МИНИСТЕРСТВО ОБРАЗОВАНИЯ КАМЧАТСКОГО КРАЯ

Краевое государственное автономное учреждение
дополнительного образования
«Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

ПРИКАЗ № 9/2-у

г. Петропавловск-Камчатский от 01.03.2024 года

Во исполнение требований главы 14 Трудового Кодекса Российской Федерации «Защита персональных данных работника» и Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Ввести в действие Положение об обработке и защите персональных данных в краевом государственном автономном учреждении дополнительного образования «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» (далее – Положение) с 01 марта 2024 года согласно приложению №1 к настоящему приказу.
2. Ввести в действие Положение по организации и проведению работ по обеспечению безопасности персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» (далее – Положение) с 01 марта 2024 года согласно приложению №2 к настоящему приказу.
3. Утвердить перечень должностей, допущенных к работе с персональными данными:

Директор, Ю.Е. Моторина, доступ без ограничений;

Заместитель директора, В.И. Иванова, доступ без ограничений;

Секретарь делопроизводитель, А.А. Теплых, доступ без ограничений;

Программист, С.В. Обухов, доступ без ограничений;

Старший методист, В.В. Киселев, доступ без ограничений;

Методист, А.В. Карабанов, доступ без ограничений.

4. Назначить ответственным лицом за получение, обработку, хранение и уничтожение персональных данных – А.А. Теплых.
5. Ответственному лицу ознакомить лиц, допущенных к работе с персональными данными с Положением и настоящим приказом.

Директор  Ю.Е. Моторина

С приказом ознакомлены:

Заместитель директора		01.03.24	В.И. Иванова
Секретарь делопроизводитель		01.03.24	А.А. Теплых
Программист		01.03.24	С.В. Обухов
Старший методист		01.03.24	В.В. Киселев
Методист		01.03.24	А.В. Карабанов

Приложение№ 2 к приказу
КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»
от 01.03.2024г. № 9/1-у

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

Перечень терминов и сокращений

Обозначение	Описание
Безопасность информации	состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.
Доступность информации	состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
Конфиденциальность информации	обязательное для выполнения лицом, получившим доступ к информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
Компьютерный инцидент	факт нарушения и (или) прекращения функционирования «ИС», сети электросвязи, используемой для организации взаимодействия объекта, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.
Межсетевое взаимодействие	Способ соединения компьютерной сети с другими сетями с помощью шлюзов, которые обеспечивают общепринятый порядок маршрутизации пакетов информации между сетями.
Несанкционированный доступ (НСД)	доступ к информации или действия с информацией, нарушающие правила разграничения доступа, с использованием штатных средств.
Обработка ПДн	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
Ответственный за организацию обработки ПДн	лицо, осуществляющее внутренний контроль за соблюдением организацией и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.
Персональные данные	любая информация, относящаяся к прямо или косвенно

(ПДн)	определенному или определяемому физическому лицу (субъекту ПДн).
Средства защиты информации (СЗИ)	техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.
Средства криптографической защиты информации (СКЗИ)	средства шифрования — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении; средства имитозащиты — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации; средства электронной подписи (ЭП) — аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭП, подтверждение подлинности ЭП, создание Ключей ЭП.
Уполномоченный орган по защите прав субъектов ПДн	федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн.
ФЗ «О персональных данных»	Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1. Общие положения

Целью настоящего положения по организации и проведению работ по обеспечению безопасности персональных данных (далее – ПДн) в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» (далее - Учреждение) является обеспечение защиты прав субъектов ПДн, а также определение основных целей и задач по обеспечению безопасности информации, структуры системы обеспечения безопасности информации и мер по обеспечению безопасности информации в Учреждении.

Правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее — Постановление № 1119), Приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», внутренними организационно-распорядительными документами Учреждения по обеспечению безопасности информации.

Требования настоящих правил обязательны для всех работников, осуществляющих обработку ПДн.

2. Цели и задачи обеспечения безопасности информации

Целью обеспечения безопасности информации является обеспечение устойчивого функционирования информационной системы персональных данных при проведении в отношении нее компьютерных атак.

Основными задачами обеспечения безопасности информации являются:

– предотвращение неправомерного доступа к защищаемой информации, обрабатываемой в Учреждении, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

– недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование

– восстановление функционирования компонентов «информационной системы», обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации.

3. Порядок определения уровня защищенности персональных данных

Определение уровня защищенности осуществляется комиссией, назначенной Приказом директора, на основании Постановления № 1119 и в соответствии с порядком, представленным ниже.

Определение уровня защищенности осуществляется комиссией на основании следующей информации:

– актуальная категория угроз;

– тип ИСПДн;

– количество субъектов, чьи ПДн обрабатываются;

– являются ли Субъекты ПДн работниками Учреждения или нет.

В соответствии с п. 5 Постановления № 1119 выделяются следующие типы информационных систем:

ИСПДн-С: информационная система, обрабатывающая специальные категории ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

ИСПДн-Б: информационная система, обрабатывающая биометрические ПДн, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям ПДн;

ИСПДн-Д: информационная система, обрабатывающая общедоступные ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со ст. 8 ФЗ «О персональных данных»;

ИСПДн-И: информационная система, обрабатывающая иные ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим и общедоступным ПДн.

В соответствии с п. 6 Постановления № 1119 под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке, результатом которого могут стать

уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия. Выделяют следующие категории угроз:

– угрозы 1-го типа — угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в «СУИТ»;

– угрозы 2-го типа — угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в «СУИТ»;

– угрозы 3-го типа — угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в «СУИТ».

Для определения уровня защищенности выполняются следующие действия:

– составляется список компонентов, в которых обрабатываются ПДн;

– определяются цели обработки ПДн;

– определяются компоненты, для которых цели обработки ПДн определяют другие юридические лица или государственные органы, и/или Учреждение не является владельцем системы (не является владельцем средств обработки информации), и/или в которых обрабатываются ПДн, не позволяющие определить Субъекта ПДн. Выявленные компоненты исключаются из дальнейшего рассмотрения;

– определяются типы компонентов;

– определяются категории актуальных угроз;

– определяется количество Субъектов ПДн, являющихся работниками Учреждения и не являющихся таковыми;

– определяются уровни защищенности компонентов в соответствии с Постановлением № 1119.

Комиссия фиксирует результаты определения уровня защищенности в «Акте определения уровня защищенности персональных данных». Пересмотр уровня защищенности осуществляется в рамках ежегодного в рамках аудита.

4. Уведомление об обработке ПДн

Учреждение в соответствии со ст. 22 ФЗ «О персональных данных» обязано подать уведомление об обработке ПДн (далее –– Уведомление) в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее –– Роскомнадзор).

Подготовку, контроль отправки Уведомления в Роскомнадзор, внесение изменений в уведомление в случае необходимости, взаимодействие с Роскомнадзором по вопросам, касающимся уведомления, осуществляет ответственный за организацию обработки ПДн.

Для подготовки уведомления ответственный за организацию обработки ПДн руководствуется требованиями ФЗ «О персональных данных», а также методическими рекомендациями по заполнению Уведомления, размещенными на официальном сайте Роскомнадзора: https://rkn.gov.ru/.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки ПДн ответственный за организацию обработки ПДн обязан уведомить об этом Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн, посредством отправки информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн.

5. Уведомление об инцидентах

В Учреждении в соответствии со ст. 19 ФЗ «О персональных данных» необходимо проводить обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них.

Учреждение обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Учреждение обязано с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех 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;

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).

6. Структура системы обеспечения информационной безопасности

В Учреждении объектами, подлежащими защите от угроз безопасности информации (объектами защиты), являются:

– защищаемая информация (ПДн, учетные данные пользователей, данные о конфигурации информационной системы);

– узел вычислительной сети, включая: автоматизированные рабочие места, виртуальные серверы.

– программно-аппаратные средства[1] обработки и хранения ПДн, включая: съемные машинные носители информации, машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);

– сетевой трафик;

– средство защиты информации;

– сетевое (телекоммуникационное) оборудование;

– сетевое программное обеспечение;

– системное программное обеспечение;

– прикладное программное обеспечение (далее в настоящем документе рассмотрено в составе узлов: АРМ и виртуальных серверов);

---

[1] Имеющие объекты файловой системы

– обеспечивающие системы.

Для обеспечения безопасности информации в Учреждении функционирует система обеспечения информационной безопасности, в рамках которой реализованы правовые, организационные, технические и иные меры, направленные на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к прекращению или нарушению функционирования компонентов ИС и обеспечивающих (управляемого, контролируемого) им процессов, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации) и обеспечивающие устойчивое функционирование компонентов ИС при проведении в отношении него компьютерных атак.

Система обеспечения информационной безопасности включает силы обеспечения информационной безопасности и используемые ими средства обеспечения информационной безопасности.

К силам обеспечения информационной безопасности относятся:

– Ответственный за обеспечение безопасности ПДн;

– Ответственный за обработку ПДн;

– Администратор информационной безопасности;

– подразделения (работники), эксплуатирующие «ИС»;

– подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) компонентов «ИС».

К средствам обеспечения информационной безопасности относятся программные и программно-аппаратные средства, применяемые для обеспечения информационной безопасности: средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства обнаружения (предотвращения) вторжений (компьютерных атак), средства антивирусной защиты, средства (системы) контроля (анализа) защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

7. Меры по обеспечению безопасности информации

Система обеспечения информационной безопасности должна соответствовать уровню защищенности ПДн, а также обеспечивать нейтрализацию актуальных угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях.

Учреждение вправе привлекать юридических лиц, имеющих соответствующие лицензии ФСТЭК России для осуществления деятельности по технической защите информации, в том числе по внедрению СЗИ.

Состав подлежащих реализации организационных и технических мер по обеспечению безопасности информации определяется и обосновывается на этапе проектирования системы обеспечения информационной безопасности.

В целях обеспечения безопасности информации в «*ИС*» реализуются следующие меры:

– идентификация и аутентификация;

– управление доступом;

– защита машинных носителей персональных данных;

– регистрация событий информационной безопасности;

– защита межсетевого взаимодействия;

– антивирусная защита;

– анализ защищенности информации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– управление конфигурацией и системой обеспечения информационной безопасности;

– криптографическая защита информации;

– безопасность технических средств и помещений;

– повышение осведомленности по вопросам обеспечения безопасности информации;

– контроль порядка обработки и защиты информации.

При использовании в «ИС» новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации. При этом в ходе разработки организационных и технических мер по обеспечению безопасности информации должно быть обосновано применение компенсирующих мер.

Технические меры по обеспечению безопасности информации реализуются посредством использования программных и программно-

аппаратных средств – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение), а также обеспечения безопасности программного обеспечения и программно-аппаратных средств.

Безопасность информации должна обеспечиваться на всех технологических этапах обработки, в том числе при проведении ремонтных и регламентных работ. Для обеспечения безопасности информации должны применяться СЗИ, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

8. Контроль и управление доступом пользователей к информационным ресурсам

Перечень работников, допущенных к обработке ПДн, утверждается директором Учреждения. Доступ работников к обработке ПДн предоставляется по согласованию с Ответственным за обеспечение безопасности ПДн.

Контроль прав доступа пользователей проводится на регулярной основе, не реже одного раза в год.

Пользователи допускаются к обработке ПДн только после прохождения инструктажа по вопросам обеспечения безопасности ПДн.

При взаимодействии Учреждения с юридическими и физическими лицами, при котором Учреждение осуществляет передачу ПДн такому лицу, должно быть оформлено соответствующее поручение на обработку ПДн этим лицом.

Надзорному органу, осуществляющему функции контроля (надзора) в области ПДн (Роскомнадзор), должны предоставляться права доступа к ПДн, обрабатываемым Учреждением, только в сфере их компетенции и в объеме, предусмотренном законодательством Российской Федерации.

Учреждением должна обеспечиваться однозначная идентификация и аутентификация субъектов доступа (внутренних, внешних) при доступе к объектам доступа.

Запрещается повторное использование пароля пользователя, а также совместное использование одного пароля несколькими пользователями.

Любые действия пользователей до прохождения процедуры идентификации и аутентификации на автоматизированном рабочем месте пользователя запрещены.

В процессе ввода пароля должно осуществляться его сокрытие посредством отображения специальных условных знаков, например, «*», «•».

В «ИС» должны быть предусмотрены меры своевременного блокирования доступа пользователя в случае компрометации пароля пользователя, отзыва прав доступа, нарушения политики безопасности.

В «ИС» должно быть ограничено количество неуспешных попыток входа, а также должно обеспечиваться блокирование сеанса доступа после установленного времени бездействия пользователя или по запросу пользователя.

Несанкционированное подключение к «ИС» мобильных технических средств и портативных рабочих станций запрещено.

9. Ограничение программной среды

В Учреждении должен быть определен перечень компонентов ПО (состава и конфигурации), подлежащих установке после загрузки операционной системы.

Параметры установки компонентов ПО должны исключать установку компонентов ПО, использование которых не требуется для реализации информационной технологии. При установке ПО должна быть возможность выбора конфигурации устанавливаемых компонентов ПО.

Контроль за установкой компонентов ПО (состав компонентов, параметры установки, конфигурация компонентов) осуществляется ответственными за обеспечение безопасности информации в пределах своих компетенций.

Параметры настройки компонентов ПО, включая программные компоненты СЗИ, должны обеспечивать реализацию мер защиты информации, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации.

10. Обеспечение безопасности носителей информации

Должен быть разработан журнал машинных носителей защищаемой информации и места их хранения (далее — Перечень).

Запрещается хранить защищаемую информацию в местах, не указанных в Перечне.

Для хранения носителей информации используются специально оборудованные хранилища (сейфы, шкафы, и т.п.), исключающие возможность несанкционированного копирования информации и хищения носителей информации.

Перемещение носителей информации за пределы Учреждения допускается по согласованию в простой письменной форме по электронной почте с ответственными за обеспечение безопасности информации в пределах их компетенций.

В Учреждении должен быть определен порядок работы с носителями защищаемой информации, который должен предусматривать

порядок учета, хранения и обращения с носителями информации, а также порядок их уничтожения.

11. Регистрация событий информационной безопасности

К событиям безопасности, подлежащим регистрации в «ИС», относятся проявления состояния и системы защиты, указывающие на возможность нарушения Конфиденциальности, Целостности или Доступности информации, нарушения процедур, установленных внутренними нормативными документами Учреждения по защите информации, а также на нарушения штатного функционирования СЗИ. Регистрации подлежат события информационной безопасности, связанные с применением выбранных в Учреждении, мер по защите информации в «ИС».

В Учреждении должны быть определены правила и процедуры регистрации событий безопасности, которые должны предусматривать события безопасности, подлежащие регистрации, состав и содержание информации о событиях безопасности, сроки хранения соответствующих записей регистрационных журналов, а также защиту информации о событиях безопасности.

12. Защита межсетевого взаимодействия

В рамках обеспечения защиты межсетевого взаимодействия в Учреждении должна осуществляться фильтрация информационных потоков в соответствии со списками контроля доступа, настраиваемыми работниками на средствах межсетевого экранирования.

Маршруты, по которым разрешено передавать информацию, должны определяться, исходя из архитектуры сети и процессов обработки информации, и настраиваться работниками посредством создания списков контроля доступа на межсетевых экранах и телекоммуникационном оборудовании.

Правила управления информационными потоками должны учитывать, как минимум, адреса источника и получателя информации.

13. Антивирусная защита

Средства антивирусной защиты должны устанавливаться на всех рабочих станциях и серверах «ИС».

Средства антивирусной защиты, должны обеспечивать:

– автоматическую проверку на наличие вредоносных программ (вирусов);

– механизмы автоматического блокирования обнаруженных вредоносных программ (вирусов);

– регулярную проверку (с устанавливаемой периодичностью) на предмет наличия вредоносных программ;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов).

В Учреждении должны быть определены правила и процедуры антивирусной защиты, обновления базы данных признаков вредоносных программ (вирусов), а также реагирования на вирусные заражения.

14. Обнаружение вторжений

В Учреждении должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к защищаемой информации, специальные воздействия на такую информацию в целях их добывания, уничтожения, искажения и блокирования доступа к ним, с использованием систем обнаружения вторжений.

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

В Учреждении должны быть определены правила и процедуры обнаружения вторжений, обновления базы решающих правил.

15. Анализ защищенности

В Учреждении должны осуществляться регулярное выявление (поиск), анализ и устранение уязвимостей компонентов «ИС».

При выявлении (поиске), анализе и устранении уязвимостей должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении СЗИ, правильностью установки и настройки СЗИ, технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль (анализ) защищенности информации должен осуществляться посредством контроля ПО, применяемого для обработки и защиты информации, на наличие настроек, позволяющих получать и устанавливать обновления ПО.

Контроль работоспособности (неотключения) программного обеспечения и СЗИ должен включать проверку правильности функционирования программного обеспечения и СЗИ, контроль соответствия настроек программного обеспечения и СЗИ параметрам настройки.

Ответственные за обеспечение безопасности информации в пределах своих компетенций не реже одного раза в шесть месяцев должны осуществляться контроль состава технических средств, программного обеспечения и СЗИ, применяемых в «ИС».

16. Обеспечение целостности и доступности информации

Должен осуществляться контроль целостности ПО, включая программное обеспечение СЗИ.

Контроль целостности ПО, включая программное обеспечение СЗИ, должен предусматривать:

– контроль целостности ПО СЗИ, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов СЗИ в процессе загрузки и (или) динамически в процессе работы компонентов «ИС»;

– контроль целостности компонентов ПО (за исключением СЗИ), исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов ПО и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы компонентов «ИС»;

– контроль применения средств разработки и отладки программ в составе ПО;

– регулярное тестирование функций безопасности СЗИ, в том числе с помощью тест-программ, имитирующих попытки НСД;

– обеспечение физической защиты технических средств.

Для обеспечения возможности восстановления функционирования и работоспособности компонентов «ИС» и средств защиты информации при возникновении аварийных ситуаций должны быть реализованы механизмы резервного копирования и восстановления информации с резервных машинных носителей.

В рамках резервного копирования должен обеспечиваться контроль результатов всех процедур резервного копирования с целью обнаружения ошибки или аварии с последующим уведомлением заинтересованных лиц.

Порядок восстановления информации с резервных машинных носителей информации (резервных копий) должен обеспечивать восстановление информации в течение установленного интервала времени.

Должны быть определены места хранения резервных копий и предприняты меры обеспечения их безопасности. Для защиты резервируемой информации также должны быть предприняты меры, обеспечивающие ее конфиденциальность, целостность и доступность.

17. Выявление инцидентов и реагирование на них

В Учреждении должно проводиться выявление инцидентов и реагирование на них.

Пользователи должны своевременно информировать лиц, ответственных за выявление инцидентов и реагировать на них.

При реагировании на инциденты должны осуществляться:

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, ПО и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению «ИС» и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

18. Управление конфигурацией

При внесении изменений в конфигурацию компонентов «ИС» и систему обеспечения информационной безопасности необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации, на работоспособность «ИС» и систему обеспечения информационной безопасности.

Внесение изменений должно быть согласовано с ответственными за обеспечение безопасности информации в пределах своих компетенций.

Управление конфигурацией компонентов и системы обеспечения информационной безопасности должно осуществляться только ответственными за обеспечение безопасности информации, а также лицами, ответственными за администрирование и поддержку компонентов «ИС» и СЗИ.

19. Безопасность технических средств и помещений

В помещениях, в которых осуществляется обработка защищаемой информации, должен обеспечиваться режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях, где размещены технические средства «ИС», СКЗИ, носители ключевой, аутентифицирующей и парольной информации СКЗИ, лиц, не имеющих права доступа в помещения.

Помещения должны быть оснащены входными дверьми с замками или СКУД, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не допускается размещение устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

20. Повышение осведомленности по вопросам обеспечения безопасности информации

В Учреждении должны быть определены следующие виды повышения осведомленности пользователей по вопросам обеспечения безопасности информации: вводный инструктаж и внеплановый инструктаж по обеспечению безопасности информации.

Вводный инструктаж должен проходить каждый работник при приеме на работу в случае, если его функциональные обязанности подразумевают обработку защищаемой информации или обеспечение функционирования компонентов «ИС».

Внеплановый инструктаж должен проводиться в случаях, если:

– изменились организационно-технические мероприятия по обработке и защите информации, принятые в Учреждении;

– изменились функциональные обязанности Пользователя, связанные с обработкой защищаемой информации;

– изменился состав программных средств для обработки защищаемой информации;

– изменился состав средств защиты информации.

Плановый и внеплановый инструктажи должны проводиться в срок не позднее 10 рабочих дней с момента принятия на работу нового работника или внесения изменений в организационно-технические мероприятия по обработке и защите информации.

Допуск работников к обработке защищаемой информации должен осуществляться только после прохождения вводного инструктажа при приеме на работу и ознакомления с внутренними нормативными документами по вопросам обработки информации и обеспечения безопасности такой информации с обязательной письменной фиксацией факта ознакомления.

21. Контроль порядка обработки и защиты информации

В Учреждении должен быть определен состав и порядок проведения мероприятий по контролю обеспечения безопасности информации при их обработке в Учреждении.

При выявлении нарушений требований законодательства Российской Федерации и нормативных документов Учреждения в отношении обработки и обеспечения безопасности информации, в том числе настоящего Положения, ответственные за обеспечение безопасности информации в пределах своих полномочий вправе инициировать служебное расследование. Результаты служебного расследования доводятся до сведения руководства для вынесения решения по факту нарушения указанных требований.

22. Контроль эффективности обеспечения безопасности информации

С целью поддержания безопасности «ИС» необходимом и достаточном уровне в Учреждении реализуется система регулярного контроля применяемых мер по обеспечению безопасности (мероприятия по контролю).

Ответственность за планирование и проведение контрольных мероприятий возложена на ответственных за обеспечение безопасности информации в пределах своей компетенции.

23. Ответственность

Работники Учреждения, осуществляющие обработку защищаемой информации, а также ответственные за обеспечение безопасности информации в пределах своей компетенции несут дисциплинарную, гражданско-правовую,

административную или уголовную ответственность в соответствии с законодательством Российской Федерации за нарушение требований настоящего Положения, иных внутренних нормативных документов Учреждения и законодательства Российской Федерации в области защиты информации.

Приложение № 1 к приказу КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» от 01.03.2024 года № 9/1-у

Положение
об обработке и защите персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

1.Общие положения

1.1. Настоящее Положение «Об обработке и защите персональных данных работников КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» (далее -Положение) является локальным нормативным актом КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» (далее - учреждение), принятым с учетом требований главы 14 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных).

1.2. В Положении устанавливаются:

- цель, порядок и условия обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются, категории (перечни) обрабатываемых персональных данных, способы, сроки их обработки и хранения, порядок уничтожения таких данных при достижении целей обработки или при наступлении иных законных оснований;
- положения, касающиеся защиты персональных данных, процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в области персональных данных, а также на устранение последствий таких нарушений.

1.3. В Положении используются термины и определения в соответствии с их значениями, определенными в Законе о персональных данных.

1.4. Положение вступает в силу с момента его утверждения директором учреждения и действует до его отмены приказом директора учреждения или до введения нового Положения.

1.5. Внесение изменений в Положение осуществляется приказом директора Учреждения. Изменения вступают в силу с момента подписания соответствующего приказа.

2. Категории субъектов персональных данных

2.1. К субъектам, персональные данные которых обрабатываются в Учреждении в соответствии с Положением, относятся:

- кандидаты для приема на работу в учреждение;
- работники учреждения;
- бывшие работники учреждения;
- члены семей работников учреждения - в случаях, когда согласно законодательству сведения о них предоставляются работником;

- иные лица, персональные данные которых учреждение обязано обрабатывать в соответствии с трудовым законодательством и иными актами, содержащими нормы трудового права;
- обучающиеся;
- законные представители обучающихся;
- участники мероприятий;
- контрагенты.

3. Цели обработки персональных данных субъектов персональных данных, категории (перечни) обрабатываемых персональных данных

3.1. Целями обработки персональных данных субъектов персональных данных являются:
- осуществление деятельности согласно Уставу учреждения;
- исполнение договора об образовании по дополнительным общеобразовательным общеразвивающим программам;
- исполнение иных договорных отношений;
- проведение краевых конкурсных мероприятий детей и молодежи;
- оформление трудовых отношений;
- обеспечении личной безопасности работников и сохранности имущества.

3.2. В соответствии с целями, указанными в п. 3.1 Положения, в учреждении обрабатываются следующие персональные данные:
- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- пол;
- фотографическое изображение;
- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;
- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- информация о владении иностранными языками;

- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);

- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы;

- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);

- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях получения образования (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ);

- сведения о доходах, обязательствах по исполнительным документам;

- номера расчетного счета, банковской карты;

- сведения о состоянии здоровья работников, обучающихся (на спортивные образовательные программы);

- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;

- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 3.1 Положения;

- иные персональные данные, которые работник, обучающийся (законный представитель) пожелал сообщить о себе и обработка которых соответствует цели обработки, предусмотренной п. 3.1 Положения.

3.3. Учреждение не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

4. Порядок и условия обработки персональных данных

4.1. До начала обработки персональных данных учреждение обязано уведомить Роскомнадзор о намерении осуществлять обработку персональных данных.

4.2. Правовым основанием обработки персональных данных являются Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Гражданский кодекс Российской Федерации от 30.11.1994 №51-ФЗ, Семейный кодекс Российской Федерации 29.12.1995 № 223-ФЗ, Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ, иные нормативные правовые акты, содержащие нормы трудового права, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Закон РФ от 19.04.1991 № 1032-1 «О занятости населения в Российской Федерации», Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете».

4.3. Обработка персональных данных осуществляется с соблюдением принципов и условий, предусмотренных законодательством в области персональных данных и настоящим Положением.

4.4. Обработка персональных данных в учреждении выполняется следующими способами:

- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

4.5. Обработка персональных данных в учреждении осуществляется с согласия субъекта персональных данных (законного представителя субъекта персональных данных) на обработку его персональных данных, если иное не предусмотрено законодательством в области персональных данных.

4.5.1. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 Закона о персональных данных.

Согласие на обработку таких персональных данных оформляется отдельно от других согласий на обработку персональных данных. Согласие предоставляется субъектом персональных данных лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.

4.5.2. Обработка биометрических персональных данных допускается только при наличии письменного согласия субъекта персональных данных. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 Закона о персональных данных.

4.6. Трансграничная передача персональных данных может осуществляться в соответствии с требованиями, предусмотренными ст. 12 Закона о персональных данных.

4.7. Обработка персональных данных осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, обезличивания, блокирования, удаления, уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

4.7.1. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных в учреждении осуществляются посредством:

- получения оригиналов документов либо их копий;
- копирования оригиналов документов;
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения персональных данных в информационные системы персональных данных.

4.8. Передача (распространение, предоставление, доступ) персональных данных субъектов персональных данных осуществляется в случаях и в порядке, предусмотренных законодательством в области персональных данных и Положением.

5. Сроки обработки и хранения персональных данных

5.1. Обработка персональных данных в учреждении прекращается в следующих случаях:

- при выявлении факта неправомерной обработки персональных данных. Срок прекращения обработки - в течение трех рабочих дней с даты выявления такого факта;
- при достижении целей их обработки (за некоторыми исключениями);
- по истечении срока действия или при отзыве субъектом персональных данных согласия на обработку его персональных данных (за некоторыми исключениями), если в соответствии с Законом о персональных данных их обработка допускается только с согласия;
- при обращении субъекта персональных данных к учреждению с требованием о прекращении обработки персональных данных (за исключением случаев, предусмотренных частью 5.1 статьи 21 Закона о персональных данных). Срок прекращения обработки - не более десяти рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

5.2. Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Исключение - случаи, когда срок хранения персональных данных установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных.

5.3. Персональные данные на бумажных носителях хранятся в учреждении в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения (утвержден Приказом Росархива от 20.12.2019 № 236).

5.4. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

6. Порядок блокирования и уничтожения персональных данных

6.1. Учреждение блокирует персональные данные в порядке и на условиях, предусмотренных законодательством в области персональных данных.

6.2. При достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей персональные данные уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.

6.3. Незаконно полученные персональные данные или те, которые не являются

необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом персональных данных (его представителем) подтверждающих сведений.

6.4. Персональные данные, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления неправомерной обработки.

6.5. Персональные данные уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иным соглашением между ним и учреждением либо если учреждение не вправе обрабатывать персональные данные без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.5.1. При достижении максимальных сроков хранения документов, содержащих персональные данные, персональные данные уничтожаются в течение 30 дней.

6.6. Персональные данные уничтожаются (если их сохранение не требуется для целей обработки персональных данных) в течение 30 дней с даты поступления отзыва субъектом персональных данных согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект персональных данных, иное соглашение между ним и учреждением. Кроме того, персональные данные уничтожаются в указанный срок, если учреждение не вправе обрабатывать их без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6.7. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению, осуществляют сотрудники Учреждения, обрабатывающие персональные данные.

6.8. Уничтожение персональных данных осуществляет комиссия, созданная приказом директора Учреждения.

6.8.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих персональные данные, которые подлежат уничтожению.

6.8.2. Персональные данные на бумажных носителях уничтожаются с использованием шредера. Персональные данные на электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.

6.8.3. Комиссия подтверждает уничтожение персональных данных, указанных в п. п. 6.4, 6.5, 6.6 Положения, согласно Требованиям к подтверждению уничтожения персональных данных, утвержденным Приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении персональных данных - если данные обрабатываются

без использования средств автоматизации;

- актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных - если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом директора учреждения.

6.8.4. После составления акта об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных комиссия передает их в общий отдел для последующего хранения. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

6.8.5. Уничтожение персональных данных, не указанных в п. 6.8.3 Положения, подтверждается актом, который оформляется непосредственно после уничтожения таких данных. Форма акта утверждается приказом директора.

7. Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

7.1. Без письменного согласия субъекта персональных данных учреждение не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

7.2. Запрещено раскрытие и распространение персональных данных субъектов персональных данных по телефону.

7.3. С целью защиты персональных данных в учреждении назначаются (утверждаются):

- работники, ответственные за организацию обработки персональных данных;
- перечень должностей, при замещении которых обрабатываются персональные данные;
- перечень персональных данных, к которым имеют доступ работники, занимающие должности, предусматривающие обработку персональных данных;
- порядок доступа в помещения, в которых ведется обработка персональных данных;
- порядок передачи персональных данных в пределах учреждения;
- форма согласия на обработку персональных данных, форма согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области персональных данных.

7.4. Работники, которые занимают должности, предусматривающие обработку

персональных данных, допускаются к ней после подписания обязательства об их неразглашении.

7.5. Материальные носители персональных данных хранятся в шкафах, запирающихся на ключ. Помещения учреждения, в которых они размещаются, оборудуются запирающими устройствами. Выдача ключей от шкафов и помещений осуществляется под подпись.

7.6. Доступ к персональной информации, содержащейся в информационных системах Учреждения, осуществляется по индивидуальным паролям.

7.7. В учреждении используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

7.8. Работники учреждения, обрабатывающие персональные данные, периодически проходят обучение требованиям законодательства в области персональных данных.

7.9. В должностные инструкции работников учреждения, обрабатывающих персональные данные, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к персональным данным.

7.10. В учреждении проводятся внутренние расследования в следующих ситуациях:

- при неправомерной или случайной передаче (предоставлении, распространении, доступе) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в иных случаях, предусмотренных законодательством в области персональных данных.

7.11. Работники, ответственные за организацию обработки персональных данных, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку персональных данных, требований законодательства в области персональных данных, локальных нормативных актов;
- соответствием указанных актов, требованиям законодательства в области персональных данных.

7.12. Внутренний контроль проходит в виде внутренних проверок.

7.12.1. Внутренние плановые проверки осуществляются на основании ежегодного плана, который утверждается директором учреждения.

7.12.2. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки персональных данных. Основанием для них служит информация о нарушении законодательства в области персональных данных, поступившая в устном или письменном виде.

7.12.3. По итогам внутренней проверки оформляется докладная записка на имя директора учреждения. В случае выявления нарушений в документе приводятся перечень мероприятий по их устранению и соответствующие сроки.

7.13. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее - инцидент).

7.13.1. В случае инцидента учреждение в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) персональных данных;
- принятых мерах по устранению последствий инцидента;
- представителе учреждения, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

При направлении уведомления нужно руководствоваться Порядком и условиями 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, утвержденными Приказом Роскомнадзора от 14.11.2022 № 187.

7.13.2. В течение 72 часов учреждение обязано:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

7.14. При направлении уведомления также необходимо руководствоваться Порядком и условиями 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, утвержденными Приказом Роскомнадзора от 14.11.2022 № 187.

7.15. В случае предоставления субъектом персональных данных (его представителем) подтвержденной информации о том, что персональные данные являются неполными, неточными или неактуальными, в них вносятся изменения в течение семи рабочих дней. Учреждение уведомляет в письменном виде субъекта персональных данных (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы персональные данные.

7.16. Учреждение уведомляет субъекта персональных данных (его представителя) об устранении нарушений в части неправомерной обработки персональных данных. Уведомляется также Роскомнадзор, если он направил обращение субъекта персональных данных (его представителя) либо сам сделал запрос.

7.17. В случае уничтожения персональных данных, которые неправомерно обрабатывались, уведомление направляется в соответствии с п. 7.13 Положения.

7.18. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, учреждение уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Учреждение уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

7.19. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», осуществляется в соответствии с Приказом Роскомнадзора от 27.10.2022 № 178 «Об

утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

8.Ответственность за нарушение норм, регулирующих обработку персональных данных

8.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Кроме того, они привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

8.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к их защите, установленных Законом о персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение 1 к Положению об обработке и защите персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

Порядок доступа работников КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» в помещения, в которых ведется обработка персональных данных

1. Настоящее Положение о порядке доступа работников КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход» в помещения, в которых ведется обработка персональных данных, разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей», предусмотренных Федеральным законом «О персональных данных».

2. Персональные данные относятся к конфиденциальной информации. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установление правил доступа в помещения, где обрабатываются персональные данные в информационной системе персональных данных и без использования средств автоматизации.

4. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники организации, ответственные за обработку персональных данных, назначенные приказом директора учреждения.

6. Нахождение лиц в помещениях КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход», не имеющих соответствующий допуск, возможно только в сопровождении ответственного сотрудника организации на время, ограниченное необходимостью решения вопросов, связанных с исполнением функции.

7. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится лицом ответственным за организацию обработки персональных данных.

Приложение 2 к Положению об обработке и защите персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

Акт уничтожения персональных данных

г. Петропавловск-Камчатский «____» _____ 20___г

В соответствии с положениями ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в связи с _____ (причина) _____.

Комиссия в составе:

Председатель комиссии: _____(должность) _____(Ф.И.О.)

Члены комиссии: _____(должность) _____(Ф.И.О.)

_____(должность) _____(Ф.И.О.)

_____(должность) _____(Ф.И.О.)

на основании приказа № _____ от _____г. составила настоящий акт о том, что «_____» _____20__г. в присутствии комиссии ведущий специалист по кадрам произвел уничтожение следующих персональных данных:

№ п/п	Субъект и вид персональных данных	Дата уничтожения	Процедура уничтожения	Причина уничтожения

Персональные данные на бумажном носителе/ в электронном виде (тип носителя) уничтожены путем _____ (способ уничтожения), что гарантирует полное уничтожение персональных данных.

Председатель комиссии:

_____(должность) _____(Ф.И.О.) _____(дата)

Члены комиссии:

_____(должность) _____(Ф.И.О.) _____(дата)

_____(должность) _____(Ф.И.О.) _____(дата)

_____(должность) _____(Ф.И.О.) _____(дата)

Приложение 3 к Положению об обработке и защите персональных данных в КГАУ ДО «Региональный центр выявления, развития и поддержки способностей и талантов у детей и молодежи «Восход»

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество - при наличии)
основной документ, удостоверяющий личность: _____
_____
(вид документа, серия, номер, дата выдачи документа, наименование выдавшего органа)

зарегистрированный(ая) по адресу: _____
_____
даю свое согласие на обработку моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство; сведения об инвалидности, банковские реквизиты и иные сведения.

Я даю согласие на использование персональных данных исключительно в целях рассмотрения моих документов, а также на хранение данных об этих результатах
на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных,
а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что получатель сведений гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

«___» _____20____ г. /_____/ _____
(Подпись) *(Расшифровка)*