

УТВЕРЖДЕНО:

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

МЕТОДИКА
по реагированию на Инциденты с персональными данными

Горно-Алтайск, 2025

1. Общие положения

1.1 Настоящая Методика по реагированию на Инциденты с персональными данными (далее – Методика) подготовлена в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ), приказа Роскомнадзора от 14.11.2022 №187¹ (далее – Приказ Роскомнадзора №187), а также Стандарта Банка России СТО БР БФБО-1.5-2023² (далее - СТО БР).

1.2 Методика регламентирует порядок выявления и установления (подтверждения) Инцидентов с ПДн, а также порядок информирования об Инциденте с ПДн Надзорных органов³⁴, Оператора, поручившего Компании обработку персональных данных (далее – ПДн), Субъектов ПДн в Автономной некоммерческой организации "Центр регионального развития, реализации социально значимых проектов и поддержки общественных инициатив "Территория добра" (далее – Компания).

2. Выявление и установление (подтверждение) Инцидента с ПДн

2.1 В отношении Инцидента с ПДн Законом №152-ФЗ выделяется два режима:

- **Выявление**⁵ Инцидента с ПДн может быть произведено как Компанией, так и Надзорным органом, Оператором или лицом, осуществляющим обработку по поручению Компании (далее – Обработчик ПДн), а также иным заинтересованным лицом (например, путем обнаружения ПДн в сети Интернет);

- **Установление**⁶ (подтверждение) факта Инцидента с ПДн может быть произведено исключительно Компанией на основе критериев, указанных в п. 3 настоящей Методики.

2.2 Инцидент с ПДн подразделяется на:

- выявленный (обнаруженный) Инцидент с ПДн, но не установленный (не подтвержденный);
- выявленный (обнаруженный) и установленный (подтвержденный) Инцидент с ПДн.

3. Критерии установления (подтверждения) Инцидента с ПДн

3.1 Критериями установления (подтверждения) Инцидента с ПДн, является **одновременное** выполнении следующих условий:

- в результате Инцидента с ПДн **нарушена конфиденциальность ПДн** (ПДн стали доступны неограниченному кругу лиц (например, в результате опубликования базы данных (далее – БД), содержащей ПДн, в сети Интернет);

- Инцидент с ПДн произошел в результате **неправомерных или случайных, в т.ч. несанкционированных Компанией**⁷, действий/бездействий третьих лиц, включая работников

¹ Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

² Стандарт Банка России СТО БР БФБО-1.5-2023 «Безопасность финансовых (банковских) операций Управление инцидентами, связанными с реализацией информационных угроз, и инцидентами операционной надежности О формах и сроках взаимодействия Банка России с кредитными организациями, некредитными финансовыми организациями и субъектами национальной платежной системы при выявлении инцидентов, связанных с реализацией информационных угроз, и инцидентов операционной надежности» (принят и введен в действие приказом Банка России от 8 февраля 2023 г. № ОД-215).

³ По смыслу настоящей Методики к Надзорным органам относятся Роскомнадзор и Банк России.

⁴ Информирование Банка России об Инциденте с ПДн осуществляется в случае, если Банк России осуществляет надзор за деятельностью Компании.

⁵ Под выявлением понимается обнаружение ПДн субъектов ПДн в открытом доступе, в т.ч. баз с ПДн в сети Интернет.

⁶ Под установлением (подтверждением) факта Инцидента с ПДн понимается установление одновременной совокупности обстоятельств, предусмотренных п.3.1. настоящей Методики

⁷ То есть не по воле и вне контроля Компании.

или бывших работников Компании, и/или **нарушения требований кибербезопасности**⁸;

- Инцидент с ПДн произошел **исключительно в отношении ПДн, которые Компания обрабатывает как Оператор или как Обработчик ПДн** по поручению другого лица на основании договора;

- Инцидент с ПДн влечет **нарушение прав Субъектов ПДн** – причинение вреда (ущерба) Субъектам ПДн. Для того, чтобы установить (подтвердить) или опровергнуть нарушение прав/причинение вреда - Субъектам ПДн, необходимо провести оценку вреда. Оценка вреда проводится в соответствии с требованиями приказа Роскомнадзора от 27.10.2022 №178⁹ (далее - Приказ Роскомнадзора №178) и с учетом критериев согласно Приложению №1 к настоящей Методике. Результаты оценки вреда с выводами о предполагаемых последствиях фиксируются в первичном уведомлении, направляемом в Роскомнадзор с учетом требований, предъявляемых к нему Приказом Роскомнадзора №187. В т.ч. сведения о вреде, нанесенном правам субъектов ПДн, указываются в дополнительном уведомлении о результатах внутреннего расследования.

3.2 Не признаются Инцидентом с ПДн случаи, которые не отвечают указанным ранее критериям Инцидента с ПДн, в частности (но не исключительно):

- несанкционированный доступ работников Компании/иных уполномоченных лиц, являющихся пользователями автоматизированной системы (далее – АС) Компании, к ПДн без воспроизведения БД (в т.ч. без копирования, скачивания, сохранения, иных способов изготовления и/или записи);

- изменение, удаление, уничтожение, блокирование ПДн в инфраструктуре Компании, вызванные любыми причинами (например, техническими сбоями и/или причинами природного/природно-техногенного характера), в отсутствие передачи (предоставления, распространения, доступа) ПДн.

4. Порядок действий в случае выявления Инцидента с ПДн и установления (подтверждения) Инцидента с ПДн

4.1 Лицо, ответственное за организацию обработки ПДн и лицо, ответственное за обеспечение информационной безопасности в Компании, являются ответственными за организацию процесса по реагированию на Инциденты с ПДн и информированию об Инцидентах с ПДн Надзорных органов в установленных Законом №152-ФЗ, приказом Роскомнадзора №187 и СТО БР случаях.

4.2 Организация информирования Оператора, поручившего Компании обработку ПДн, Субъектов ПДн, а также заинтересованных лиц осуществляется бизнес-подразделением Компании, ответственным за взаимодействие с указанными лицами.

4.3 Для целей реагирования на Инцидент с ПДн по решению лица, ответственного за

⁸ Таковыми случаями могут быть признаны, в частности:

- ② неправомерное (несанкционированное) воспроизведение (в т.ч. копирование, скачивание, сохранение, иные способы изготовления и/или записи) и/или распространение (в т.ч. противоправный оборот) БД (или ее части), содержащей ПДн;
- ② несанкционированное размещение БД (или ее части), содержащей ПДн, в информационной-телекоммуникационной сети «Интернет» (в том числе, в теневого интернете);
- ② хищение или утрата Материальных носителей, содержащих ПДн;
- ② намеренная или непреднамеренная (в отсутствие умысла) передача третьим лицам Материальных носителей, содержащих ПДн, неуполномоченным на их получение.

⁹ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

обеспечение информационной безопасности, формируется группа экспертов (далее – Команда реагирования), в состав которой в обязательном порядке входит лицо, ответственное за организацию обработки ПДн, или его уполномоченный представитель¹⁰. Состав Команды реагирования формируется из работников Компании по информационной безопасности, а также работников, обладающих соответствующими компетенциями для решения конкретного Инцидента с ПДн. Руководителем Команды реагирования является лицо, ответственное за обеспечение информационной безопасности в Компании.

Команда реагирования не имеет фиксированного состава. Для каждого Инцидента с ПДн собирается свой состав.

4.4 Источники поступления информации об Инциденте с ПДн:

Компания может самостоятельно выявить Инцидент с ПДн в ходе мониторинга кибербезопасности собственной инфраструктуры и системы защиты ПДн¹¹, а также получить информацию об Инциденте с ПДн от третьих лиц:

- Роскомнадзора;
- Банка России (если является надзорным органом);
- работника Компании;
- Оператора или Обработчика ПДн;
- иного заинтересованного лица¹².

4.4.1. При поступлении в Компанию документального запроса от Надзорных органов о выявленном (обнаруженном) Инциденте с ПДн подразделение, ответственное за прием корреспонденции в Компании, проводит регистрацию поступившего запроса и доводит информацию до руководства Компании, лица, ответственного за организацию обработку ПДн, и лица, ответственного за обеспечение информационной безопасности, согласно установленным правилам внутреннего документооборота.

4.4.2. При выявлении (обнаружении) Инцидента с ПДн/подозрении на Инцидент с ПДн работником Компании информация направляется лицу, ответственному за организацию обработки ПДн, и лицу, ответственному за обеспечение информационной безопасности, в порядке, установленном процессом по реагированию на Инциденты с ПДн.

4.4.3. При выявлении Инцидента с ПДн Оператором или Обработчиком ПДн в отношении ПДн, обработка которых осуществляется на основании заключенного с Компанией договора, информация об Инциденте с ПДн направляется Оператором или Обработчиком ПДн лицу, ответственному за сопровождение заключенного договора, в порядке, предусмотренном таким договором. Работник Компании, ответственный за сопровождение указанного договора, направляет полученную информацию, в порядке, установленном процессом по реагированию на Инциденты с ПДн.

4.4.4. При поступлении в Компанию обращения от заинтересованного лица о выявленном (обнаруженном) Инциденте с ПДн обработка обращений осуществляется в порядке, установленном

¹⁰ Лицо, ответственное за организацию обработки ПДн входит в состав Команды реагирования с целью определения отнесения данных, в отношении которых произошел Инцидент, к ПДн, определения правомерности обработки ПДн, оценки вреда, который может быть причинен субъектам ПДн и участия в установлении причин Инцидента с ПДн, формировании мер по исключению/минимизации вреда субъектам ПДн, а также выработке мер по предотвращению повторения Инцидентов с ПДн.

¹¹ В том числе, может быть организован мониторинг общедоступных источников: СМИ, мессенджеров и т.п. на наличие информации об утечках.

¹² Например, потенциальные контрагенты Компании, запросы от органов государственной власти, депутатский запрос и т.п.

в Компании для рассмотрения обращений¹³.

4.5 При выявлении (обнаружении) Инцидента с ПДн или получении информации о выявленном (обнаруженном) Инциденте с ПДн/подозрении на Инцидент с ПДн по решению лица, ответственного за обеспечение информационной безопасности, формируется Команда реагирования для осуществления действий по реагированию на Инцидент с ПДн, направленных на установление (подтверждение) Инцидента с ПДн, либо на его опровержение на основе критериев согласно разделу 3 настоящей Методики. Указанные действия осуществляются в кратчайшие сроки, но не позднее 24 часов¹⁴ с момента выявления (обнаружения) Инцидента с ПДн¹⁵.

4.6 При выявлении (обнаружении) Инцидента с ПДн или получении информации о выявленном (обнаруженном) Инциденте с ПДн/подозрении на Инцидент с ПДн проводится реагирование на Инцидент с ПДн.

В ходе реагирования на Инцидент с ПДн Команда реагирования:

- осуществляется сбор и анализ информации, связанной с Инцидентом с ПДн;
- коррелируется и сопоставляется информация, полученная в ходе этапа сбора и анализа информации;
- подтверждается или опровергается факт возникновения Инцидента с ПДн;
- выдвигаются гипотезы о возможных причинах Инцидента с ПДн;
- проверяются гипотезы путем непосредственного обнаружения причин, прямого логического доказывания (подтверждения новыми фактами) или косвенного логического доказывания (опровержение и исключение всех ложных гипотез);
- проводится расследование Инцидента с ПДн;
- оценивается вред, нанесенный правам субъектов ПДн вследствие Инцидента с ПДн в соответствии с требованиями Приказа Роскомнадзора №178 и с учетом критериев согласно Приложению №1 к настоящей Методике;
- формируется перечень мер по устранению последствий Инцидента с ПДн, а также по устранению несоответствий в процессах Компании (если применимо).

4.7 Лицо, ответственное за организацию обработки ПДн, на основании информации, полученной в ходе расследования Инцидента с ПДн, организывает¹⁶ и/или осуществляет информирование о факте установления (подтверждения) Инцидента с ПДн¹⁷ Роскомнадзора, Банка России в случае, когда Компания является Оператором в порядке, установленном настоящей Методикой.

4.8 Информирование о факте установления (подтверждения) Инцидента с ПДн Оператора в соответствии с положениями Закона № 152-ФЗ¹⁸ в случае обработки Компанией ПДн по поручению Оператора, осуществляется подразделением Компании, которое является

¹³ Обработка обращения осуществляется в зависимости от лица, обратившегося с таким запросом. При этом информация, указанная в обращении в обязательном порядке должна быть доведена до сведения Ответственных лиц.

¹⁴ Не позднее в течение 3 часов с момента выявления Инцидента с ПДн при информировании Банка России.

¹⁵ В случае, если не удастся установить (подтвердить) факт Инцидента с ПДн, то в таком случае необходимо направить первичное уведомление в течении 24 часов с информацией о выявленном, но не установленном факте Инцидента с ПДн, а уже при направлении дополнительного уведомления, направляемого в течении 72 часов, предоставить недостающую информацию или направить совместно с таким уведомлением акт о проведении внутреннего расследования, подтверждающего отсутствие факта Инцидента с ПДн с учетом положений п.5.5. настоящей Методики.

¹⁶ По решению руководителя Компании или лица, ответственного за организацию обработки ПДн, могут быть назначены ответственные работники для осуществления информирования о факте установления (подтверждения) Инцидента с ПДн Роскомнадзора, Банка России, в случае, когда Компания является Оператором.

¹⁷ Решение об информировании принимается в порядке, установленном Компанией.

¹⁸ В случае, если поручением на обработку ПДн предусмотрены более сжатые сроки, то информирование осуществляется в сроки, предусмотренные поручением на обработку.

ответственным за сопровождение заключенного договора, содержащим поручение на обработку ПДн, в порядке, установленном настоящей Методикой. Информация для уведомления Оператора формируется лицом, ответственным за организацию обработки ПДн.

4.9 Информирование Субъектов ПДн, в отношении ПДн которых произошел Инцидент с ПДн в целях минимизации возможного вреда Субъектам ПДн, осуществляет бизнес-подразделение Компании, ответственное за взаимодействие с Субъектами ПДн.

5. Порядок информирования об Инциденте с ПДн Роскомнадзора

5.1. Информирование Роскомнадзора осуществляется во исполнение требований ч. 3.1 ст. 21 Закона № 152-ФЗ и с учетом п. 4.6. настоящей Методики:

- информирование об установленном (подтвержденном) Инциденте с ПДн путем направления первичного уведомления в течение 24 часов с момента выявления (обнаружения) Инцидента с ПДн Компанией или с момента получения информации об Инциденте с ПДн от Надзорных органов, Обработчика ПДн, иных заинтересованных лиц по форме Уведомления о факте неправомерной или случайной передачи (предоставлении, распространении, доступе) ПДн, повлекшей нарушение прав Субъектов ПДн, с учетом положений Приказа Роскомнадзора №187;
- информирование о результатах внутреннего расследования путем направления дополнительного уведомления осуществляется в течение 72 часов с момента выявления (обнаружения) Инцидента с ПДн Компанией или с момента получения информации об Инциденте с ПДн от Обработчика ПДн, иных заинтересованных лиц с учетом положений Приказа Роскомнадзора №187.

5.2. Уведомления об Инциденте с ПДн направляются в адрес Роскомнадзора в виде документа на бумажном носителе или в форме электронного документа. Уведомления об Инциденте с ПДн могут быть направлены электронным документом посредством заполнения специализированной формы на официальном сайте Роскомнадзора¹⁹ после авторизации с учетной записью Компании посредством ЕСИА.

5.3. В случае получения от Роскомнадзора в соответствии с Приказом Роскомнадзора №187 запроса о представлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений, недостающие сведения и (или) пояснения относительно некорректности предоставляются в течение 3 рабочих дней со дня получения запроса, способом, указанным в запросе.

5.4. В случае получения от Роскомнадзора в соответствии с Приказом Роскомнадзора №187 требования о необходимости предоставить сведения о результатах внутреннего расследования по факту выявленного Роскомнадзором Инцидента с ПДн, в Роскомнадзор направляется в течение 1 рабочего дня со дня получения запроса соответствующее уведомление с учетом положений п. 5.2. настоящей Методики.

5.5. В случае неподтверждения Инцидента с ПДн результаты проведенного Компанией внутреннего расследования оформляются актом, подтверждающим отсутствие Инцидента с ПДн в деятельности Компании. Акт внутреннего расследования²⁰ оформляется в качестве приложения к Уведомлению о результатах внутреннего расследования.

¹⁹ <https://pd.rkn.gov.ru/incidents/form/>.

²⁰ В соответствии с абз. 2 п. 16 Приказа Роскомнадзора №187 данный Акт прикладывается к дополнительному уведомлению в случае неподтверждения факта Инцидента с ПДн и/или неустановления принадлежности скомпрометированной базы данных, содержащей ПДн, соответствующему оператору в деятельности такого оператора. Форма Акта Приказом Роскомнадзора №187 не установлена.

5.6. В случае установления Компанией, Роскомнадзором или иным заинтересованным лицом Инцидента с ПДн, характеристики которого полностью соответствуют Инциденту с ПДн, по которому ранее уже были направлены уведомления в порядке согласно п.5.1. настоящей Методики, в Роскомнадзор направляется повторное уведомление с указанием дат и номеров ранее направленных уведомлений.

6. Порядок информирования об Инциденте с ПДн Банка России²¹

6.1. Информирование Банка России осуществляется во исполнение требований СТО БР посредством ФинЦЕРТ в порядке, установленном СТО БР по формам, утвержденным СТО БР и с учетом п. 4.6. настоящей Методики.

6.2. В случае выявления (обнаружения) Инцидента с ПДн Компанией информирование Банка России осуществляется:

- О выявленном (обнаруженном) Инциденте с ПДн в течение 3 часов²² или 24 часов с момента выявления (обнаружения) Инцидента с ПДн Компанией по форме СТО БР (Форма представления участниками информационного обмена данных о выявлении незаконного раскрытия банковской тайны и/или защищаемой информации в соответствии с нормативными актами Банка России).
- О результатах внутреннего расследования в течение 30 дней с момента выявления (обнаружения) Инцидента с ПДн Компанией по форме СТО БР (Форма представления участниками информационного обмена данных о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны и/или защищаемой информации в соответствии с нормативными актами Банка России).

6.3. В случае получения от Банка России запроса в соответствии со СТО БР о подтверждении факта незаконного раскрытия банковской тайны и/или защищаемой информации информирование Банка России осуществляется в случае установления (подтверждения) Инцидента с ПДн в течение 24 часов и о результатах внутреннего расследования в порядке согласно разделу 6 настоящей Методики.

6.4. В случае неподтверждения по результатам проведенного внутреннего расследования Инцидента с ПДн в деятельности Компании информация об отсутствии Инцидента с ПДн направляется в Банк России в течение 24 часов по форме СТО БР (Форма представления ответа на запрос Банка России в целях подтверждения факта незаконного раскрытия банковской тайны и/или защищаемой информации в соответствии с нормативными актами Банка России).

7. Информирование об Инциденте с ПДн Оператора²³

Информирование Оператора в соответствии с ч. 3 ст. 6 Закона №152-ФЗ в случае установления (подтверждения) Инцидента с ПДн осуществляется в порядке, предусмотренном условиями договора, содержащего поручение на обработку ПДн, заключенного между Оператором

²¹ Данный раздел применим для Компаний, за деятельностью которых осуществляет надзор Банк России.

²² В течение 3 часов с момента выявления инцидента защиты информации для участников информационного взаимодействия, реализующих усиленный или стандартный уровни защиты информации в соответствии с ГОСТ Р 57580.1-2017.

²³ Компания может выступать как в роли Оператора, так и в роли Обработчика ПДн, обрабатывающего ПДн по поручению другого Оператора.

и Обработчиком ПДн²⁴.

8. Информирование об Инциденте с ПДн заинтересованного лица²⁵

8.1. Информирование заинтересованного лица, от которого поступило обращение с информацией о выявленном (обнаруженном) Инциденте с ПДн, о факте подтверждения или неподтверждения Инцидента с ПДн, осуществляется в порядке, установленном в Компании. Информирование заинтересованного лица осуществляет подразделение ответственное за обработку обращений и запросов, в установленном в Компании порядке.

8.2. Ответ на обращение заинтересованного лица должен содержать информацию:

- в случае, если Инцидент с ПДн установлен (подтвержден) – общую информацию о факте Инцидента с ПДн, а также о принятых мерах по локализации/минимизации вреда Субъектам ПДн (если применимо);
- в случае, если Инцидент с ПДн не установлен (не подтвержден) – разъяснения, содержащие обоснование причин, которыми обусловлен такой вывод (например, информацию о том, что в отношении раскрытых ПДн Компания не является Оператором).

8.3. Ответ на обращение заинтересованного лица не должен содержать ПДн, сведения, которые содержат конфиденциальную информацию, в отношении которых произошел Инцидент с ПДн.

9. Информирование Субъектов ПДн об Инциденте с ПДн

9.1. Информирование Субъектов ПДн об установленном (подтвержденном) Инциденте с ПДн²⁶ осуществляется с учетом п. 4.9. настоящей Методики в случае, если Компания является Оператором, при условии, что Субъекту ПДн может быть причинен существенный²⁷ вред (в т.ч. материальный или нематериальный ущерб, вред жизни, здоровью), определенный в соответствии с требованиями Приказа Роскомнадзора №178 и с учетом критериев согласно Приложению №1 к настоящей Методике.

9.2. Информационное сообщение в адрес Субъектов ПДн может содержать:

- описание состава ПДн, в отношении которых произошел Инцидент с ПДн, и возможных последствий Инцидента с ПДн для Субъекта ПДн;
- информацию о принятых или планируемых Компанией мерах, направленных на устранение последствий Инцидента с ПДн, в т.ч. мерах по смягчению возможного отрицательного воздействия установленного (подтвержденного) Инцидента с ПДн;
- перечень действий, которые рекомендуется предпринять Субъектам ПДн для минимизации возможного вреда;
- сведения о канале коммуникации, по которому можно получить более подробную информацию об Инциденте с ПДн.

9.3. Информирование Субъектов ПДн осуществляется с использованием контактных данных Субъектов ПДн, предоставленных ими или их представителями в рамках взаимодействия с

²⁴ В договор, содержащий поручение на обработку ПДн, должны быть включены условия предоставления в случае Инцидента с ПДн информации об инциденте (при первичном уведомлении и о результатах внутреннего расследования или акта о проведенном внутреннем расследовании, подтверждающего отсутствие Инцидента с ПДн) а также канал и сроки информирования, не превышающие сроки, установленные Законом №152-ФЗ.

²⁵ Не признается заинтересованным лицом тот, кого не представляется возможным установить (идентифицировать).

²⁶ Имеется в виду Инцидент с ПДн, затронувший права соответствующего Субъекта ПДн.

²⁷ Существенность вреда определяется путем соотношения степени вреда в установленном в Компании порядке, и зависит от того, представляется ли возможной локализация последствий Инцидента с ПДн и/или были ли локализованы последствия.

Компанией (например, при получении услуг и сервисов Компании).

9.4. Если информирование Субъектов ПДн требует несоразмерного усилия²⁸, делается сообщение для информирования общественности или принимается аналогичная мера, посредством которой информируются Субъекты ПДн, в отношении которых произошел Инцидент с ПДн.

9.5. Информирование Субъектов ПДн не требуется, если соблюдается любое из следующих условий:

- Компания реализовала соответствующие технические и организационные меры защиты в отношении ПДн, затронутых Инцидентом с ПДн, в особенности те меры, посредством которых ПДн будут недоступны третьим лицам;
- Компанией приняты меры, в результате которых не может быть причинен существенный вред Субъекту ПДн (в т.ч. материальный ущерб, вред жизни, здоровью).

10. Заключительные положения

Настоящая Методика подлежит пересмотру в случае изменения требований, содержащихся в Законе №152-ФЗ и в нормативных правовых актах, принятых в соответствии с ним.

Приложение: Возможные критерии для оценки вреда субъектам персональных данных в случае инцидента с персональными данными.

²⁸ Например, несоразмерность в части затрат на информирование по отношению к возможному вреду Субъектам ПДн.