

УТВЕРЖДЕНО:
Приказом Генерального директора
№ 3 от «14» апреля 2026г

МЕТОДИКА

**осуществления внутреннего контроля соответствия обработки и защиты персональных
данных требованиям законодательства о персональных данных и локальным нормативным
актам в Автономной некоммерческой организации "Центр регионального развития,
реализации социально значимых проектов и поддержки общественных инициатив
"Территория добра"**

1. Общие положения

1.1. Настоящая Методика осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства о персональных данных и локальным нормативным актам в Автономной некоммерческой организации "Центр регионального развития, реализации социально значимых проектов и поддержки общественных инициатив "Территория добра" (далее – Методика) регламентирует процесс проведения контроля состояния организации обработки и защиты персональных данных (далее – ПДн) (далее – Контроль) в Автономной некоммерческой организации "Центр регионального развития, реализации социально значимых проектов и поддержки общественных инициатив "Территория добра" (далее – Компания) и определяет перечень мероприятий, проводимых в рамках Контроля.

1.2. Методика разработана в соответствии с требованиями законодательства о ПДн и положениями локальных нормативных актов Компании, регламентирующими порядок обработки и защиты ПДн.

1.3. Методика предназначена для исполнения всеми работниками Компании, участвующими в процессе проведения Контроля.

1.4. Целями проведения Контроля являются:

- обеспечение соответствия деятельности Компании требованиям законодательства РФ в части обработки и защиты ПДн и локальных нормативных актов, регламентирующих обработку и защиту ПДн;
- оценка достаточности и эффективности реализованных мер обеспечения безопасности ПДн в рамках правовых, организационных и технических мер, реализуемых системой защиты ПДн (далее – СЗПДн);
- своевременное выявление несоответствий и выработка мер и рекомендаций по их устранению;

- мониторинг устранения выявленных несоответствий.

1.5. Настоящая Методика определяет:

- виды и сроки проведения Контроля;
- порядок планирования Контроля и инициации внепланового Контроля;
- порядок осуществления Контроля;
- порядок формирования результатов Контроля;
- мероприятия по результатам проведения Контроля.

1.6. Контроль в рамках настоящей Методики организуется и проводится лицом, ответственным за организацию обработки ПДн совместно с лицом, ответственным за обеспечение безопасности ПДн, (вместе – Ответственные лица) – в пределах своих полномочий и функций. В т.ч. при возникновении необходимости может быть образована внутренняя комиссия для проведения Контроля, состав которой утверждается приказом уполномоченного лица в Компании (далее – Уполномоченное лицо)¹.

2. Виды и сроки проведения Контроля

2.1. Контроль подразделяется на плановый и внеплановый.

2.1.1. Плановый Контроль осуществляется на основании **Плана осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям**

¹ Например, генеральным директором или иным уполномоченным в Компании лицом. При этом председателем Комиссии всегда должно быть лицо, ответственное за организацию обработки ПДн в Компании.

законодательства о ПДн и локальным нормативным актам (далее – План) по форме **Ошибка!**
Источник ссылки не найден. к Методике (далее – План).

2.1.2. Внеплановый Контроль может проводиться в случаях:

- поступления в Компанию запроса Роскомнадзора, связанного с нарушением прав субъекта ПДн;
- поступления информации о несоответствии в процессе и/или в ИСПДн;
- опубликования в СМИ или иных открытых источниках информации о нарушениях Компанией требований законодательства о ПДн;
- возникновения инцидента с ПДн, который может привести к нарушению безопасности ПДн и нарушению прав субъектов ПДн;
- выявления фактов не устранения или неполного устранения несоответствий, выявленных в ходе проведенного планового Контроля;
- в иных случаях, не относящихся к плановому Контролю.

2.2. Сроки проведения Контроля:

2.2.1. Плановый Контроль должен проводиться в Компании не реже 1 (одного) раза в год.

2.2.2. В случае проведения внепланового Контроля сроки его проведения определяются Ответственными лицами, а затем утверждаются Уполномоченным лицом.

3. Планирование Контроля

3.1. Плановый контроль проводится в соответствии с Планом, который разрабатывается, дополняется, актуализируется Ответственными лицами.

3.2. План не позднее, чем за _____² до проведения планового Контроля в установленном в Компании порядке утверждается приказом Уполномоченного лица о проведении Контроля, содержащий в т.ч.:

- сроки проведения;
- наименования структурных подразделений и ИСПДн, в отношении которых будет проводиться Контроль;
- перечень контрольных мероприятий;
- _____³

3.3. Утвержденный План рассылается структурным подразделениям, которые участвуют в процессах обработки ПДн.

4. Проведение Контроля

4.1. Ответственные лица, при проведении планового и внепланового Контроля, должны руководствоваться законодательством РФ о ПДн, а также локальными нормативными актами Компании, регламентирующими обработку и обеспечение безопасности ПДн.

4.2. Работники проверяемых структурных подразделений обязаны способствовать проведению планового и внепланового Контроля, представлять запрошенные Ответственными лицами сведения и документацию.

4.3. При проведении планового и внепланового Контроля Ответственные лица учитывают методы проведения Контроля, контрольные мероприятия, а также направления Контроля.

4.3.1. Методами проведения Контроля являются:

- интервьюирование;

² Указывается срок.

³ Указывается информация, которая содержится в приказе Уполномоченного лица.

- проверка документов;
- проверка действий работников при работе с ПДн;
- изучение технической информации.

4.3.2. Контрольные мероприятия⁴ включают в себя:

- проверку мероприятий по контролю за организацией обработки ПДн;
- проверку мер обеспечения безопасности ПДн, реализованных в рамках СЗПДн.

4.3.3. Направление Контроля может быть реализовано в виде:

4.3.3.1. Проверки документов:

- проверка наличия документов, регламентирующих организацию обработки ПДн⁵;
- проверка наличия перечней/реестров по организации обработки ПДн^{6 7};
- проверка наличия документов о назначении должностных лиц, ответственных за организацию обработки и обеспечение безопасности ПДн, а также действующих комиссий⁸;
- проверка осведомленности работников Компании об обработке ПДн⁹;
- проверка наличия функциональных обязанностей следующих должностных лиц, ответственных в части организации обработки и обеспечения безопасности ПДн¹⁰.

4.3.3.2. Проверки соблюдения прав субъектов ПДн:

- проверка актуальности сведений, содержащихся в Реестре операторов, осуществляющих обработку ПДн¹¹;
- проверка соответствия состава обрабатываемых ПДн заявленным целям обработки;
- проверка организации работы по сбору согласий субъектов ПДн;
- проверка порядка передачи информации, содержащей ПДн, третьим лицам и наличия оснований на передачу, в т.ч. способы передачи;
- проверка порядка ведения Журналов учета обращений и запросов субъектов ПДн и Надзорного органа и соблюдения их законных прав субъектов ПДн при обработке их ПДн в Компании;
- проверка иных обстоятельств, затрагивающих права и интересы субъекта ПДн.

4.3.3.3. Проверки обеспечения безопасности ПДн в ИСПДн:

- наличия модели угроз безопасности для каждой ИСПДн¹²;
- соответствия установленного уровня защищенности ИСПДн;
- наличия проекта системы защиты ИСПДн;

⁴ При проведении планового Контроля – указываются в Плане.

⁵ В частности, Политики в отношении обработки ПДн и размещения ее в открытом доступе (интернет-сайт, информационный стенд в офисе т. п.); Положения об обработке ПДн; Положения об обработке ПДн работников; Методики оценки вреда субъектам ПДн и иных документов, регламентирующих порядок обработки ПДн в Компании.

⁶ В частности, реестра процессов, в которых осуществляется обработка ПДн, перечня ИСПДн и иных перечней/реестров по организации обработки ПДн в Компании.

⁷ В ходе Контроля определяется необходимость актуализации перечней/реестров в связи с произошедшими изменениями (организационно-штатными, расположения, состава технических средств и т.п.).

⁸ В частности, документов, о назначении лица, ответственного за организацию обработки ПДн; о назначении лица, ответственного за обеспечение безопасности ПДн; о создании комиссии по уничтожению ПДн и иных документов по данному направлению.

⁹ В частности, подписанных работниками листов ознакомления с требованиями законодательства и локальных нормативных актов о ПДн; подписанных работниками обязательств о неразглашении конфиденциальной информации; подписанных уведомлений работников о факте обработки ПДн без использования средств автоматизации и иных документов Компании, подтверждающих осведомленность работников об обработке ПДн.

¹⁰ В частности, ответственного за организацию обработки ПДн; ответственного за обеспечение безопасности ПДн обрабатываемых в ИСПДн; работников, допущенных к обработке ПДн; администраторов и пользователей ИСПДн и иных лиц, имеющих доступ к ПДн.

¹¹ <https://pd.rkn.gov.ru/operators-registry/operators-list/>

¹² Также определяется необходимость пересмотра имеющихся угроз безопасности ИСПДн.

- полноты и качества выполнения организационных и технических мер, необходимых для поддержания установленного уровня защищенности ИСПДн;
- порядка установки (инсталляции) только разрешенного к использованию программного обеспечения и (или) его компонентов;
- наличия актов и (или) заключений о возможности использования средств защиты информации, в т.ч. криптографических;
- порядка уничтожения, удаления, обезличивания ПДн на машинных носителях;
- порядка реагирования на сбои при регистрации событий безопасности, в т.ч. аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- порядка обеспечения резервного копирования баз данных;
- состояния резерва технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования ИСПДн;
- обеспечения системой кондиционирования помещений серверных ИСПДн;
- организации системы бесперебойного питания серверов и средств вычислительной техники ИСПДн;
- иных обстоятельств, связанных с обеспечением безопасности ПДн в ИСПДн.

4.3.3.4. Проверки порядка доступа к ИСПДн:

- доведения до сведения работников Компании локальных нормативных актов по вопросам обработки и обеспечения безопасности ПДн¹³;
- наличия документов по допуску к ИСПДн;
- непосредственно доступа к ИСПДн¹⁴.

4.3.3.5. Проверки соблюдения правил обработки ПДн пользователями ИСПДн и работниками¹⁵.

5. Оформление результатов Контроля

5.1. Результаты планового Контроля оформляются Ответственными лицами в своей части в виде **Отчета о результатах осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства и внутренним нормативным документам по форме** **Ошибка! Источник ссылки не найден. к Методике** (далее – Отчет), после чего подписываются ими и запускаются на согласование в установленном в Компании порядке.

¹³ В частности, проверяется наличие подписей всех работников Компании, допущенных к обработке ПДн, об ознакомлении с локальными нормативными актами по вопросам обработки и обеспечения безопасности ПДн, а также порядок допуска вновь прибывших работников к обработке ПДн: ознакомление с локальными нормативными актами по вопросам обработки и обеспечения безопасности ПДн; проведение инструктажа; подпись обязательства о неразглашении конфиденциальной информации.

¹⁴ В частности, проверяются мероприятия, связанные с получением доступа к ИСПДн, например, присутствия работников Компании, участвующих в обработке ПДн, в перечнях помещений, используемых для хранения ПДн и в Матрице доступа к ИСПДн; реализации управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей; разделения полномочий и организации доступа к информационным объектам и обработке ПДн в ИСПДн в соответствии с Перечнями (помещений, АРМ, должностных лиц) и Матрицей доступа и в объеме, необходимом для выполнения функциональных обязанностей; выдачи под подпись ответственным за средства вычислительной техники электронных носителей по журналу учета МНИ; выдачи под подпись пользователям ИСПДн средств защиты от несанкционированного доступа по журналу учета средств защиты информации и т.п.

¹⁵ В частности, пользователями ИСПДн - парольной политики; правил работы со съемными носителями ПДн; правил антивирусной защиты и т.п., а работниками - порядка формирования материальных носителей ПДн; порядка неавтоматизированной обработки ПДн; порядка хранения материальных носителей ПДн и т.п.

5.2. По результатам внепланового Контроля может быть оформлен отчет по форме Приложения №2 к настоящей Методике или справка, заключение, докладная записка в свободной форме, содержащие обстоятельства проведения Контроля.

6. Мероприятия по результатам проведения Контроля

6.1. В случае выявления несоответствий Ответственными лицами формируется перечень таких несоответствий, а также сроки их устранения, и направляется в установленном порядке в адрес соответствующего структурного подразделения.

6.2. Структурное подразделение на основе поступившей информации формирует план устранения всех выявленных несоответствий (далее – План устранения несоответствий) и в соответствии с ним осуществляет работу по повышению уровня соответствия законодательству о ПДн путем устранения всех указанных в Отчете нарушений.

6.3. План устранения несоответствий направляется в адрес Ответственных лиц в установленном порядке.

6.4. В установленный на устранение нарушений срок Структурное подразделение направляет Отчет об устранении нарушений в адрес Уполномоченного лица и Ответственных лиц.

7. Заключительные положения

7.1. Пересмотр Методики должен проводиться периодически, не реже _____¹⁶, а также:

- при изменении требований законодательства РФ в области обработки ПДн и обеспечения безопасности ПДн;
- при изменениях в бизнес-процессах Компании;
- при изменении используемых технологий в Компании;
- при изменении организационной структуры;
- при изменении информационных и (или) телекоммуникационных систем (или введении новых);
- по фактам возникновения инцидентов, обнаружения уязвимостей информационной безопасности и иных значимых событий информационной безопасности, по решению Уполномоченного лица.

7.2. Все изменения в Методику вносятся и утверждаются в установленном в Компании порядке.

Приложения:

1. Форма Плана осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства и внутренним нормативным документам;

2. Форма Отчета о результатах осуществления внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства и внутренним нормативным документам.

¹⁶ Указывается периодичность.