МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ
РЕСПУБЛИКИ КРЫМ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ДЕТСКО-ЮНОШЕСКОГО ТУРИЗМА И КРАЕВЕДЕНИЯ»
untur@crimeaedu.ru тел. + 7 (978) 973 25 98
295001 г. Симферополь, ул. Крылова, 60

# ПОЛИТИКА

**в области обработки и защиты персональных данных**

**в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения»**

**Симферополь**
**2023 г.**

УТВЕРЖДАЮ

Директор ГБОУ ДО РК «ЦДЮТК»

Осокина Е.А.

пр. № 512 «29» декабря 2023 г.

# ПОЛИТИКА
## в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения»

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях поддержания деловой репутации и гарантирования выполнения норм федерального законодательства в полном объеме Государственное бюджетное образовательное учреждение дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения» (далее – Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая Политика разработана на основании статей Конституции Российской Федерации (далее – Конституция РФ), Трудового кодекса Российской Федерации (далее – ТК РФ), Кодекса Российской Федерации об административных правонарушениях, Гражданского кодекса Российской Федерации, Уголовного кодекса Российской Федерации, Федерального закона Российской Федерации от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации» (далее – 273-ФЗ), Федерального закона Российской Федерации от 27.07.2006 № 149 – ФЗ "Об информации, информационных технологиях и о защите информации", Федерального закона Российской Федерации от 27.07.2006 № 152 – ФЗ "О персональных данных" (далее 152-ФЗ), Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети Интернет и обновления информации об образовательной организации, утвержденными постановлением Правительства от 20.10.2021 г. (далее Правила от 20.10.2021 г. ) , иными федеральными и региональными нормативными актами в сфере защиты персональных данных.

1.3. Настоящая Политика в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения» (далее – Политика) характеризуется следующими признаками:

1.3.1. Разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных.

1.3.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.3.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

1.3.4. Утверждается и вводится в действие приказом директора и является обязательной для исполнения всеми работниками, имеющими доступ к персональным данным.

1.4. Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

1.5. Основные понятия, используемые в Политике:

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

1.5.2. 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 152 – ФЗ;

1.5.3. оператор 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;

1.5.4. субъект персональных данных – участник операций с информацией о его личности;

1.5.5. обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя, в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

1.5.6. автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

1.5.7. распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

1.5.8. предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

1.5.10. 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;

1.5.11. обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
1.5.12. информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
1.5.13. трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
1.6. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области (ст. 86 ТК РФ).
1.7. Неотъемлемой часть настоящей Политики являются:
1.7.1. Перечень персональных данных, обрабатываемых в ГБОУ ДО РК «ЦДЮТК» (Приложение № 1).
1.7.2. Перечень основных видов угроз безопасности персональных данных в информационных системах персональных данных (Приложение № 2).
1.7.3. Обязательство о неразглашении персональных данных работников (Приложение 3).
1.7.4. Согласие на обработку персональных данных работника (Приложение 4).
1.7.5. Согласие субъекта на получение его персональных данных у третьей стороны (Приложение 5).
1.7.6. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приложение 6).

## 2. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ

Наименование: Государственное бюджетное образовательное учреждение дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения»
ИНН: 9102057796
Фактический адрес: 295011, Россия, Республика Крым, г. Симферополь, ул. Турецкая, дом 8
Тел. + 7978 973 25 98
Реестр операторов, осуществляющих обработку персональных данных: https://rkn.gov.ru/personal-data/register/?id=91-18-008253

## 3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Оператор обрабатывает персональные данные исключительно в следующих целях:
– Исполнения положений нормативных актов, указанных в п. 4.1 настоящей Политики.
– Принятия решения о трудоустройстве кандидата в ГБОУ ДО РК «ЦДЮТК».
– Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами.
– Осуществления пропускного и внутриобъектового режима.
3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определённых и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Целью настоящей Политики является обеспечение прав и свобод человека и гражданина при обработке его персональных данных.

3.4. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, выявление неправомерной обработки персональных данных либо ликвидация ГБОУ ДО РК «ЦДЮТК» а также основания, предусмотренные законодательством Российской Федерации.

## 4. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Правовым основанием обработки персональных данных» является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, а именно:

- Конституция РФ.
- Трудовой Кодекс РФ.
- Кодекс РФ об административных правонарушениях.
- Гражданский кодекс РФ.
- Налоговый кодекс РФ.
- Закон РФ от 27.11.1992 № 4015-1 «Об организации страхового дела в Российской Федерации».
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных».
- Федеральный закон от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации».
- Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».
- Постановление Правительства Российской Федерации от 20.10.2021 № 1802 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации».
- Приказ Федеральной службы по надзору в сфере образования и науки от 14.08.2020 № 831 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации (зарегистрирован Министерством юстиции Российской Федерации № 60867 от 12.11.2020 г.).
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Иные нормативные акты, регулирующие отношения, связанные с обработкой персональных данных.
- Уставные документы ГБОУ ДО РК «ЦДЮТК».
- Договоры, заключаемые ГБОУ ДО РК «ЦДЮТК» с субъектами персональных данных.
- Согласия на обработку персональных данных, получаемые Оператором.

## 5. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Содержание и объём обрабатываемых персональных данных соответствуют заявленным целям обработки и не являются избыточными по отношению к заявленным целям их обработки.

5.2. К категориям субъектов персональных данных относятся:

5.2.1. Персональные данные сотрудников. Источники получения: субъекты персональных данных ГБОУ ДО РК «ЦДЮТК».

5.2.2. Персональные данные учредителей, директора. Источники получения: субъекты персональных данных ГБОУ ДО РК «ЦДЮТК».

5.2.3. Персональные данные контрагентов (и их представителей). Источники получения: субъекты персональных данных ГБОУ ДО РК «ЦДЮТК», налоговые органы.

5.2.4. Персональные данные посетителей. Источники получения: субъекты персональных данных - посетители.

5.2.5. Персональные данные кандидатов. Источники получения: субъекты персональных данных кандидаты на должность.

5.2.6. Сроки обработки и хранения персональных данных определяются настоящей Политикой.

5.3. Категории обрабатываемых персональных данных определяются Приложением № 1 (Перечень персональных данных, обрабатываемых в ГБОУ ДО РК «ЦДЮТК») к настоящей Политике.

5.4. Состав персональных данных работника:

5.4.1. анкета;

5.4.2. автобиография;

5.4.3. паспортные данные;

5.4.4. фамилия, имя, отчество (при наличии);

5.4.5. дата рождения;

5.4.6. место рождения;

5.4.7. адрес места жительства (данные о прописке и фактическом месте проживания);

5.4.8. сведения о воинском учете;

5.4.9. сведения о составе семьи;

5.4.10. фамилия, имя, отчество (при наличии), дата рождения детей;

5.4.11. сведения об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении учетной степени, ученого звания (если таковые имеются) и т.п.;

5.4.12. данные о страховом номере индивидуального лицевого счета;

5.4.13. данные Полиса обязательного медицинского страхования;

5.4.14. информация о наличии/отсутствии судимостей и/или наличие обязательств по исполнительным листам.

5.4.15. свидетельство о постановке на учет физического лица в налоговом органе;

5.4.16. сведения о трудовом и общем стаже;

5.4.17. сведения о предыдущих местах работы;

5.4.18. данные сведений о трудовой деятельности;

5.4.19. сведения о заработной плате сотрудника (оклад, премии, надбавки);

5.4.20. номера банковских карт и расчетных счетов;

5.4.21. сведения о социальных льготах;

5.4.22. контактные данные (номер домашнего и/или мобильного телефона, адрес электронной почты);

5.4.23. сведения о социальных льготах;

5.4.24. специальность;

5.4.25. занимаемая должность;

5.4.26. данные трудового договора и соглашений к нему;
5.4.27. данные личной карточки по формам Т-1 и Т-2;
5.4.28. содержание декларации, подаваемой в налоговую инспекцию;
5.4.29. подлинники и копии приказов по личному составу;
5.4.30. личные дела и трудовые книжки сотрудников;
5.4.31. основания к приказам по личному составу;
5.4.32. дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
5.4.33. копии отчетов, направляемые в органы статистики, копии других отчетов;
5.4.34. результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
5.4.35. рекомендации, характеристики, благодарственные письма, грамоты и т.п.;
5.4.36. фотографии.
5.4.37. Указанные в п. 5.4. сведения являются конфиденциальными и не подлежат разглашению иначе как по основаниям, предусмотренным законодательством РФ.
5.4.38. Персональные данные работников содержатся в их личных делах, картотеках и базах данных кадровых информационных систем.
5.4.39. Персональные данные родственников работников содержатся в личных делах и базах данных кадровых информационных систем.

## 6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. **Основные принципы обработки, передачи и хранения персональных данных:**

6.1.1. Обработка персональных данных осуществляется на законной и справедливой основе.
6.1.2. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 и условий обработки персональных данных, указанных в ст. 6 Федерального закона 152-ФЗ «О персональных данных».
6.1.3. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность), за исключением цифрового фотографического изображения лица, используемого для обеспечения однократного и/или многократного прохода на территорию Оператора. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.
6.1.4. Оператор не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных частями 2 и 2_1 ст. 10 152 – ФЗ.
6.1.5. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.
6.1.6. Обработка персональных данных осуществляется с использованием средств автоматизации и без использования таких средств (на бумажном носителе информации).

6.1.7. Оператор не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

6.1.8. По мотивированному запросу, исключительно для выполнения возложенных законодательством функций и полномочий, персональные данные субъекта без его согласия могут быть переданы:

1) в судебные органы в связи с осуществлением правосудия;

2) в органы федеральной службы безопасности;

3) в органы прокуратуры;

4) в органы полиции;

5) в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

6.1.8. Оператор не поручает обработку персональных данных другим лицам на основании договора.

6.2. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

6.3. **Создание персональных данных работника.**

6.3.1. Документы, содержащие персональные данные работника, создаются путем:

– копирования оригиналов (документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

– внесения сведений в учетные формы (на бумажных и электронных носителях);

– получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, медицинское заключение).

6.4. **Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.**

6.4.1. Согласие субъекта персональных данных на обработку его персональных данных.

6.4.1.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

6.4.1.2. Если в соответствии с федеральным законом предоставление персональных данных и (или) получение оператором согласия на обработку персональных данных являются обязательными, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.4.1.3. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

6.4.1.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2-11 части 1 ст. 6, части 2 статьи 10 и части 2 ст. 11 152 – ФЗ.

6.4.1.5. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

6.4.1.6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

6.4.1.7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

6.4.1.8. Форма согласия субъекта на обработку персональных данных представлена в приложении № 4 к настоящей Политике.

6.4.1.9. Согласие субъекта на обработку персональных данных действует с даты подписания согласия в течение всего срока действия трудового договора и до достижения цели обработки персональных данных, либо до отзыва субъектом согласия на обработку персональных данных.

6.4.2. Обработка персональных данных субъекта персональных данных.

6.4.2.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных (ст. 6 152-ФЗ).

6.4.2.2. Обработка персональных данных должна осуществляться с соблюдением условий, предусмотренных 152 – ФЗ (статья 6).

6.4.2.3. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

6.4.2.4. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных 152 – ФЗ (ст. 10_1).

6.4.2.5. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов (ст. 86 ТК РФ).

6.4.2.6. Обработка персональных данных соискателей ведется исключительно в целях определения возможности их трудоустройства.

6.4.2.7. Обработка персональных данных работника осуществляется исключительно в целях (ст. 86 ТК РФ):

– обеспечения соблюдения законов и иных нормативных правовых актов;

– содействия работникам в трудоустройстве;
– обеспечения личной безопасности работников;
– получении образования и продвижении по службе;
– контроля количества и качества выполняемой работы;
– обеспечения сохранности имущества работника и работодателя.

6.4.2.8. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы N Т-1 и Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях.

6.4.3. Получение персональных данных.

6.4.3.1. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны (приложение 5).

6.4.3.2. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия (ст. 86 ТК РФ).

В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:
– о целях получения персональных данных;
– о предполагаемых источниках и способах получения персональных данных;
– о характере подлежащих получению персональных данных;
– о последствиях отказа работника дать письменное согласие на их получение.

6.4.3.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом (ст. 86 ТК РФ).

6.4.3.4. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения (ст. 86 ТК РФ).

6.4.4. Передача персональных данных.

6.4.4.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

6.4.4.2. Работники ГБОУ ДО РК «ЦДЮТК», имеющие доступ к персональным данным соискателей, работников и родственников работников, при передаче этих данных должны соблюдать следующие требования (ст. 88 ТК РФ):
– не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается;
– разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей;
– не передавать и не распространять персональные данные без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо:
  – для предупреждения угрозы жизни и здоровью субъекта персональных данных, если получить такое согласие невозможно;
  – для статистических и исследовательских целей (при обезличивании);
  – в случаях, напрямую предусмотренных федеральными законами.
– передавать без согласия субъекта персональных данных информацию в государственные и негосударственные функциональные структуры, в том числе в

налоговые инспекции, фонды медицинского и социального страхования, пенсионный фонд, правоохранительные органы, страховые агентства, военкоматы, медицинские организации, контрольно-надзорные органы при наличии оснований, предусмотренных в федеральных законах, или запроса от данных структур со ссылкой на нормативное правовое основание для предоставления такой информации.

– размещать в целях обеспечения информационной открытости ГБОУ ДО РК «ЦДЮТК» на официальном сайте ГБОУ ДО РК «ЦДЮТК» в информационно-телекоммуникационной сети Интернет:

– Информацию о директоре. его заместителях, руководителях филиалов и структурных подразделений, в том числе:

- фамилию, имя, отчество (при наличии);
- должность;
- контактные рабочие телефоны;
- адрес электронной почты.

– Информацию о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы, в том числе:

- фамилию, имя, отчество (при наличии);
- должность (должности);
- преподаваемые дисциплины;
- ученую степень (при наличии);
- ученое звание (при наличии);
- информацию о педагогической деятельности;
- наименование направления подготовки и (или) специальности;
- данные о повышении квалификации и (или) профессиональной переподготовке (при наличии);
- общий стаж работы;
- стаж работы по специальности.

6.4.5. Лица, которые получают персональные данные, должны быть предупреждены о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Директор ГБОУ ДО РК «ЦДЮТК» и уполномоченные им лица вправе требовать подтверждения исполнения этого правила.

6.4.6. Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

6.4.7. <u>Хранение персональных данных.</u>

6.4.7.1. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

6.4.7.2. Порядок хранения и использования персональных данных работников устанавливается работодателем с соблюдением требований Трудового Кодекса и иных федеральных законов (ст. 87 ТК РФ).

6.4.7.3. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.4.7.4. Хранение персональных данных:

– личные дела в бумажном виде в папках хранятся в специально отведенном месте, доступ к которому имеет только специалист по кадрам;
– трудовые и медицинские книжки работников хранятся в бумажном виде в ГБОУ ДО РК «ЦДЮТК» в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа;
– персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК специалиста по кадрам;
– документы воинского учета, карточка формы N Т-1 и Т-2 хранятся в запертом шкафу или металлическом сейфе.

6.4.7.5. Документы, содержащие персональные данные работников и родственников работников, подлежат хранению и уничтожению в сроки и в порядке, предусмотренные номенклатурой дел и архивным законодательством Российской Федерации.

6.4.8. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения. Обработка персональных данных, разрешенных субъектом персональных данных для распространения осуществляется в соответствии с нормами, закрепленными статьями 152-ФЗ:
– согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обеспечивает субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
– в случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных согласился с распространением персональных данных, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без права распространения;
– в случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные ч. 9 ст. 10.1 152-ФЗ, или если в предоставленном субъектом персональных данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с ч. 9 т. 10.1 152-ФЗ, такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц;
– молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения;
– в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий, предусмотренных настоящей статьей, не допускается;

– установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных субъектом персональных данных для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации;

– передача (распространение, предоставление, доступ) персональных данных, разрешенных субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования.

## 7. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ, БЛОКИРОВАНИЕ, ОБЕЗЛИЧИВАНИЕ, УДАЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ НА ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7.2. Работники вправе требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса или иного федерального закона.

7.3. Персональные данные оценочного характера работник вправе дополнить заявлением, выражающем его собственную точку зрения.

7.4. По требованию работника работодатель обязан известить всех лиц, которым ранее были сообщены неверные или неполные персональные данные этого работника, обо всех произведенных в них исключениях, исправлениях и дополнениях.

7.5. <u>Доступ к персональным данным. Запрос на доступ к персональным данным.</u>

7.5.1. Право доступа к персональным данным субъектов имеют работники ГБОУ ДО РК «ЦДЮТК», входящие в перечень лиц, осуществляющих обработку персональных данных, определенный приказом директора.

7.5.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

7.5.3. Работники ГБОУ ДО РК «ЦДЮТК», получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).

7.5.4. Субъект может получить доступ к своим персональным данным на основании письменного запроса или при обращении, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

7.5.5. ГБОУ ДО РК «ЦДЮТК» предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

7.5.6. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.5.7. Внутренний доступ (доступ внутри ГБОУ ДО РК «ЦДЮТК»).

7.5.7.1. Доступ к персональным данным соискателя имеют:

– директор в полном объеме;
– специалист по кадрам в полном объеме.

7.5.7.2. Право доступа к персональным данным работников имеют:

– директор в полном объеме;
– специалист по кадрам в полном объеме;
– заместители директора в пределах, необходимых для исполнения их трудовых обязанностей;
– главный бухгалтер в полном объеме;
– бухгалтер в полном объеме;
– специалист по охране труда, в пределах, необходимых для исполнения его трудовых обязанностей;
– юрисконсульт, в пределах, необходимых для исполнения его трудовых обязанностей;
– сам работник, носитель данных;
– другие сотрудники ГБОУ ДО РК «ЦДЮТК», определяемые приказом директора при выполнении ими своих служебных обязанностей.

7.5.7.3. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора ГБОУ ДО РК «ЦДЮТК».

7.5.8. Внешний доступ.

7.5.8.1. К числу массовых потребителей персональных данных вне ГБОУ ДО РК «ЦДЮТК» можно отнести государственные и негосударственные функциональные структуры:

– налоговые инспекции;
– правоохранительные органы;
– органы статистики;
– страховые агентства;
– военкоматы;
– органы социального страхования;
– пенсионные фонды;
– Учредитель.

7.5.8.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7.5.8.3. Организации, в которые сотрудник может осуществлять перечисление денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения и т.п.), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

7.5.8.4. Другие организации.

7.5.8.5. Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

7.5.8.6. Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

7.5.8.7. В случае развода бывшая супруга (супруг) имеет право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (ТК РФ).

7.6. Порядок блокировки и разблокировки персональных данных.

7.6.1. Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

7.6.2. Блокировка персональных данных подразумевает:

7.6.2.1. Запрет редактирования персональных данных.

7.6.2.2. Запрет распространения персональных данных любыми средствами.

7.6.2.3. Запрет использования персональных данных в массовых рассылках.

7.6.2.4. Запрет открытия банковских счетов.

7.6.2.5. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота ГБОУ ДО РК «ЦДЮТК» и запрет их использования.

7.6.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

7.6.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

7.6.5. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

7.7. Порядок обезличивания и уничтожения персональных данных.

7.7.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.

7.7.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

7.7.3. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются путем стирания или замазывания.

7.7.4. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются путем стирания или замазывания.

7.7.5. Организация обязана обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

7.7.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

7.7.7. При уничтожении персональных данных субъекта работники ГБОУ ДО РК «ЦДЮТК» не могут получить доступ к персональным данным субъекта в информационных системах.

7.7.8. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

7.7.9. Операция уничтожения персональных данных необратима.

## 8. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

8.1. Защита персональных данных.

8.1.1. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий (ст. 19 152-ФЗ).

8.1.2. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

8.1.3. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и не заинтересованные в возникновении угрозы лица.

8.1.4. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности ГБОУ ДО РК «ЦДЮТК».

8.1.5. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом (ст. 86 ТК РФ).

8.2. Внутренняя защита.

8.2.1. Регламентация доступа работников к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителем и специалистами организации.

8.2.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранению тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками отделов по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места работников. Личные дела могут выдаваться на рабочие места только директору, и в исключительных случаях, по письменному разрешению директора, - заведующему отдела или заместителю директора

(например, при подготовке материалов для аттестации работника).
8.2.3. Защита персональных данных работника на электронных носителях: персональные компьютеры специалиста по кадрам, главного бухгалтера, бухгалтера и других лиц, работающих с персональными данными, должны быть защищены паролем.
8.3. Внешняя защита.
8.3.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.
8.3.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности ГБОУ ДО РК «ЦДЮТК», посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов кадровой службы.
8.3.3. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (приложение 3), а также предупреждаются о возможной дисциплинарной, административной, гражданско-правовой и уголовной ответственности в случае нарушения норм и требований действующего законодательства Российской Федерации в области обработки персональных данных.
8.3.4. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.
8.4. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:
8.4.1. Назначением ответственных за организацию обработки персональных данных.
8.4.2. Осуществлением внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.
8.4.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных.
8.4.4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
8.4.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.
8.4.6. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
8.4.7. Учетом машинных носителей персональных данных.
8.4.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих 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.
8.4.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
8.4.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.
8.4.11. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.
8.5. Оператор и иные 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 (ст. 7 152-ФЗ).
8.6. Оператор обязан 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.
8.7. Указанная в ч. 12 ст. 19 152-ФЗ информация (за исключением информации, составляющей государственную тайну) передается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, в уполномоченный орган по защите прав субъектов персональных данных.
8.8. Порядок передачи информации в соответствии с ч. 13 ст. 19 152-ФЗ устанавливается совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных.

## 9. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Субъект персональных данных имеет право (ст. 89 ТК РФ):
9.1.1. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
9.1.2. Отозвать согласие на обработку персональных данных на основании письменного заявления.
9.1.3. Требовать перечень обрабатываемых персональных данных, имеющихся в ГБОУ ДО РК «ЦДЮТК» и источник их получения.
9.1.4. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.
9.1.5. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.
9.1.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей (ст. 14 152-ФЗ):
- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут

быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

– информацию о способах исполнения оператором обязанностей, установленных ст. 18.1. 152-ФЗ;

– иные сведения, предусмотренные 152-ФЗ или другими федеральными законами.

9.1.7. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

9.1.8. Сведения, указанные в ч. 7 ст. 14 152-ФЗ, предоставляются субъекту персональных данных или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Оператор предоставляет сведения, указанные в ч. 7 ст. 14 152-ФЗ, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе

9.1.9. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

9.1.10. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

9.1.11. Другие права, предусмотренные законодательством Российской Федерации.

9.1.12. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

## 10. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. ГБОУ ДО РК «ЦДЮТК» вправе:

10.1.1. Отстаивать свои интересы в суде.

10.1.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.).

10.1.3. Отказать в предоставлении персональных данных в случаях, предусмотренных законом.

10.1.4. Использовать персональные данные субъекта без его согласия в случаях, предусмотренных законом.

10.1.5. Осуществлять внутренний контроль за соблюдением настоящего Положения.

10.2. Обязанности:

10.2.1. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети "Интернет", с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

10.2.2. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети (ст. 18_1 152-ФЗ).

10.2.3. Иные обязанности, предусмотренные федеральным законодательством.

10.2.4. Оператор в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

10.2.5. Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ и принятыми в соответствии с ним нормативными правовыми

актами, если иное не предусмотрено 152-ФЗ или другими федеральными законами. К таким мерам, в частности, относятся:

– назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

– издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

– ) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со ст. 19 152-ФЗ;

– осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

– оценка вреда, который может быть причинен субъектам персональных данных;

– ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

10.2.6. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке регламентируются ст. 19 152-ФЗ.

10.2.7. Оператор исполняет обязанности, предусмотренные 152-ФЗ при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

10.2.8. Исполняет обязанности по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.

## 11. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКА

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных соискателей и работников, в том числе бывших, и их родственников, привлекаются к дисциплинарной и материальной ответственности, а в случаях, установленных законодательством РФ, - к гражданско-правовой. административной и

уголовной ответственности в порядке, установленном федеральными законами (ст. 90 ТК РФ).

11.2. Ответственность за достоверность предоставленных персональных данных несут лица, их предоставившие.

## 12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Настоящая Политика утверждается приказом директора ГБОУ ДО РК «ЦДЮТК».

12.2. Настоящая Политика действует до принятия новой.

12.3. Настоящая Политика обязательна для соблюдения и подлежит доведению до всех сотрудников ГБОУ ДО РК «ЦДЮТК».

12.4. Контроль за соблюдением Политики осуществляет директор ГБОУ ДО РК «ЦДЮТК».

**Приложение № 1**
**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК»**
**утв. пр. № 512 от «29» декабря 2023 г.**

## Перечень персональных данных, обрабатываемых в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения»

1. Анкета.
2. Автобиография.
3. Паспортные данные.
4. Фамилия, имя, отчество (при наличии).
5. Дата рождения.
6. Место рождения.
7. Адрес места жительства (данные о прописке и фактическом месте проживания).
8. Сведения о составе семьи.
9. Сведения о воинском учете.
10. Сведения об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении учетной степени, ученого звания (если таковые имеются) и т.п.
11. Специальность.
12. Занимаемая должность.
13. Сведения о заработной плате (оклад, премии, надбавки).
14. Номера банковских карт и расчетных счетов.
15. Данные о страховом номере индивидуального лицевого счета.
16. Данные Полиса обязательного медицинского страхования.
17. Свидетельство о постановке на учет физического лица в налоговом органе.
18. Сведения о социальных льготах.
19. Информация о наличии/отсутствии судимостей и/или наличие обязательств по исполнительным листам.
20. Личные дела и трудовые книжки сотрудников.
21. Данные сведений о трудовой деятельности.
22. Трудовой и общий стаж.
23. Данные о предыдущих местах работы.
24. Данные личной карточки по формам Т-1 и Т-2.
25. Данные трудового договора и соглашений к нему.
26. Подлинники и копии приказов по личному составу.
27. Основания к приказам по личному составу.
28. Дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям.
29. Копии отчетов, направляемые в органы статистики, копии других отчетов.
30. Содержание декларации, подаваемой в налоговую инспекцию.
31. Результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей.

32. Контактные данные (номер домашнего и/или мобильного телефона, адрес электронной почты).

33. Фамилия, имя отчество (при наличии), дата рождения детей.

34. Рекомендации, характеристики, благодарственные письма, грамоты, благодарности и т.п.

35. Фотографии.

**Приложение № 2**
**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК»**
**утв. пр. № 512 от «29» декабря 2023 г.**

# ПЕРЕЧЕНЬ ОСНОВНЫХ ВИДОВ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБОУ ДО РК «ЦДЮТК»

## 1. Перечень обозначений и сокращений

1.1. АРМ - автоматизированное рабочее место;
1.2. АИС – автоматизированная информационная система;
1.3. БД – база данных;
1.4. ИБ – информационная безопасность;
1.5. ИР - информационный ресурс;
1.6. ИСПДн - информационная система персональных данных;
1.7. СЗПДн – система защиты персональных данных;
1.8. КЗ - контролируемая зона;
1.9. ПДн - персональные данные;
1.10. ПО - программное обеспечение;
1.11. ПТС - программно-технические средства;
1.12. ПЭМИН - побочные электромагнитные излучения и наводки;
1.13. СЗИ - средства защиты информации;
1.14. СКЗИ - средства криптографической защиты информации;
1.15. ФСБ - Федеральная служба безопасности;
1.16. ФСО - Федеральная служба охраны;
1.17. ФСТЭК - Федеральная служба по техническому и экспертному контролю.

## 2. Общие положения

Настоящий Перечень основных видов угроз безопасности персональных данных в информационных системах персональных данных (далее – Перечень) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в ИСПДн Государственного бюджетного образовательного учреждения дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения».

Определение нарушителей и угроз безопасности персональных данных при их обработке является одним из необходимых мероприятий по обеспечению безопасности ПДн в информационных системах.

Выявление и учет угроз безопасности ПДн в конкретных условиях составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в информационных системах ПДн.

## 3. Основные виды угроз безопасности ПДн в ИСПДн

### 3.1. Типы угроз безопасности ПДн

Угрозы безопасности ПДн классифицируются по типу используемой уязвимости ИСПДн. Выделяются следующие типы угроз:

– угрозы, связанные с наличием недокументированных (не декларированных) возможностей в системном программном обеспечении, используемом в ИСПДн (угрозы 1-го типа);
– угрозы, связанные с наличием недокументированных (не декларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн (угрозы 2-го типа);
– угрозы, не связанные с наличием недокументированных (не декларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн (угрозы 3-го типа).

3.2. **Угрозы утечки информации по техническим каналам**

При обработке ПДн в ИСПДн возможно возникновение угроз безопасности ПДн за счет реализации следующих технических каналов утечки информации:
– Угрозы утечки акустической (речевой) информации.
– Угрозы утечки видовой информации.
– Угрозы утечки информации по каналам ПЭМИН.

3.2.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:
– с помощью аппаратных закладок;
– за счет съема виброакустических сигналов;
– за счет излучений, модулированных акустическим сигналом (микрофонный эффект и ВЧ облучение);
– за счет оптического излучения, модулированного акустическим сигналом.

3.2.2. Угрозы утечки видовой информации

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно- вычислительных комплексов, технических средств обработки графической, видео - и буквенно-цифровой информации, входящих в состав ИСПДн.

Кроме этого, просмотр (регистрация) ПДн возможен с использованием специальных электронных устройств съема, внедренных в служебных помещениях или скрытно используемых физическими лицами при посещении ими служебных помещений.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:
– за счет удаленного просмотра экранов дисплеев и других средств отображения информации,
– с помощью видео аппаратных закладок.

3.2.3. Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных (не связанных с прямым функциональным значением элементов ИСПДн) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Генерация информации, содержащей ПДн и циркулирующей в технических средствах ИСПДн в виде электрических информативных сигналов, обработка и передача указанных

сигналов в электрических цепях технических средств ИСПДн сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и размеров ИСПДн.

Регистрация ПЭМИН осуществляется с целью перехвата информации, циркулирующей в технических средствах, осуществляющих обработку ПДн (средствах вычислительной техники, информационно-вычислительных комплексах и сетях, средствах и системах передачи, приема и обработки ПДн, средствах и системах звукозаписи, звукоусиления, звуковоспроизведения, переговорных и телевизионных устройствах, средствах изготовления, тиражирования документов и других технических средствах обработки речевой, графической, видео - и буквенно-цифровой информации).

Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Утечка информации по каналам ПЭМИН может быть осуществлена:

- за счет побочных электромагнитных излучений электронно- вычислительной техники;
- за счет наводок по цепям питания;
- за счет радиоизлучений, модулированных информационным сигналом.

3.3. Угрозы несанкционированного доступа

Угрозы НСД в ИСПДн с применением программных и программно- аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн, и включают в себя:

- Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн.
- Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети.
- Угрозы внедрения (в том числе по сети) вредоносных программ (программно-математического воздействия).

3.3.1. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн.

Данные угрозы могут быть реализованы нарушителем в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн. При этом можно выделить следующие угрозы:

1) Угрозы, реализуемые в ходе загрузки операционной системы.

Эти угрозы безопасности информации направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода-вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду ИСПДн. Чаще всего такие угрозы реализуются с использованием отчуждаемых носителей информации.

2) Угрозы, реализуемые после загрузки операционной среды, независимо от того, какая прикладная программа запускается пользователем.

Эти угрозы, как правило, направлены на выполнение непосредственно несанкционированного доступа к информации. При получении доступа в операционную среду нарушитель может воспользоваться как стандартными функциями операционной системы (уничтожение, копирование, перемещение, форматирование носителей информации и т.п.) или какой-либо прикладной программой общего пользования (например, системы управления базами данных), так и специально созданными для выполнения несанкционированного доступа программами, например:

- программами просмотра и модификации реестра;
- программами поиска текстов в текстовых файлах, по ключевым словам, и копирования;

– специальными программами просмотра и копирования записей в базах данных;
– программами быстрого просмотра графических файлов, их редактирования или копирования;
– программами поддержки возможностей реконфигурации программной среды (настройки ИСПДн в интересах нарушителя) и др.
– кроме того, к данным угрозам необходимо отнести угрозы утечки информации путем копирования ее на съемные носители.

3) Угрозы, реализуемые после загрузки операционной среды, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз представляет собой угрозы внедрения вредоносных программ.

3.3.2. Угрозы, связанные с реализацией протоколов сетевого взаимодействия, реализуемые внутри распределенной сети.

Можно выделить следующие угрозы, реализуемые с использованием протоколов сетевого взаимодействия, реализуемые внутри распределенной сети:

1) Угрозы «Анализа сетевого трафика».

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль, а также конфиденциальная информация.

2) Угрозы сканирования сети.

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них с целью выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбора идентификаторов и паролей пользователей.

3) Угрозы выявления паролей.

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

4) Угрозы навязывания ложного маршрута сети.

Данная угроза реализуется путем несанкционированного изменения маршрутно-адресных данных. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализация угрозы основывается на несанкционированном использовании протоколов изменений в маршрутно-адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

5) Угрозы внедрения ложного объекта сети.

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата

нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом- жертвой, будет проходить через ложный объект сети.

6) Угрозы типа «Отказ в обслуживании».

Эти угрозы основаны на недостатках сетевого программного обеспечения, Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Может быть выделено несколько разновидностей таких угроз:

– скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо- запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;

– явный отказ в обслуживании, вызванный полным исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN- flooding), шторм сообщений почтовому серверу (Spam); явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации; явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «Tear Drop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, какое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

7) Угрозы удаленного запуска приложений.

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы:

– программы-закладки;
– вирусы;
– «сетевые шпионы» и т.д.

Основная цель внедренных вредоносных программ – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данной угрозы:

а) распространение файлов, содержащих несанкционированный исполняемый код. Типовые угрозы этого подкласса основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в виде макрокоманд (документы Microsoft Word, Excel и т.п.); html-документы, содержащие исполняемый код в виде элементов ActiveX, Java-апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы;

б) удаленный запуск приложения путем переполнения буфера приложений-серверов. При угрозах этого подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса»;

в) удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами. При угрозах этого подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа BackOrifice, NetBus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

3.3.3. Угрозы внедрения по сети вредоносных программ (программно- математического воздействия).

Программно-математическое воздействие -это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;
– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
– разрушать (искажать произвольным образом) код программ в оперативной памяти;
– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИСПДн, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИСПДн с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИСПДн.

Вредоносные программы основаны на использовании уязвимостей различного рода программного обеспечения и разнообразных сетевых технологий, обладают широким спектром возможностей и могут действовать во всех видах программного обеспечения.
Наличие в ИСПДн вредоносных программ может способствовать возникновению скрытых, в том числе нетрадиционных каналов доступа к информации, позволяющих вскрывать, обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную защиту.

### 3.4. Источники угроз безопасности ПДн

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Источниками угроз НСД в ИСПДн могут быть:

- нарушитель;
- носитель вредоносной программы;
- аппаратная закладка.

## 4. Модель нарушителя

В настоящем разделе определяется совокупность условий и факторов, создающих опасность нарушения характеристик безопасности возможных объектов угроз.

В данном разделе под угрозами будут пониматься атаки.

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

Внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

Внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

### 4.1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

### 4.2. Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, не составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

К **внутренним нарушителям** могут относиться:

- администратор безопасности ИСПДн (категория I);
- администраторы конкретных подсистем или баз данных ИСПДн (категория II);
- пользователи ИСПДн (категория III);
- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал (водитель, уборщик помещений и т.п.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

На лиц категорий I-II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

К лицам категорий I-II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I-II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- общая информация – информации о назначении и общих характеристиках ИСПДн;

– эксплуатационная информация – информация, полученная из эксплуатационной документации;
– чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:
– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
– сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
– данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
– данные о реализованных в программных средствах защиты информации принципах и алгоритмах;
– исходные тексты программного обеспечения ИСПДн;
– сведения о возможных каналах реализации угроз;
– информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в автоматизированной информационной системе (АИС), к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об АИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в АИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией о ИСПДн и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными о ИСПДн являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности, предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз:
– аппаратные компоненты средства защиты ПДн (СЗПДн);
– доступные в свободной продаже технические средства и программное обеспечение;
– специально разработанные технические средства и программное обеспечение.

**Приложение № 3**

**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК» утв. пр. № 512 от «29» декабря 2023 г.**

Обязательство

о неразглашении персональных данных работников

Я, _____

_____,

(Ф.И.О., должность)

паспорт _____ выдан _____

серии, номер

_____,

кем, когда, код подразделения

предупрежден (а), что на период исполнения должностных обязанностей мне будет предоставлен доступ к персональным данным работников.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными работников соблюдать все описанные в Политике в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения» требования.

В случае моего увольнения, все носители, содержащие персональные данные (документы, копии документов, дискеты, диски, магнитные ленты, распечатки на принтерах, черновики, кино- и фотонегативы, позитивы и пр.), которые находились в моем распоряжении в связи с выполнением мною трудовых обязанностей во время работы у работодателя, передать ответственному за обеспечение безопасности персональных данных или другому работнику по указанию директора учреждения.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудников, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.

С Политикой в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения» и гарантиями их защиты ознакомлен(а).

Дата: «_____» _____ 20___ г. Подпись: _____ _____

**Приложение № 4**
**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК»**
**утв. пр. № 512 от «29» декабря 2023 г г.**

# СОГЛАСИЕ
# НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ
**работника**

Я, _____,
*(Ф.И.О.)*

_____
*(должность)*

Проживающий по адресу: _____
Паспорт: №_____, выданный: _____

_____
*(кем и когда)*

настоящим даю свое согласие на обработку в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения», расположенного по адресу: 295011, город Симферополь, ул. Крылова, д. 60, ИНН 9102057796, КПП 910201001 моих персональных данных, к которым относятся:

- паспортные данные;
- данные о страховом номере индивидуального лицевого счета;
- свидетельство о постановке на учет физического лица в налоговом органе;
- данные документа воинского учета;
- документы об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются);
- анкетные данные, предоставленные мною при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- данные иных документов, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены мною при заключении трудового договора или в период его действия;
- данные трудового договора и соглашений к нему;
- данные кадровых приказов о моем приеме, переводах, увольнении;
- данные личной карточки по формам Т-2 и Т-1;
- данные документов о прохождении мной аттестации, собеседования, повышения квалификации, результатов оценки и обучения;
- фотография;
- иные сведения обо мне, которые необходимы Работодателю для корректного документального оформления правоотношений между мною и Работодателем.

Я даю согласие на использование моих персональных данных в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- корректного документального оформления трудовых правоотношений между мною и Работодателем;
- обеспечения выполнения мною должностных обязанностей (трудовой функции);
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством;
- предоставления информации в медицинские учреждения, страховые компании;
- обеспечения предоставления мне социального пакета.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством Российской Федерации.

Работодатель гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством Российской Федерации и Политикой в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения», с которым я ознакомлен (а) при трудоустройстве в учреждение.

Данное Согласие на обработку персональных данных действует с момента заключения мною Трудового договора с Работодателем и до истечения сроков, установленных действующим законодательством Российской Федерации, в течение всего срока действия трудового договора и до достижения цели обработки персональных данных, либо до отзыва согласия на обработку персональных данных.

Я ознакомлен(а), что согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: «_____» _____ 20___ г. Подпись: _____ _____

**Приложение № 5**
**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК»**
**утв. пр. № 512 от «29» декабря 2023 г г.**

## Согласие
## субъекта на получение его персональных данных у третьей стороны

Я, _____,
*(Ф.И.О.)*

Проживающий по адресу: _____

_____

Паспорт: №_____, выданный: _____

_____

в соответствии со ст. 86 Трудового Кодекса Российской Федерации _____ на
*(согласен/не согласен)*

получение моих персональных данных:
а именно: _____

_____

_____

*(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.)*

для обработки в целях _____

_____

_____,

*(указать цели обработки)*

у следующих лиц _____

_____

_____

*(указать Ф.И.О. физического лица или наименование организации)*

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

Я ознакомлен(а), что данное согласие может быть отозвано мной на основании письменного заявления в произвольной форме.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: «_____» _____ 20___ г. Подпись: _____ _____

**Приложение № 6**
**к Политике в области обработки и защиты персональных данных в ГБОУ ДО РК «ЦДЮТК»**
**утв. пр. № 512 от «29» декабря 2023 г.**

# СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ПЕРСОНАЛЬНЫХ ДАННЫХ ДЛЯ РАСПРОСТРАНЕНИЯ

Я, _____,
*(Ф.И.О.)*

_____
*(должность)*

Проживающий по адресу: _____
Паспорт: №_____, выданный: _____
_____
*(кем и когда)*

Номер телефона: _____,
Адрес электронной почты: _____

руководствуясь ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» настоящим даю свое согласие на распространение Государственным бюджетным образовательным учреждением дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения» (далее – Оператор), расположенного по адресу: 295011, город Симферополь, ул. Крылова, д. 60 (ИНН 9102057796, КПП 910201001, ОКВЭД 85.41, ОКПО 00772524, ОКОГУ 2300223, ОКОПФ 75203, ОКФС 13) моих персональных данных, к которым относятся:

| Категория персональных данных | Перечень персональных данных | Разрешаю к распространению неограниченному кругу лиц (да/нет) | Условия и запреты | Дополнительные условия |
|---|---|---|---|---|
| Общие персональные данные | фамилия | да | | |
| | имя | да | | |
| | отчество (при наличии) | да | | |
| | год рождения | нет | | |
| | месяц рождения | да | | |
| | дата рождения | да | | |
| | место рождения | **нет** | | |
| | адрес | **нет** | | |
| | семейное положение | **нет** | | |
| | должность (должности) | да | | |
| | образование, уровень образования | да | | |

| | | | | |
|---|---|---|---|---|
| | наименование направления подготовки и (или) специальности | да | | |
| | ученая степень (при наличии) | да | | |
| | ученое звание (при наличии) | да | | |
| | профессия | да | | |
| | повышение квалификации и (или) профессиональная переподготовка | да | | |
| | общий стаж работы | да | | |
| | стаж работы по специальности | да | | |
| | преподаваемые учебные предметы, курсы, дисциплины (модули) | да | | |
| | информация о награждениях, благодарностях, грамотах, званиях | да | | |
| Биометрические персональные данные | цветное цифровое фотографическое изображение полностью или фрагментарно | да | | |
| | материалы видеосъемок, видеозаписи (видеоматериалы созданные в период проведения мероприятий ГБОУ ДО РК «ЦДЮТК») | да | | |
| | материалы видеосъемок, видеозаписи, предоставленные мной | да | | |

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

| Адрес информационного ресурса | Наименование информационного ресурса | Действия с персональными данными |
|---|---|---|
| http://crimuntur.ru | Официальный сайт Оператора в информационно-телекоммуникационной сети «Интернет» | Предоставление сведений неограниченному кругу лиц |
| https://www.youtube.com/channel/UCX37Qy9TeaoNIC_j47BVTbw/featured | Видеоканал Оператора в видеохостинге Ютуб в информационно-телекоммуникационной сети «Интернет» | Предоставление сведений неограниченному кругу лиц |
| https://www.instagram.com/accounts/login/?next=/cdutk/ | Официальная страница Оператора в социальной сети Инстаграм в информационно-телекоммуникационной сети «Интернет» | Предоставление сведений неограниченному кругу лиц |
| https://vk.com/crimuntur | Официальная страница Оператора в социальной сети ВКонтакте в информационно-телекоммуникационной сети «Интернет» | Предоставление сведений неограниченному кругу лиц |
| http://crimuntur.ru<br>Печатные материалы (сборники, буклеты, книги и т.п.) | Методический сборник (методические материалы) | Предоставление сведений неограниченному кругу лиц |

Я даю согласие на распространение моих персональных данных в целях:

– обеспечения соблюдения требований статьи 29 Федерального закона от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации», постановления Правительства Российской Федерации от 10.07.2013 г. № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации», приказа Федеральной службы по надзору в сфере образования и науки от

14.08.2020 г. № 831 «Об утверждении Требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления информации», иных законов и нормативных правовых актов;

– формирования открытых и общедоступных информационных ресурсов, содержащих информацию о деятельности Оператора в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети «Интернет»;

– осуществления обработки персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законодательством.

Оператор гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством Российской Федерации и Политикой в области обработки и защиты персональных данных в Государственном бюджетном образовательном учреждении дополнительного образования Республики Крым «Центр детско-юношеского туризма и краеведения», с которым я ознакомлен (а) при трудоустройстве в учреждение.

Данное Согласие на обработку персональных данных действует с момента его подписания мной: с «_____» _____ 20___г. по «_____» _____ 20____г, либо до отзыва согласия на обработку персональных данных.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

Я ознакомлен(а), что согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: «_____» _____ 20___ г. Подпись: _____ _____