в том, что «__» _____ 201_ г.
_____ (комиссией)
(должность, Ф.И.О. сотрудника)

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: _____