УТВЕРЖДАЮ:
Директор ГБОУ гимназии г.Сызрани
_____/Ж.И. Назаренко/
«___»_____2023г.

приказ ГБОУ гимназии г.Сызрани
от 01.03.2023г. № 121-од

РЕГЛАМЕНТ
ПО ПРОВЕДЕНИЮ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ И РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ, СВЯЗАННЫЕ С НЕПРАВОМЕРНОЙ ИЛИ СЛУЧАЙНОЙ ПЕРЕДАЧЕЙ (ПРЕДОСТАВЛЕНИЕМ, РАСПРОСТРАНЕНИЕМ, ДОСТУПОМ) ПЕРСОНАЛЬНЫХ ДАННЫХ

1. СОКРАЩЕНИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Оператор – государственный орган, 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.

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.

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет единый и обязательный порядок реагированию на инциденты, связанные с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных, повлекшей нарушение прав субъектов персональных данных, а также порядок проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в ГБОУ гимназии г.Сызрани (далее – Оператор, Организация).

3. ОПРЕДЕЛЕНИЕ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИСПДН

К инцидентам, связанным с неправомерной или случайной передачей (предоставлением, распространением, доступом) персональных данных (далее – инциденты информационной безопасности, инциденты ИБ) относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;
- отказ оборудования, сервисов, средств обработки и (или) защиты ПДн;
- несоблюдение требований внутренней организационно-распорядительной документации и действующего законодательства Российской Федерации в области защиты и обработки персональных данных;
- заражение вредоносными программами информационных систем персональных данных,

в случае если эти события привели к неправомерной или случайной передачи (предоставлению, распространению, доступу) персональных данных, повлекшей нарушение прав субъектов персональных данных.

К инцидентам информационной безопасности в ИСПДн также относятся попытки и факты получения несанкционированного доступа к информационным системам персональных данных:

- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн с нарушением установленного времени доступа;
- сеансы работы Пользователей ИСПДн, срок действия полномочий которых истек либо в состав полномочий которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
- совершение попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты ПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для наступления случаев, описанных выше.

4. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 ОПОВЕЩЕНИЕ ОБ ИНЦИДЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Последовательность действий работника Оператора в случае выявления инцидента ИБ:

– прекратить работу с ресурсом, в котором выявлен инцидент ИБ;

– оповестить непосредственного руководителя о факте выявления инцидента ИБ;

– непосредственный руководитель работника должен оповестить зам.директора по УВР (по безопасности персональных данных) о факте выявления инцидента;

– после извещения ответственных сотрудников по их решению представить всю необходимую информацию.

Зам.директора по УВР проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его наступлению, и составляет краткую справку, в которой описываются произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ.

4.2 МЕРОПРИЯТИЯ ПРИ НАСТУПЛЕНИИ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СТАВШЕГО ПРИЧИНОЙ НЕГАТИВНЫХ ПОСЛЕДСТВИЙ ДЛЯ СУБЪЕКТА ПДН

В случае если инцидент ИБ может стать (или уже стал) причиной негативных последствий для субъектов ПДн, персональные данные этих субъектов необходимо немедленно блокировать до устранения причин, повлекших наступление инцидента ИБ и его последствий. Решение о блокировании персональных данных принимает зам.директора по УВР. Для этой цели зам.директора по УВР блокирует персональные данные.

Менеджер обработки ПДн уведомляет субъекта о блокировании его персональных данных.

Персональные данные остаются заблокированными до устранения причин, повлекших наступление инцидента ИБ.

Если причины возникновения инцидента ИБ невозможно устранить, то персональные данные должны быть уничтожены. Менеджер обработки ПДн и Администратор безопасности персональных данных обеспечивают немедленное уничтожение персональных данных.

Менеджер обработки ПДн оповещает субъекта ПДн о прекращении и уничтожении его персональных данных.

4.3 УСТРАНЕНИЕ ПОСЛЕДСТВИЙ И ПРИЧИН ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на Администратора безопасности персональных данных. Не позднее 24 часов с момента наступления инцидента Администратор безопасности составляет План устранения последствий и причин наступления инцидента информационной безопасности. В данный план целесообразно включить:

– общую информацию о произошедшем инциденте;

– анализ ситуации, оперативные контрмеры, которые можно применить для локализации инцидента;

– определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента;

– определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента.

4.4 ПРОВЕДЕНИЕ РАССЛЕДОВАНИЯ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Разбирательство и составление заключений в обязательном порядке должны проводиться

в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности персональных данных;

– выявление факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;

– халатность и несоблюдение требований по обеспечению безопасности персональных данных;

– несоблюдение условий хранения носителей персональных данных;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/ целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

Внутреннее расследование проводится в соответствии с Регламентом проведения внутреннего расследования в связи с произошедшим инцидентом в области персональных данных.

Результаты внутреннего расследования оформляются в виде заключения.

Заключение с резолюцией руководителя, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле.

Дело о внутренних расследованиях вносится в номенклатуру дел Оператора.

4.5 ПРЕВЕНТИВНЫЕ МЕРЫ ПО НЕДОПУЩЕНИЮ ПОВТОРНОГО ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение в зависимости от произошедшего инцидента ИБ включают в себя:

– мониторинг событий в информационной системе персональных данных;

– восстановление операционной системы рабочей станции, на которой произошел инцидент ИБ, на заводские настройки;

– своевременное удаление неиспользуемых учетных записей;

– контроль и мониторинг действий пользователей в информационной системе персональных данных;

– контроль над действиями системных администраторов;

– проведение обучения (повторного обучения) пользователей правилам обработки и защиты персональных данных;

– ознакомление пользователей с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм и правил обработки персональных данных, а также за разглашение полученных данных;

– пересмотр организационно-распорядительной документации, устанавливающей правила обработки и обеспечения безопасности при работе с персональными данными.

5. ОЦЕНКА ЭФФЕКТИВНОСТИ РЕАЛИЗОВАННЫХ МЕР В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится комиссией по проведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных.

Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных Оператора организуется и проводится администратором безопасности информационных систем персональных данных.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер и контроль за выполнением требований защиты персональных данных в информационных системах

персональных данных проводится администратором безопасности информационных систем персональных и менеджером обработки персональных данных не реже 1 раза в 12 месяцев. Итоги проведенных мероприятий по проверке состояния защиты персональных данных вносятся в План внутренних проверок состояния защиты персональных данных (Приложение 1).

6. УВЕДОМЛЕНИЕ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБ ИНЦИДЕНТЕ

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Оператор обязан с момента выявления такого инцидента Оператором, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом (первичное уведомление);

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии) (дополнительное уведомление).

Взаимодействие Оператора с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций в рамках ведения реестра учета инцидентов в области персональных данных осуществляется в рамках приказа 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».

Первичное уведомление должно содержать:

1) Сведения:

- о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – скомпрометированная база данных), количество содержащихся в ней записей. Дополнительно оператор может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);

- о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);

- о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда, проведенной в соответствии с пунктом 5 части 1 статьи 18.1 Федерального закона «О персональных данных»);

- о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых оператором организационных и технических мер по устранению последствий инцидента в соответствии со статьями 18.1, 19 Федерального закона «О персональных данных»);

- о лице, уполномоченном оператором на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

2) Данные оператора, направившего уведомление:

- фамилию, имя и отчество (при наличии) гражданина, индивидуального предпринимателя;

- полное и сокращенное (при наличии) наименование юридического лица;

- идентификационный номер налогоплательщика юридического лица, индивидуального предпринимателя, физического лица;

- адрес регистрации по месту жительства (пребывания) физического лица, индивидуального предпринимателя;

- адрес юридического лица в пределах места нахождения юридического лица;

- адрес электронной почты (при наличии).

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

Дополнительное уведомление должно содержать сведения:

- о результатах внутреннего расследования выявленного инцидента (информация о причинах, повлекших нарушение прав субъектов персональных данных, и вреде, нанесенном правам субъектов персональных данных, о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии), а также о решении оператора о проведении внутреннего расследования с указанием его реквизитов);

- о лицах, действия которых стали причиной выявленного инцидента (при наличии) (фамилия, имя, отчество (при наличии) должностного лица оператора с указанием должности (если причиной инцидента стали действия сотрудника оператора), фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента, IP-адрес компьютера или устройства, предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц) и иные сведения о выявленном инциденте, имеющиеся в распоряжении оператора).

В случае если оператор на момент направления первичного уведомления располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Уведомление в форме электронного документа направляется оператором посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети "Интернет" (далее – Портал персональных данных), после прохождения процедуры идентификации и аутентификации посредством федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (далее – ЕСИА) и подписывается электронной подписью.

Оператору с момента поступления уведомления в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления.

При направлении дополнительного уведомления посредством Портала персональных данных оператор должен указать номер и ключ уведомления.

В случае направления оператором неполных или некорректных сведений Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций по адресу электронной почты, указанному в первичном уведомлении, не позднее трех рабочих дней со дня получения первичного или дополнительного уведомления направляет запрос оператору о представлении недостающих сведений и (или) пояснений относительно некорректности представленных в уведомлении сведений.

Недостающие сведения и (или) пояснения относительно некорректности представленных в уведомлении сведений предоставляются оператором в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций в течение трех рабочих дней со дня получения запроса.

6. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ В ДОКУМЕНТЫ ОПЕРАТОРА

Пересмотр положений настоящего и иных локальных документов Оператора, касающихся вопросов обработки и обеспечения безопасности персональных данных, проводится в следующих случаях, если иное не установлено в пересматриваемых документах:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности персональных данных;
- по результатам внутреннего контроля (аудита) системы защиты персональных данных в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности персональных данных и выявивших недостатки в правилах предоставления доступа к персональным данным.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности персональных данных и Менеджер обработки ПДн.

Внесение изменений производится на основании соответствующего приказа руководителя Оператора.

ПРИЛОЖЕНИЕ 1

ПЛАН ВНУТРЕННИХ ПРОВЕРОК

СОСТОЯНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наименование мероприятий	Срок/периодичность	Ответственный/исполнитель
Контроль за выполнением требований защиты персональных данных в информационных системах персональных данных	1 раз в 12 месяцев	Менеджер обработки ПДн
Оценка эффективности реализованных в рамках системы защиты персональных данных мер	1 раз в 12 месяцев	Администратор безопасности ИСПДн
<...>		

C=RU, O=ГБОУ гимназия г. Сызрани, CN=Назаренко Жанна Игоревна, E=gymn_szr@samara.edu.ru
00d6bd7f5107e9b81
2023.03.01 13:50:41+04'00'