



**АДМИНИСТРАЦИЯ
ГОРОДСКОГО ОКРУГА СТРЕЖЕВОЙ
РАСПОРЯЖЕНИЕ**

15.02.2024

№ 81

Об утверждении порядка внешнего информационного взаимодействия
Администрации городского округа Стрежевой по инцидентам в области
персональных данных

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ
«О персональных данных»

Утвердить Порядок внешнего информационного взаимодействия
Администрации городского округа Стрежевой по инцидентам в области
персональных данных согласно приложению к настоящему распоряжению.

Мэр городского округа

В.В. Дениченко

Порядок внешнего информационного взаимодействия Администрации городского округа Стрежевой по инцидентам в области персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок внешнего информационного взаимодействия Администрации городского округа Стрежевой по инцидентам в области персональных данных (далее — Порядок) разработан с учетом:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 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»;
- приказа Федеральной службы безопасности Российской Федерации от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

1.2. Целью разработки данного Порядка является установление порядка, условий и правил внешнего информационного взаимодействия Администрации городского округа Стрежевой (далее — учреждение) по инцидентам в области персональных данных (далее — ПДн) с:

- уполномоченным органом по защите прав субъектов ПДн (Роскомнадзор);
- государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

1.3. Настоящий Порядок предназначен для сотрудника учреждения, назначенного ответственным за организацию обработки ПДн в учреждении (далее – Ответственный).

1.4. Настоящий Порядок подлежит анализу и пересмотру (при необходимости) в следующих случаях:

- периодически – не реже чем один раз в год;
- изменения нормативных правовых актов, указанных в пункте 1.1 настоящего Порядка – не позднее десяти рабочих дней с момента вступления в силу соответствующих изменений.

1.5. Сокращения, используемые в рамках настоящего Порядка:

1.5.1. Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

1.5.2. Портал персональных данных – портал персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и

массовых коммуникаций в информационно-телекоммуникационной сети «Интернет» (<https://pd.rkn.gov.ru/>).

1.5.3. ЕСИА – федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

1.5.4. Скомпрометированная база данных – база данных, содержание которой стало доступно неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн.

1.5.5. Инцидент в области персональных данных (инцидент) – установленный факт неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей за собой нарушение прав субъектов ПДн.

1.5.6. Компьютерный инцидент – факт нарушения и (или) прекращения функционирования информационного ресурса, сети электросвязи, используемой для организации взаимодействия информационных ресурсов, и (или) нарушения безопасности обрабатываемой в информационном ресурсе информации, в том числе произошедший в результате компьютерной атаки.

1.5.7. ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

1.5.8. НКЦКИ – национальный координационный центр по компьютерным инцидентам.

2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ СВЕДЕНИЙ В РОСКОМНАДЗОР

2.1. Предоставление сведений учреждением в Роскомнадзор об инцидентах в области ПДн осуществляется в форме направления соответствующих уведомлений. Ответственным должно быть предоставлено в Роскомнадзор:

2.1.1. В течение двадцати четырёх часов (24 часа) с момента выявления инцидента – уведомление с информацией о произошедшем инциденте (далее – Первичное уведомление).

2.1.2. В течение семидесяти двух часов (72 часа) с момента выявления инцидента – уведомление с информацией о результатах внутреннего расследования выявленного инцидента (далее – Дополнительное уведомление).

2.2. Уведомления направляются в виде документа на бумажном носителе или в форме электронного документа. Решение о способе направления уведомлений принимается Ответственным по каждому инциденту индивидуально.

2.3. При принятии решения о направлении уведомления в виде документа на бумажном носителе такое уведомление оформляется и направляется по адресу Роскомнадзора:

– по Первичному уведомлению – по форме, представленной в ПРИЛОЖЕНИИ 1 к настоящему Порядку;

– по Дополнительному уведомлению – по форме, представленной в ПРИЛОЖЕНИИ 2 к настоящему Порядку.

2.4. При принятии решения о направлении уведомления в форме электронного документа такое уведомление формируется Ответственным посредством заполнения

специализированной формы, размещенной на Портале персональных данных, после прохождения процедуры идентификации и аутентификации посредством ЕСИА и подписывается электронной подписью Мэра городского округа учреждения в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2.5. Все факты направления уведомлений в Роскомнадзор должны быть зафиксированы в Журнале внешнего информационного взаимодействия Администрации городского округа Стрежевой по инцидентам в области персональных данных. Форма журнала представлена в ПРИЛОЖЕНИИ 3 к настоящему Порядку.

2.6. Первичное уведомление должно содержать:

2.6.1. Сведения о произошедшем инциденте:

- дата и время выявления инцидента;
- характеристика (характеристики) ПДн (содержание скомпрометированной базы данных, количество содержащихся в ней записей, информация об актуальности скомпрометированной базы данных, период, в течение которого собраны ПДн).

2.6.2. Сведения о предполагаемых причинах, повлекших нарушение прав субъектов ПДн (предварительные причины неправомерного распространения ПДн, повлекшего нарушение прав субъектов ПДн);

2.6.3. Сведения о предполагаемом вреде, нанесенном правам субъектов ПДн (результаты предварительной оценки вреда, который может быть нанесен субъектам ПДн, в связи с неправомерным распространением ПДн, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»). Степень возможного вреда, который мог быть причинен субъектам ПДн в результате инцидента, определяется на основании Акта оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона «О персональных данных», утвержденного Мэром городского округа учреждения.

2.6.4. Сведения о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых учреждением организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.6.5. Сведения об Ответственном (лице, уполномоченном учреждением на взаимодействие с Роскомнадзором по вопросам, связанным с выявленным инцидентом).

2.6.6. Данные учреждения:

- полное и сокращенное (при наличии) наименование;
- идентификационный номер налогоплательщика;
- юридический адрес;
- адрес электронной почты Ответственного для получения информации о зарегистрированном уведомлении, номера и ключа уведомления.

2.6.7. Иные сведения и материалы, находящиеся в распоряжении учреждения, в том числе об источнике получения информации об инциденте, а также подтверждающие принятие мер по устранению последствий инцидента (при наличии).

2.7. Дополнительное уведомление должно содержать:

2.7.1. Сведения о Первичном уведомлении (номер и ключ).

2.7.2. Сведения о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов ПДн, и вреде, нанесенном правам субъектов ПДн, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении учреждения о проведении внутреннего расследования с указанием его реквизитов).

2.7.3. Сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии):

– фамилия, имя, отчество (при наличии) должностного лица учреждения с указанием должности или фамилия, имя, отчество (при наличии) индивидуального предпринимателя или полное наименование юридического лица, чьи действия стали причиной выявленного инцидента;

– IP-адрес компьютера или устройства и его местонахождение (предполагаемое местонахождение, если причиной инцидента стали действия посторонних лиц);

– иные сведения о выявленном инциденте, имеющиеся в распоряжении учреждения.

3. ПОРЯДОК РАССМОТРЕНИЯ ЗАПРОСОВ ОТ РОСКОМНАДЗОРА

3.1. Настоящий Порядок регламентирует действия Ответственного при получении следующих запросов от Роскомнадзора:

3.1.1. Запрос на предоставление недостающих сведений и (или) пояснений относительно некорректности в направленных ранее учреждением уведомлениях по инцидентам сведений (далее — Требование о пояснении).

3.1.2. Запрос с требованием о необходимости предоставления сведений о результатах внутреннего расследования выявленного инцидента (далее — Требование о предоставлении сведений), если такие сведения не были предоставлены учреждением согласно пункту 2.1.2 настоящего Порядка.

3.1.3. Запрос с требованием о предоставлении сведений по инциденту, сведения о котором не были предоставлены учреждением (далее — Требование о предоставлении уведомления).

3.2. Требование о пояснении направляются Роскомнадзором на адрес электронный почты, указанный в Первичном уведомлении. При получении учреждением Требования о пояснении Ответственный должен в течение трех рабочих дней со дня получения такого требования сформировать ответ и направить в Роскомнадзор одним из способов, указанных в пункте 2.2 настоящего Порядка.

3.3. Требование о предоставлении сведений направляется Роскомнадзором в случае нарушения сроков предоставления Дополнительного уведомления. При получении учреждением Требования о предоставлении сведений Ответственный должен в течение одного рабочего дня со дня получения такого требования сформировать ответ и направить в Роскомнадзор одним из способов, указанных в пункте 2.2 настоящего Порядка.

3.4. Требование о предоставлении уведомления направляется Роскомнадзором в случае выявления им факта неправомерного распространения скомпрометированной базы данных, содержание которой указывает на ее

принадлежность учреждению. При получении учреждением Требования о предоставлении уведомления Ответственный должен:

3.4.1. В течение 24 часов с момента получения требования направить Первичное уведомление одним из способов, указанных в пункте 2.2 настоящего Порядка.

3.4.2. В течение 72 часов провести внутреннее расследование по Требованию о предоставлении уведомления и оформить результаты расследования в виде акта, подтверждающего факт инцидента или подтверждающего отсутствие факта инцидента. Форма акта о проведении внутреннего расследования представлена в приложении 4 к настоящему Порядку.

3.4.3. В течение 72 часов с момента получения Требования о предоставлении уведомления направить Дополнительное уведомление одним из способов, представленных в пункте 2.2 настоящего Порядка. К Дополнительному уведомлению должна быть приложена сканированная копия акта о проведении внутреннего расследования, подписанная Мэром городского округа учреждения.

3.5. Все факты направления уведомлений в ответ на запросы Роскомнадзора должны быть зафиксированы в Журнале внешнего информационного взаимодействия Администрации городского округа Стрежевой по инцидентам в области персональных данных.

4. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ СВЕДЕНИЙ В ГОССОПКА

4.1. Взаимодействие учреждения с ГосСОПКА, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн, осуществляется через НКЦКИ.

4.2. учреждение направляет информацию о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, путем подачи уведомлений согласно разделу 2 настоящего Порядка. Дальнейшая передача информации о компьютерных инцидентах в НКЦКИ на ответственности Роскомнадзора в соответствии с частью 11 статьи 23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.3. Подтверждением передачи учреждением в НКЦКИ информации о компьютерных инцидентах является присвоение НКЦКИ компьютерным инцидентам идентификаторов. Идентификаторы направляются НКЦКИ учреждению в течение 24 часов с момента их присвоения по тем же каналам, по которым сведения о компьютерном инциденте были направлены.

5. РАССМОТРЕНИЕ ЗАПРОСОВ ОТ НКЦКИ

5.1. При получении от НКЦКИ запроса о проверке сведений о компьютерном инциденте, повлекшем неправомерную передачу (предоставление, распространение, доступ) ПДн, Ответственный должен в течение 24 часов с момента получения запроса подготовить ответ на запрос и направить его в НКЦКИ по тем же каналам, по которым запрос был получен (информировать НКЦКИ о результатах проверки).

6. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений, предусмотренных настоящим Порядком.

Приложение 1
к порядку внешнего информационного
взаимодействия Администрации городского
округа Стрежевой по инцидентам в области
персональных данных

**Форма первичного уведомления об инциденте
(на бумажном носителе)**

Сведения об операторе	
Наименование оператора	
ИНН	
Адрес оператора	
Адрес электронной почты для отправки информации об уведомлении	
Сведения об инциденте	
Дата и время выявления инцидента	
Предполагаемые причины, повлекшие нарушение прав субъектов ПДн	
Характеристики ПДн	
Предполагаемый вред, нанесенный правам субъектов ПДн	
Принятые меры по устранению последствий инцидента	
Дополнительные сведения	
Контактные данные	
ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту	
Контактные данные лица, уполномоченного на взаимодействие	
Результаты внутреннего расследования*	
Результаты внутреннего расследования инцидента	
Сведения о лицах, действия которых стали причиной инцидента	

* указывается в случае, если на момент формирования Первичного уведомления имеются сведения о результатах внутреннего расследования по выявленному инциденту



Приложение 2
к порядку внешнего информационного
взаимодействия Администрации городского
округа Стрежевой по инцидентам в области
персональных данных

**Форма дополнительного уведомления об инциденте
(на бумажном носителе)**

Сведения об операторе	
Наименование оператора	
ИНН	
Адрес оператора	
Адрес электронной почты для отправки информации об уведомлении	
Сведения о первичном уведомлении	
Номер уведомления	
Ключ	
Контактные данные	
ФИО лица, уполномоченного оператором на взаимодействие с Роскомнадзором по инциденту	
Контактные данные лица, уполномоченного на взаимодействие	
Результаты внутреннего расследования	
Результаты внутреннего расследования инцидента	
Сведения о лицах, действия которых стали причиной инцидента	



Приложение 3
к порядку внешнего информационного
взаимодействия Администрации
городского округа Стрежевой по
инцидентам в области персональных
данных

Форма журнала внешнего информационного взаимодействия Администрации городского округа Стрежевой с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций по инцидентам в области персональных данных

№ п/п	Описание инцидента	Дата и время направления уведомления	Способ передачи сведений	Реквизиты запроса, в ответ на который направлено уведомление	Исполнитель	Примечание



Приложение 4
к порядку внешнего информационного
взаимодействия Администрации городского
округа Стрежевой по инцидентам в области
персональных данных

**Акт о проведении внутреннего расследования по инциденту в области персональных
данных, сведения о которых получены от Роскомнадзора**

1. Лица, ответственные за проведение внутреннего расследования:

2. Реквизиты запроса Федеральной службы по надзору в сфере связи,
информационных технологий и массовых коммуникаций с требованием о предоставлении
сведений по инциденту, сведения о котором не были представлены:

3. Период проведения внутреннего расследования:

4. Результат внутреннего расследования:

Лица, ответственные за проведение внутреннего расследования:

_____ (дата)

_____ (подпись)

_____ (расшифровка подписи)

