

БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ
ВОЛОГОДСКОЙ ОБЛАСТИ
«СОЦИАЛЬНО-РЕАБИЛИТАЦИОННЫЙ ЦЕНТР ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ
«РОСТОК» ГОРОДА ЧЕРЕПОВЦА»

П Р И К А З

от 12.09.2024 № 421 /01-17

О совершенствовании деятельности
по защите персональных данных

В целях совершенствования деятельности по защите персональных данных сотрудников и получателей услуг БУ СО ВО «Социально-реабилитационного центра для несовершеннолетних «Росток» города Череповца» (далее – учреждение) во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,

ПРИКАЗЫВАЮ:

1. Утвердить в новой редакции:

1.1. Политику обработки и защиты персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 1);

1.2. Положение об обработке и защите персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 2);

1.3. Перечень информационных систем персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 3);

1.4. Правила работы с обезличенными персональными данными в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 4);

1.5. Положение об обеспечении сохранности конфиденциальной информации и персональных данных в служебных помещениях бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 5);

1.6. Порядок доступа работников учреждения, посетителей в помещения бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», в которых ведется обработка персональных данных», прилагается (приложение № 6);

1.7. Правила рассмотрения запросов субъектов персональных данных или их представителей на получение информации, касающейся обработки его персональных данных, обращений уполномоченного органа по защите прав субъектов персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 7);

1.8. Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 8).

1.9. Руководство по порядку использования и организации работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 9).

1.10. Инструкцию пользователя информационных систем персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 10).

1.11. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 11);

1.12. Порядок обработки персональных данных без использования средств автоматизации в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 12).

1.13. Политику конфиденциальности персональных данных официального сайта бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 13).

1.14. Положение об антивирусной защите в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (приложение № 14).

1.15. Модель угроз безопасности персональных данных информационных систем персональных данных бюджетного учреждения социального обслуживания

Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», прилагается (Приложение 15).

2. Признать утратившими силу приказы учреждения:

- от 20.07.2016 № 509/01-17 «О совершенствовании деятельности по защите персональных данных»;

- от 09.10.2017 № 655/01-17 «Об утверждении правил оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных»;

- от 09.10.2017 № 656/01-17 «О внесении изменений и утверждении Положения»;

- от 09.10.2017 № 657/01-17 «О назначении ответственного за организацию защиты персональных данных и утверждение обязанностей администратора ИСПДн»;

- от 23.11.2017 № 730/01-17 «О приведении в соответствие отдельных положений учреждения».

3. Заведующему отделением консультативной и методической помощи (Курнышева О.А.) организовать размещение настоящего приказа на официальном сайте учреждения в течение 10 дней со дня его подписания.

4. Заведующему канцелярией (Цветкова И.К.) ознакомить с настоящим приказом заместителей директора, заведующих отделениями под подпись не позднее 3-х рабочих дней от даты его подписания.

5. Заместителям директора, заведующим отделениями ознакомить с настоящим приказом сотрудников, находящихся в непосредственном подчинении, под подпись в срок до 30.09.2024. Листы ознакомления передать на хранение заведующему канцелярией.

6. Специалисту по персоналу (Гульнева Т.А.) включить настоящий приказ в перечень локальных нормативных актов учреждения, подлежащих ознакомлению вновь принятыми сотрудниками учреждения.

7. Контроль за исполнением приказа оставляю за собой.

Директор

Е.Ю. Каневская

ПОЛИТИКА
обработки и защиты персональных данных
в бюджетном учреждении социального обслуживания
Вологодской области «Социально-реабилитационный центр для
несовершеннолетних «Росток» города Череповца»
(новая редакция)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика обработки и защиты персональных данных (далее – Политика) в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – Учреждение, Оператор) разработана во исполнение требований ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Учреждение осуществляет обработку персональных данных, в том числе: Конституция Российской Федерации; Трудовой кодекс Российской Федерации, согласие субъектов персональных данных на обработку их персональных данных и иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Учреждения.

1.3. Понятия, связанные с обработкой персональных данных, используются в том значении, в котором они приведены в Законе о персональных данных»:

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

Персональные данные, разрешенные субъектом персональных данных для распространения – это 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.

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.

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 (предоставление, доступ);
- распространение;
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

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

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

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

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

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

Защита персональных данных – деятельность, направленная на предотвращение утечки защищаемых персональных данных, несанкционированных и непреднамеренных воздействий на защищаемые персональные данные.

1.4. Действие настоящей Политики распространяется на персональные данные, обрабатываемые в Учреждении с применением автоматизированной и неавтоматизированной обработки персональных данных.

1.5. При сборе персональных данных, в том числе посредством информационно телекоммуникационной сети интернет, Учреждение обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

2. ПРИНЦИПЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных в Учреждении осуществляется на основе принципов законности и справедливости и ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Персональные данные, цели обработки которых несовместимы между собой, обрабатываются Учреждением в различных базах данных, содержание и объем персональных данных которых соответствует заявленным целям обработки.

2.3. 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. Должностные лица Учреждения должны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

2.4. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению или обезличиванию по достижению целей обработки, если иное не предусмотрено действующим законодательством.

2.5. Сотрудники Учреждения 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 законодательством Российской Федерации.

2.6. Обработке в Учреждении подлежат только те персональные данные, которые отвечают нижеследующим целям обработки:

- обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;
- обеспечение соблюдения законодательства в области социального обслуживания;
- осуществление деятельности в соответствии с Уставом Учреждения, в том числе в целях противодействия коррупции;
- ведения кадровой работы;
- бухгалтерского учета;
- статистическим целям;
- исполнение договоров, стороной которого является субъект персональных данных;
- осуществление пропускного режима.

3. КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ, СРОКИ ИХ ОБРАБОТКИ, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ

3.1. К категориям субъектов, персональные данные которых обрабатываются в Учреждении, относятся:

- сотрудники – физические лица, состоящие в трудовых отношениях с Учреждением;
- граждане, осуществляющие деятельность в пользу Учреждения на основании договоров гражданско-правового характера (ГПХ);
- получатели социальных услуг, предоставляемых Учреждением;

- граждане, обратившиеся в Учреждение с обращением (жалоба, предложение, заявление) по вопросам, относящимся к компетенции Учреждения;
- иные физические лица, персональные данные которых предоставлены в Учреждение в рамках исполнения им своих полномочий.

3.2. Документы, содержащие персональные данные обрабатываются в сроки, обусловленные заявленными целями их обработки.

3.3. Использование персональных данных осуществляется с момента их получения оператором и прекращается:

- по достижению целей обработки персональных данных;
- в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных.

3.4. Хранение персональных данных осуществляется 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.

Персональные данные на бумажных носителях хранятся в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в Российской Федерации.

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

3.5. Уничтожение документов (носителей), содержащих персональные данные, может производиться путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

3.6. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.7. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей.

4. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании законодательства;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен законодательством;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных законодательством;

- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных.

4.2. Право субъекта персональных данных на доступ к его персональным данным ограничивается в соответствии с частью 8 статьи 14 Закона о персональных данных.

4.3. Субъект персональных данных вправе требовать от Учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.4. Сведения, указанные в пункте 4.1. раздела 4 Политики, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4.5. Если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных, или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Учреждения в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

4.6. 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.

4.7. Субъект персональных данных обязан:

- передавать Учреждению достоверные, документированные персональные данные, состав которых установлен законодательством;
- своевременно сообщать сотрудникам Учреждения, уполномоченным на получение, обработку, хранение, передачу и любое другое использование персональных данных, об изменении своих персональных данных.

5. ПРАВА И ОБЯЗАННОСТИ СОТРУДНИКОВ УЧРЕЖДЕНИЯ, УПОЛНОМОЧЕННЫХ НА ПОЛУЧЕНИЕ, ОБРАБОТКУ, ХРАНЕНИЕ, ПЕРЕДАЧУ И ЛЮБОЕ ДРУГОЕ ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Сотрудники учреждения, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных обязаны:

- знать и выполнять требования законодательства в области обеспечения защиты персональных данных;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

5.2. При обработке персональных данных сотрудникам Учреждения, уполномоченным на получение, обработку, хранение, передачу и любое другое использование персональных данных запрещается:

- использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях – при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

- передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации.

5.3. Сотрудники Учреждения, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных имеют право:

- предоставлять персональные данные третьим лицам при наличии согласия на это субъекта персональных данных, а также в других случаях предусмотренных действующим законодательством, в том числе передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Социальный фонд и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

- продолжать обработку персональных данных после отзыва согласия субъектом персональных данных в случаях, предусмотренных законодательством;

- мотивированно отказать субъекту персональных данных (его представителю) в удовлетворении запроса о предоставлении информации, касающейся обработки персональных данных субъекта, при наличии оснований, предусмотренных законодательством Российской Федерации.

5.4. Виновные в нарушении требований законодательства в области защиты персональных данных, в том числе допустившие разглашение персональных данных сотрудники Учреждения, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных, несут персональную гражданскую, уголовную, административную, дисциплинарную ответственность, предусмотренную законодательством.

6. МЕРЫ, ПРИНИМАЕМЫЕ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учреждение 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 принимает следующие меры:

- назначение лиц, ответственных за организацию обработки персональных данных в Учреждении;

- издание настоящей Политики, а также разработки иной документации с учетом требований законодательства в области защиты персональных данных;

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения законодательства в области защиты информации;

- разграничение доступа сотрудников к информации;

- установление индивидуальных паролей доступа сотрудников к информации содержащей персональные данные субъектов персональных данных, в соответствии с их должностными обязанностями;
- учет съемных машинных носителей информации;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных и уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;
- ограничение доступа в помещения, где размещены технические средства, осуществляющие обработку персональных данных, а также где хранятся носители информации;
- соблюдение сотрудниками, допущенных к обработке персональных данных субъектов, требований, установленных законодательством Российской Федерации в области персональных данных и локальными нормативными актами Учреждения, Департамента социальной защиты населения Вологодской области;
- системное обучение и проверка знаний в области защиты информации, содержащей персональные данные;
- дает ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.

7. ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Подтверждение факта обработки персональных данных Учреждением, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Учреждением субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

7.2. В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

7.3. 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 Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением;

подпись субъекта персональных данных или его представителя.

7.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.5. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

8. ИСПОЛЬЗОВАНИЕ ФАЙЛОВ cookie

8.1. Посещая сайт Оператора, Пользователь дает согласие Оператору на обработку файлов cookie с использованием метрических сервисов Google Analytics (Гугл Аналитике), Google Adwords (Гугл Адвордс), Yandex Metrika (Яндекс Метрика), Yandex.Direct (Яндекс.Директ), аналитическая система «Спутник» для анализа использования, измерения и повышение уровня производительности сайта Оператора.

8.2. Виды cookies:

- обязательные - необходимы в процессе пользования сайтом, без них сайт, или часть функционала окажутся неработоспособными. Например, локализация языка сайта;

- функциональные - позволяют настраивать сайт под Пользователя. Например, «запоминают» использование версии для слабовидящих;

- аналитические - позволяют собирать информацию о том, как используется сайт. Например, какие страницы просматриваются чаще остальных, статистика посещаемости.

8.3. Обработка файлов cookie Оператором осуществляется в обобщенном виде и никогда не соотносится с персональными данными (личными сведениями) Пользователей.

8.4. В случае отказа от обработки файлов cookie Пользователю необходимо прекратить использование сайта Оператора или отключить использование файлов cookie в настройках браузера, при этом некоторые функции сайта Оператора могут стать недоступны.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Во исполнение части 2 статьи 18.1 Закона о персональных данных настоящая Политика публикуется на официальном сайте Учреждения.

9.2. Настоящая Политика вступает в силу с момента утверждения и действует бессрочно до принятия новой Политики.

9.3. Все изменения и дополнения к настоящей Политике, утверждаются приказом Учреждения.

9.4. Иные локальные нормативные акты Учреждения должны издаваться в соответствии с настоящей Политикой и действующим законодательством в области персональных данных.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных
в бюджетном учреждении социального обслуживания
Вологодской области «Социально-реабилитационный центр для
несовершеннолетних «Росток» города Череповца» (далее – Положение)
(новая редакция)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ, Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Уставом бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее - учреждение) и другими нормативными правовыми актами.

1.2. Настоящее Положение определяет порядок работы и устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников (работников) учреждения и гарантии конфиденциальности сведений, предоставляемых гражданами в учреждение.

1.3. Персональные данные являются конфиденциальной информацией.

1.4. Порядок ввода в действие и изменения Положения.

1.4.1. Настоящее Положение вступает в силу с момента его утверждения директором учреждения и действует бессрочно, до утверждения новой редакции Положения.

1.4.2. Все изменения в Положение вносятся приказом учреждения.

1.5. Все сотрудники учреждения должны быть ознакомлены с настоящим Положением под подпись.

1.6. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75 лет (до 2003 года) и 50 лет (после 2003 года) срока их хранения, или продлевается на основании заключения экспертной комиссии учреждения, если иное не определено законом.

2. ОСНОВНЫЕ ПОНЯТИЯ И ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В настоящем Положении используются понятия, применяемые в значениях, определенных в Федеральном законе от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

2.2. В учреждении обрабатываются следующие персональные данные:

2.2.1. Персональные данные получателей социальных услуг, физических лиц, в связи с рассмотрением обращений:

– фамилия, имя, отчество (данные о смене фамилии, имени, отчества);

- статус представителя получателя социальных услуг (фамилия, имя, отчество);
- день, месяц, год рождения;
- данные о гражданстве (в т.ч. измененное - прежнее гражданство, наличие другого гражданства);
- место регистрации и место фактического проживания, номер домашнего/мобильного телефона;
- данные паспорта, свидетельства о рождении;
- данные о регистрации брака, рождении детей; образовании;
- сведения о близких родственниках (ФИО, степень родства, дата рождения, адрес проживания);
- сведения о судимости/отсутствии судимости;
- сведения о трудовой/учебной деятельности;
- данные документов воинского учета;
- данные страхового свидетельства обязательного пенсионного страхования;
- данные свидетельства о постановке физического лица на учет в налоговом органе по месту жительства на территории Российской Федерации;
- данные полиса обязательного медицинского страхования;
- фотографии (для несовершеннолетних, находящихся на стационарном обслуживании);
- биометрические данные (в связи с использованием в учреждении видеокамер).

2.2.2. Персональные данные сотрудников:

- фамилия, имя, отчество (данные о смене фамилии, имени, отчества);
- день, месяц, год рождения;
- данные о гражданстве (в т.ч. измененное – когда и по какой причине, прежнее гражданство, наличие другого гражданства);
- данные об образовании (название окончанных учебных заведений и год окончания, специальность и квалификация, наличие ученых степеней, данные о прохождении дополнительного профессионального образования);
- сведения о периодах трудовой деятельности, стаже;
- данные документов воинского учета;
- данные о регистрации брака, рождении детей;
- место регистрации и место фактического проживания, номер домашнего/мобильного телефона;
- данные паспорта гражданина Российской Федерации;
- данные страхового свидетельства обязательного пенсионного страхования;
- данные свидетельства о постановке физического лица на учет в налоговом органе по месту жительства на территории Российской Федерации;
- данные полиса обязательного медицинского страхования;
- анкетные и биографические данные;
- биометрические данные (фотография);
- сведения об отсутствии судимости;
- заключение медицинского учреждения об отсутствии заболевания, препятствующего поступлению на работу в учреждение;
- сведения о занимаемой должности и выполняемой работе по должности, основания назначения (перевода);
- содержание трудового договора;

- сведения об условиях оплаты труда по занимаемой должности;
- сведения о прохождении аттестации, датах прохождения, принятых аттестационными комиссиями решениях и о вынесенных рекомендациях;
- сведения о прохождении служебных проверок и наложении дисциплинарных взысканий;
- сведения о награждении государственными, ведомственными и иными наградами;
- данные о направлении в отпуска и служебные командировки.

Данные документы являются конфиденциальными, но учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных в учреждении осуществляется в целях реализации возложенных на учреждение полномочий, определяемых законодательством РФ, Уставом учреждения, иными нормативными правовыми актами.

3.2. Персональные данные субъектов персональных данных являются сведениями конфиденциального характера (за исключением сведений установленных законодательством РФ).

Сотрудники (работники) и их представители должны быть ознакомлены под подпись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3. Учреждение является оператором, организующим и осуществляющим обработку персональных данных. Функции оператора возлагаются на должностных лиц, осуществляющих обработку персональных данных. Перечень должностей сотрудников, осуществляющих обработку персональных данных, определяется приложением 6 к настоящему Положению.

3.4. Оператор (должностные лица, осуществляющие обработку персональных данных) при обработке персональных данных обладает полномочиями и исполняет трудовые обязанности, установленные Федеральным законом «О персональных данных», Трудовым кодексом Российской Федерации, настоящим Положением и иными нормативными правовыми актами.

3.5. Лица, непосредственно осуществляющие обработку персональных данных, в обязательном порядке под подпись знакомятся с документацией по сохранности и защите персональных данных, в том числе с настоящим Положением, локальными нормативными актами учреждения по вопросам обработки персональных данных и документами, устанавливающими обязанности данных лиц по соблюдению требования конфиденциальности и безопасности персональных данных.

3.6. В случае попытки кого-либо получить от лиц, осуществляющих обработку персональных данных, сведения, являющиеся персональными данными, а также о причинах и условиях возможной утечки этих данных указанные лица обязаны сообщать непосредственному руководителю, как только им стало известно.

3.7. В соответствии с ч. 1 ст. 8 Федерального закона «О персональных данных» в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги, электронные сайты). 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, предоставленные субъектом персональных данных.

В соответствии с ч. 2 ст. 8 Федерального закона «О персональных данных» сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных (приложение 2 к настоящему Положению) либо по решению суда или иных уполномоченных государственных органов.

3.8. Обработка персональных данных работников осуществляется с их письменного согласия, по форме установленной приложением 1 к настоящему Положению, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, получении образования и продвижении по работе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Для перевода персональных данных сотрудников в категорию общедоступных требуется их согласие по форме установленной приложением 3 к настоящему Положению.

3.9. Согласие сотрудника (работника) на обработку персональных данных не требуется в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных на учреждение функций, полномочий и обязанностей;

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

- обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- 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;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов учреждения или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

3.10. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или

философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных законодательством РФ

3.11. Персональные данные получают учреждением лично у гражданина, за исключением случаев, предусмотренных законодательством и настоящим Положением.

3.12. Граждане, получатели социальных услуг, предоставляют в учреждение достоверные сведения о себе и своевременно сообщают ему об изменении своих персональных данных. Для обработки объема персональных данных граждан берется согласие на обработку персональных данных по форме установленной приложением 9 к настоящему Положению. Учреждение вправе проверить достоверность сведений, предоставленных гражданами, сверяя данные с имеющимися в учреждении документами.

3.13. В случаях, необходимости получения учреждением персональных данных о гражданине у третьего лица, учреждение обязано уведомить об этом гражданина и получить от него письменное согласие по установленной приложением 4 к настоящему Положению форме.

Учреждение обязано сообщить гражданину о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных юридических последствиях отказа гражданина дать письменное согласие на их получение, по форме установленной приложением 5 к настоящему Положению.

3.14. Персональные данные хранятся как в электронном виде, так и на бумажных носителях.

Персональные данные граждан в электронном виде хранятся в информационных системах персональных данных. Доступ к электронным базам данных, содержащим персональные данные, обеспечивается системой защиты персональных данных.

При обработке персональных данных, осуществляемой без использования средств автоматизации, хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях, должно обеспечивать раздельное хранение.

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

Помещениями, определяющими места хранения персональных данных граждан на бумажных носителях, являются: архив, кабинет отделения консультативной и методической помощи (по вопросам организации отдыха детей и их оздоровления), кабинеты отделения профилактики и безнадзорности несовершеннолетних, кабинеты отделения социальной реабилитации.

Помещениями, определяющими места хранения персональных данных сотрудников (работников), является кабинет специалиста по персоналу.

3.15. Доступ к персональным данным имеют сотрудники учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией директора учреждения, доступ к персональным данным может быть предоставлен иному работнику, должность которого не включена в перечень должностей сотрудников, имеющих доступ к персональным данным, и которым они необходимы в связи с исполнением трудовых обязанностей.

3.16. Сотрудник учреждения, имеющий доступ к персональным данным граждан в связи с исполнением трудовых обязанностей обеспечивает хранение

информации, содержащей персональные данные, исключающее доступ к ним третьих лиц.

В отсутствие сотрудника на его рабочем месте не допускается наличие документов, содержащих персональные данные. Сотрудник обязан исключить несанкционированный доступ к техническим средствам обработки персональных данных. При уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия на своем рабочем месте сотрудник обязан передать документы и иные носители, содержащие персональные данные лицу, на которое приказом учреждения возложено исполнение его должностных обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию директора учреждения.

При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные граждан, передаются другому сотруднику, имеющему доступ к персональным данным по указанию директора учреждения.

3.17. В случае заключения между учреждением и третьими лицами договоров, на основании которых данные лица должны иметь доступ к персональным данным, хранящимся в учреждении, соответствующие данные предоставляются учреждением только после подписания соглашения о неразглашении конфиденциальной информации.

В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных.

3.18. Процедура оформления доступа к персональным данным включает в себя:

- ознакомление работника под подпись с настоящим Положением, при наличии иных локальных нормативных актов, регулирующих обработку и защиту персональных данных, с ними также осуществляется ознакомление работника под подпись;

- оформление письменного обязательства о неразглашении сведений, содержащих персональные данные и соблюдении правил их обработки, по установленной приложением 7 к настоящему Положению форме.

3.19. Сотрудники учреждения, имеющие доступ к персональным данным, вправе получать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций и целей обработки.

3.20. Доступ к персональным данным без специального разрешения имеют сотрудники, занимающие в учреждении следующие должности:

- директор;
- заместитель директора (по направлениям деятельности);
- юрисконсульт.

3.21. Доступ к персональным данным получателей социальных услуг физических лиц, в связи с рассмотрением обращений граждан, в рамках своей компетенции имеют сотрудники, занимающие в учреждении следующие должности:

- заведующий отделением (по направлениям деятельности);
- специалист по социальной работе;
- специалист по работе с семьей;
- психолог;
- воспитатель;
- младший воспитатель;
- дежурный по режиму;

- сторож-вахтер;
- архивариус;
- заведующий канцелярией - в отношении персональных данных, необходимых директору, заместителю директора.

3.22. Доступ к персональным данным сотрудников в рамках своей компетенции имеют, занимающие в учреждении следующие должности:

- заведующий отделением (по направлениям деятельности и только в отношении непосредственно подчиненных работников);
- заведующий столовой, только в отношении непосредственно подчиненных работников;

- экономист;
- специалист по управлению персоналом;
- специалист по охране труда;
- архивариус.

3.23. Допуск к персональным данным других сотрудников учреждения, не имеющих надлежащим образом оформленного доступа, запрещается.

3.24. Гражданин имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Гражданин имеет право вносить предложения по внесению изменений в свои персональные данные в случае обнаружения в них неточностей.

3.25. Запрещено передавать персональные данные субъекта персональных данных третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством. При передаче необходимо руководствоваться договором с третьим лицом (физическим/юридическим), существенным условием которого должна быть обязанность обеспечения указанным лицом (физическим/юридическим) конфиденциальности и безопасности персональных данных при их обработке. При предоставлении персональных данных третьим лицам фиксировать факт передачи, подкрепленный подписью принимающего лица.

Запрещено передавать персональные данные по телефону, факсу, на основании устных запросов.

При передаче персональных данных по каналам связи, сетям общего пользования (Интернет) использовать криптографические средства защиты информации.

При передаче персональных данных граждан, сотрудники учреждения предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и истребуют от этих лиц письменное обязательство в соответствии с п. 3.12. настоящего Положения.

В случае обращения с запросом лица, не уполномоченного в соответствии с нормативными правовыми актами на получение персональных данных, либо отсутствия письменного согласия субъекта персональных данных на предоставление его персональных данных третьей стороне, либо отсутствия угрозы жизни и здоровью субъекта персональных данных оператор обязан отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации.

3.26. Передача (обмен и т.д.) персональных данных осуществляется только между сотрудниками, имеющими доступ к персональным данным.

3.27. Передача персональных данных третьим лицам осуществляется только с письменного согласия гражданина, которое оформляется по установленной приложением 8 к настоящему Положению форме и должно включать в себя:

фамилию, имя, отчество, адрес гражданина, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

наименование и адрес юридического лица, получающего согласие гражданина;

цель передачи персональных данных;

перечень персональных данных, на передачу которых дает согласие гражданин;

срок, в течение которого действует согласие, а также порядок его отзыва.

Согласия граждан на передачу их персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина; когда третьи лица оказывают услуги работодателю на основании заключенных договоров, а также в случаях, установленных федеральным законом и настоящим Положением.

3.28. Не допускается передача персональных данных сотрудников, граждан в коммерческих целях без их письменного согласия.

3.29. Передача документов (иных материальных носителей), содержащих персональные данные, осуществляется при наличии у лица, уполномоченного на их получение:

договора на оказание услуг учреждению;

соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных гражданина;

письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных несет сотрудник, а также руководитель структурного подразделения, осуществляющего передачу персональных данных третьим лицам.

3.30. Представителю гражданина (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

нотариально удостоверенной доверенности представителя гражданина;

письменного заявления гражданина, написанного в присутствии сотрудника учреждения (если заявление написано не в присутствии сотрудника учреждения, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в учреждении.

3.31. Предоставление персональных данных государственным органам производится в соответствии с требованиями действующего законодательства и настоящим Положением.

3.32. Персональные данные могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого гражданина, за исключением случаев, когда передача персональных данных без его согласия допускается действующим законодательством.

3.33. Документы, содержащие персональные данные, могут быть отправлены через организацию почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

4. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. 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.

4.2. 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 незаинтересованные в возникновении угрозы лица.

4.3. 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 деятельности учреждения.

4.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается учреждением за счет средств учреждения в порядке, установленном федеральными законами.

4.5. Защите подлежит:

информация о персональных данных;

документы, содержащие персональные данные;

персональные данные, содержащиеся на электронных носителях.

4.6. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами учреждения.

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

- ограничение и регламентация состава работников, функциональные обязанности которых требуют обработки персональных данных;

- 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 сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

- организация порядка уничтожения информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только директору, заместителям директора (по направлениям деятельности) и в исключительных

случаях, по письменному разрешению директора, руководителю структурного подразделения.

4.8. Все персональные компьютеры, содержащие персональные данные работника, должны быть защищены паролем доступа.

4.9. Защита сведений, хранящихся в электронных базах данных учреждения, от несанкционированного доступа, искажения и уничтожения информации, а также от иных неправомерных действий, обеспечивается системой защиты персональных данных.

4.10. Для защиты персональных данных 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.

4.11. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, 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 в отделе кадров.

4.12. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

4.13. По возможности персональные данные обезличиваются.

4.14. Кроме мер защиты персональных данных, установленных законодательством, учреждение, сотрудники и их представители могут вырабатывать совместные меры защиты персональных данных.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном законодательством РФ.

5.2. Разглашение персональных данных в учреждении (передача их посторонним лицам, в том числе, работникам учреждения, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания – замечания, выговора, увольнения.

Сотрудник учреждения, имеющий доступ к персональным данным и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба учреждению (п.7 ст. 243 Трудового кодекса РФ).

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
дата рождения _____
паспорт: серия _____ номер _____ выдан _____
_____ адрес регистрации и фактического места жительства (с указанием индекса)

настоящим даю **согласие на обработку персональных данных** бюджетному учреждению социальной защиты населения Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» г. Череповца» (далее – Учреждение), адрес: город Череповец, ул. Красnodонцев, д. 21, с целью обеспечения соблюдения трудового законодательства, законодательства о противодействии коррупции, иных законов и принятых в соответствии с ними нормативных правовых актов, при содействии в трудоустройстве, обучении и продвижении по работе, обеспечения личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, учета результатов исполнения должностных обязанностей, реализации возложенных на Учреждения полномочий.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (форма Т-2), трудовой книжке и (или) сведениях о трудовой деятельности и полученная в течение срока действия настоящего трудового договора, в том числе:

- фамилия, имя, отчество (в том числе информация о смене фамилии, имени, отчества – когда, где и по какой причине изменены);
- дата (число, месяц, год) и место рождения (село, деревня, город, район, область, край, республика, страна);
- гражданство (в том числе измененное - когда и по какой причине, прежнее гражданство, наличие гражданства другого государства);
- данные паспорта гражданина Российской Федерации (серия, номер, кем и когда выдан);
- место жительства и дата регистрации по месту жительства, место фактического проживания;
- номера контактных телефонов;
- адрес электронной почты;
- семейное положение (в случае развода - данные о разводе), реквизиты актов гражданского состояния;
- свидетельства о рождении детей;
- сведения о близких родственниках: отец, мать, а также супруга (супруг) (в том числе фамилия, имя, отчество, год рождения, адрес регистрации и фактического проживания);
- образование (когда и какие учебные заведения окончены, номера дипломов). Направление подготовки или специальность, квалификация по диплому;
- послевузовское профессиональное образование: аспирантура, магистратура, докторантура (наименование образовательного или научного учреждения, год окончания). Ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- сведения о судимости/отсутствии (когда и по какой статье);
- отношение к воинской обязанности и воинское звание;
- биометрические данные (фотография, в том числе размещение на сайте учреждения, на Доске Почета, информационно-телекоммуникационной сети Интернет и др);
- знание иностранных языков и языков народов Российской Федерации (степень знания);

- присвоение классных чинов, дипломатических рангов, воинских или специальных званий, квалификационных разрядов (наименование, кем и когда присвоены);
- награждение государственными и ведомственными наградами, иными наградами и знаками отличия;
- выполняемая работа с начала трудовой деятельности, включая учебу в высших и средних учебных заведениях, военную службу, работу по совместительству, предпринимательскую деятельность и т.п. (период работы, должность с указанием организации). Информация, содержащаяся в трудовой книжке;
- сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации (ИНН);
- сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования (СНИЛС);
- сведения о состоянии здоровья (заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на работу в учреждение);
- сведения о назначении на занимаемую должность, переводах на иную должность, увольнении (дата, основание), содержание трудового договора;
- сведения о занимаемой должности;
- условия оплаты труда по занимаемой должности, социальные льготы;
- сведения об отпусках и командировках;
- сведения о временной нетрудоспособности;
- данные о прохождении профессиональной переподготовки, повышении квалификации, стажировки;
- сведения о прохождении аттестации, датах прохождения, отзывах об исполнении должностных обязанностей за аттестационный период, принятых аттестационной комиссией решениях, вынесенных рекомендациях;
- сведения о поощрениях;
- документы, содержащие информацию о проведении служебных расследований и наложении дисциплинарных взысканий;
- реквизиты полиса обязательного медицинского страхования;
- номера банковских счетов;
- о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора;
- дополнительных данных, которые я сообщил (а) в анкете.

Даю согласие на передачу моих персональных данных:

1. КУ Вологодской области «Центр социальных выплат», г. Череповец, пр. Строителей, д. 23, с целью ведения бухгалтерского учета, формирования налоговой отчетности и отчетности в государственные внебюджетные фонды в соответствии с действующим законодательством:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- сведения об изменении фамилии, имени, отчества (когда, где и по какой причине);
- профессиональное образование (оконченные учебные заведения и год окончания, специальность (направление) и квалификация, наличие ученых степеней);
- сведения о трудовом стаже;
- отношение к воинской обязанности и воинское звание;
- сведения о месте регистрации и месте фактического проживания, номер домашнего телефона, номер сотового телефона, адрес электронной почты;
- данные паспорта гражданина РФ;
- номер страхового свидетельства обязательного пенсионного страхования;
- реквизиты актов гражданского состояния (состояние в браке, наличие детей и др.);
- ИНН;
- номер полиса обязательного и добровольного медицинского страхования;
- сведения о занимаемой должности (наименование занимаемой должности, дата назначения на занимаемую должность, принятия на работу, характер работы);

- сведения об условиях оплаты труда по занимаемой должности;
- сведения о награждении государственными и ведомственными наградами, иными наградами;
- сведения о временной нетрудоспособности;
- сведения с предыдущего места работы о доходах.

2. В медицинские учреждения или страховые организации, с которыми заключен соответствующий договор, в том числе для прохождения диспансеризации: фамилия, имя, отчество; дата и место рождения; домашний адрес; данные паспорта гражданина Российской Федерации, номер медицинского полиса.

Настоящее согласие предоставляется на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, извлечение, обезличивание, блокирование, удаление, уничтожение передачу (доступ, предоставление) вышеуказанных данных в течение всего периода действия моего трудового договора и после его прекращения (увольнения) – в течение срока установленного нормативными правовыми актами до передачи документов, содержащих персональные данные, в соответствии с требованиями действующего законодательства РФ на архивное хранение и Федерального закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Обязуюсь сообщать в трехдневный срок об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных.

Об ответственности за достоверность представленных персональных сведений предупрежден(а).

(фамилия, инициалы лица, давшего согласие)

(подпись)

« ____ » _____ 20 ____ года

Директору БУ СО ВО «СРЦН
«Росток» г. Череповца»

**Заявление
о прекращении обработки персональных данных**

Прошу «БУ СО ВО «СРЦН «Росток» г. Череповца», г. Череповец, ул. Краснодонцев, д. 21, прекратить обработку следующих моих персональных данных (*нужное подчеркнуть*):

1. Фамилия, имя, отчество
2. Место рождения
3. Дата рождения
4. Адрес регистрации
5. Паспортные данные гражданина Российской Федерации (серия, номер паспорта, кем и когда выдан)
6. Адрес фактического проживания
7. Телефонный номер (домашний, мобильный)
8. Телефонный номер (рабочий)
9. Семейное положение
10. Состав семьи (муж/жена, дети)
11. Номер страхового свидетельства обязательного пенсионного страхования
12. ИНН
13. Номер полиса обязательного медицинского страхования
14. Сведения о состоянии здоровья (наличие справки об инвалидности)
15. Информация о знании иностранных языков
16. Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность (направления))
17. Информация о периодах трудовой деятельности (место работы, должность, период работы, причины увольнения)
18. Данные о трудовом договоре и дополнительных соглашениях
19. Сведения о структурном подразделении, должности
20. Данные о начисленных суммах по основному месту работы
21. Данные о начисленных суммах по совместительству
22. Данные о суммах удержаний и перечислений из заработной платы работника согласно его заявлению
23. Данные о суммах удержаний из заработной платы работника согласно исполнительному листу
24. Данные о банковской карте
25. Общий трудовой стаж (сведения по стажу)
26. Сведения о выходе на пенсию
27. Сведения листка временной нетрудоспособности
28. Сведения о социальных льготах
29. Сведения по совмещаемой должности

30. Данные о должностном окладе
31. Сведения о типе и сумме налогового вычета
32. Информация о командировках
33. Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета)
34. Информация о негосударственном пенсионном обеспечении
35. Данные об аттестации работников
36. Данные о повышении квалификации
37. Данные о наградах, медалях, поощрениях
38. Данные о почетных званиях
39. Данные об ученых степенях
40. Наличие дисциплинарных взысканий
41. Информация об отпусках
42. Данные о рекомендациях и характеристиках
43. Данные о наличии сертификата (дата выдачи и продления, наименование специальности)
44. Фотография
45. Другое _____

в связи с _____

(указать причину)

«__» _____ 20__ г.

_____ (подпись)

_____ (расшифровка подписи)

Приложение 3 к Положению

ФОРМА

Директору БУ СО ВО «СРЦН
«Росток» г. Череповца»

СОГЛАСИЕ

на перевод персональных данных: фамилия, имя, отчество; телефонный номер (рабочий); занимаемой должности в категорию общедоступных.

[illegible]

Директору БУ СО ВО «СРЦН
«Росток» г. Череповца»

от _____
(ФИО гражданина)

_____ (год рождения)

проживающий

по адресу: _____

паспорт: _____

выдан: _____

**Согласие
гражданина на получение его персональных данных у третьей стороны**

Я, _____,
в соответствии со ст. 86 ТК РФ _____ на получение моих персональных
данных, а именно: _____
(согласен, не согласен)

у _____
(Ф.И.О. физического лица или наименование организации, у которых получается информация)

О целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение предупрежден.

« ____ » _____ 20 ____ г.

_____ (подпись)

_____ (ФИО работника)

Примечание:

1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность работника.
2. Письменное согласие граждан заполняется и подписывается им собственноручно, в присутствии сотрудника организации.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

**Форма разъяснения субъекту персональных данных юридических последствий
отказа дать письменное согласие на их получение**

Уважаемый (-ая) (имя и отчество)!

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» и другими нормативными правовыми актами, уведомляем Вас об обязанности предоставления персональных данных.

В случае отказа в предоставлении Вами персональных данных, бюджетное учреждение социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» не сможет на законных основаниях осуществлять обработку персональных данных, что приведет к следующим юридическим последствиям – отказ в оказании социальных услуг.

В целях обеспечения защиты персональных данных Вы имеете право:

- получать сведения, подтверждающие факт обработки персональных данных БУ СО ВО «СРЦН «Росток» г. Череповца», правовые основания и цели обработки персональных данных, сроки обработки персональных данных, в том числе сроки их хранения, информацию о наименовании и месте нахождения оператора и о способах обработки персональных данных;
- получать информацию о лице, осуществляющем обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- безвозмездно знакомиться с Вашими персональными данными;
- требовать внесения необходимых изменений, уничтожения или блокирования персональных данных при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- обжаловать действия или бездействие БУ СО ВО «СРЦН «Росток» г. Череповца» в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке, если считаете, что учреждение осуществляет обработку Ваших персональных данных с нарушением требований законодательства Российской Федерации или иным образом нарушает Ваши права и свободы.

С уважением

директор БУ СО ВО «СРЦН «Росток» г. Череповца» _____

подпись

/ расшифровка подписи

Разъяснения юридических последствий отказа в предоставлении персональных данных получил (-а).

«_____» _____ 20__ г.

(подпись)

(ФИО)

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ
сотрудников учреждения, осуществляющих автоматизированную,
неавтоматизированную, смешанную обработку персональных данных

1. Директор
2. Заместитель директора (по направлениям деятельности)
3. Заведующий отделением (по направлениям деятельности)
4. Специалист по персоналу
5. Экономист
6. Специалист по социальной работе (по направлениям деятельности)
7. Специалист по работе с семьей
8. Юрисконсульт
9. Архивариус
10. Документовед
11. Дежурный по режиму
12. Сторож-вахтер

**Обязательство
о неразглашении информации, содержащей персональные данные**

Я, _____
(фамилия, имя, отчество – полностью)

выполняющий должностные обязанности по должности (профессии) _____

предупрежден(а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать и не распространять третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. Осуществлять обработку и предоставлять персональные данные в соответствии со ст.6 ФЗ № 152-ФЗ.

3. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю, либо ответственному за организацию работы по защите персональных данных в учреждении.

4. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

6. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать, не распространять и не предоставлять третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

фамилия, инициалы

подпись

« _____ » _____ 20 ____ г.

Директору БУ СО ВО «СРЦН
«Росток» г. Череповца»

от

(ФИО, должность работника)

(год рождения)

проживающий

по адресу:

паспорт:

выдан:

Согласие работника на передачу его персональных данных третьей стороне

Я, _____, в
соответствии со ст. 86 ТК РФ _____ на передачу моих персональных
(согласен, не согласен)

данных, а именно:

1. фамилия, имя, отчество;
2. паспортные данные;
3. год, месяц, дата и место рождения;
4. адрес;
5. семейное, социальное, имущественное положение;
6. образование;
7. профессия;
8. сведения о трудовом и общем стаже;
9. доходы, полученные мной в данном учреждении;
10. сведения о воинском учете;
11. домашний телефон
12. _____

13. для обработки в целях

следующим лицам _____

(указываются Ф.И.О. физического лица или наименование организации,
которым сообщаются данные)

Согласие на передачу персональных данных третьей стороне действительно в течение
всего срока действия трудового договора.

Подтверждаю, что ознакомлен с Положением об обработке и защите персональных
данных в бюджетном учреждении социального обслуживания Вологодской области
«Социально-реабилитационный центр для несовершеннолетних «Росток» города
Череповца», права и обязанности в области защиты персональных данных мне разъяснены, а
также право работодателя обрабатывать (в том числе и передавать) часть моих персональных
данных без моего согласия, в соответствии с законодательством РФ.

Подтверждаю, что отзыв согласия производится в письменном виде в соответствии с
действующим законодательством.

Всю ответственность за неблагоприятные последствия отзыва согласия беру на себя.

«___» _____ 20__ г.

(подпись)

(ФИО работника)

СОГЛАСИЕ
гражданина на обработку персональных данных

Я, _____,
(Ф.И.О)

имеющий (ая) паспорт серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____,
(когда и кем)

проживающий(ая) по адресу _____,
настоящим даю свое согласие бюджетному учреждению социального обслуживания
Вологодской области «Социально-реабилитационный центр для несовершеннолетних
«Росток» города Череповца», расположенному по адресу: 162603, Вологодская область, г.
Череповец, улица Краснодонцев, д. 21, на обработку моих персональных данных и
подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для _____
(указать цель обработки ПД)

и распространяется на следующую информацию:

1) основных данных (непосредственных): фамилии, имени, отчества, гражданстве, дате и
месте рождения, адресе проживания и регистрации, семейном, социальном, имущественном
положении, образовании (оконченные учебные заведения и год окончания, специальности и
квалификации, наличии ученых степеней), ИНН, СНИЛС, паспортных данных, данных
медицинского полиса, биометрических персональных данных, наличия либо отсутствия
судимости;

2) о трудовой деятельности: место работы, должность,

3) номера контактных телефонов;

4) данные о близких родственниках (ФИО, дата рождения, степень родства, адрес
проживания);

5) дополнительно (указать) _____

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, систематизацию, накопление, хранение,
уточнение (обновление, изменение), использование, распространение (в том числе передача),
обезличивание, блокирование, уничтожение, трансграничную передачу персональных
данных, а также осуществление любых иных действий с моими персональными данными с
учетом федерального законодательства.

В случае неправомерного использования предоставленных мною персональных данных
согласие отзывается моим письменным заявлением.

Данное согласие действует на срок _____.

(фамилия, инициалы лица, давшего согласие)

(подпись)

«__» _____ 20__ года.

**Перечень
информационных систем персональных данных
в бюджетном учреждении социального обслуживания Вологодской области
«Социально-реабилитационный центр для несовершеннолетних «Росток»
города Череповца» (далее БУ СО ВО «СРЦН «Росток» г.Череповца»**

№ п/п	Наименование информационных систем, баз и банков данных, реестров, регистров, номенклатур дел	Область применения, описание	Категория содержащейся информации (для открытого доступа/ ограниченного доступа)
1	Единый социальный регистр населения (ЕСРН) (государственная информационная система)	Оказание государственных услуг в электронном виде и межведомственное взаимодействие	Для ограниченного доступа
2	Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца»	1) Банки данных семей и детей, находящихся на сопровождении в учреждении 2) Банки данных по организации отдыха и оздоровления несовершеннолетних	Для ограниченного доступа
3	Система персональных данных сотрудников БУ СО ВО «СРЦН «Росток» г. Череповца»	Автоматизированный бухгалтерский и кадровый учет - ЕЦИС «Смета»	Для ограниченного доступа

ПРАВИЛА
работы с обезличенными персональными данными
в бюджетном учреждении социального обслуживания Вологодской области
«Социально-реабилитационный центр для несовершеннолетних «Росток»
города Череповца» (далее - Правила)
(новая редакция)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», принятыми в соответствии с нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», локальными правовыми актами и инструкциями в области защиты информации учреждения.

1.2. Настоящие Правила определяют порядок работы с обезличенными данными в учреждении.

1.3. Настоящие правила утверждаются директором учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

2.2. 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.

2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

2.5. Конфиденциальность персональных данных - обязательное для соблюдения оператора или иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ.

3. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

3.1. Обезличивание персональных данных в учреждении может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных (далее - ИСПДн) и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение - понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Для обезличивания персональных данных применяются способы явно не запрещенные законодательно.

3.5. Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, прилагается (приложение к настоящим правилам).

3.6. Сотрудники учреждения, непосредственно осуществляющие обработку персональных данных (заместитель директора (по направлениям деятельности), специалист по персоналу, архивариус, заведующий отделением (по направлениям деятельности)), готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

3.7. Ответственный за организацию обработки персональных данных в учреждении обобщает предложения по обезличиванию персональных данных директору учреждения.

3.8. Решение о необходимости обезличивания персональных данных принимает директор учреждения.

3.9. Сотрудники учреждения, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

4. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. При работе с обезличенными персональными данными должна соблюдаться конфиденциальность данных, обезличенные персональные данные не подлежат разглашению.

4.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съёмными носителями (если они используются);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ
сотрудников ответственных за проведение мероприятий
по обезличиванию обрабатываемых персональных данных

1. Директор
2. Заместитель директора (по направлениям деятельности)
3. Заведующий отделением (по направлениям деятельности)
4. Специалист по персоналу
5. Экономист
6. Архивариус

ПОЛОЖЕНИЕ

об обеспечении сохранности конфиденциальной информации и персональных данных в служебных помещениях бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца»
(далее - положение, учреждение)
(новая редакция)

1. ТРЕБОВАНИЯ К СЛУЖЕБНОМУ ПОМЕЩЕНИЮ

1.1. Служебное помещение является помещением обработки, хранения, передачи конфиденциальной информации и персональных данных: отделение профилактики безнадзорности несовершеннолетних; отделение социальной реабилитации; отделение консультативной и методической помощи; кабинет специалиста по персоналу (кадры); кабинет экономиста; архив.

1.2. Служебное помещение имеет входную дверь с надежным механическим замком.

1.3. Внутренняя планировка служебного помещения и расположение в нем рабочих мест сотрудников (работников), ответственных за сохранность конфиденциальной информации и персональных данных (далее – ответственные специалисты), должны способствовать выполнению работы в условиях, предусматривающих обеспечение персональной ответственности работников за сохранность доверенных им документов, в которых содержится конфиденциальная информация и персональные данные.

1.4. Размещение служебного помещения исключает возможность бесконтрольного проникновения в это помещение посторонних лиц, оборудование служебного помещения гарантирует сохранность находящихся в нем носителей конфиденциальной информации и персональных данных.

2. ОРГАНИЗАЦИЯ РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ И ПЕРСОНАЛЬНЫМИ ДАННЫМИ В СЛУЖЕБНОМ ПОМЕЩЕНИИ

2.1. Документы, содержащие конфиденциальную информацию и персональные данные, когда они не используются, хранятся в запираемых сейфах, металлических шкафах, ключи от которых хранятся у заведующих отделениями; специалиста по персоналу; экономиста; архивариуса.

2.2. В служебном помещении запрещается работать с документами, не имеющими непосредственного отношения к основной деятельности, а также хранить посторонние предметы.

2.3. Уборка и другие необходимые хозяйственные работы в служебном помещении проводятся в присутствии работников. Во время уборки и хозяйственных работ все носители информации должны быть убраны в соответствующие сейфы.

3. ПОРЯДОК ОПЕЧАТЫВАНИЯ И ВСКРЫТИЯ ВХОДНОЙ ДВЕРИ СЛУЖЕБНОГО ПОМЕЩЕНИЯ

3.1. Перед вскрытием служебного помещения в начале рабочего дня ответственные специалисты проверяют целостность и исправность замка. При обнаружении повреждения замка, а также других признаков, указывающих на возможное проникновение в это помещение посторонних лиц, вскрытие не производят, о случившемся составляют акт и немедленно информируют администрацию учреждения. Одновременно принимают меры по охране места происшествия. До прибытия на место представителя администрации в служебное помещение никто не допускается.

3.2. В случае выхода ответственных специалистов из служебного помещения в течение рабочего дня дверь служебного помещения закрывается на ключ.

3.3. В конце рабочего дня документы, содержащие конфиденциальную информацию и персональные данные, убираются ответственными специалистами в запираемые сейфы или металлические шкафы.

3.4. Ключи от запираемых сейфов или металлических шкафов и служебного помещения складываются заведующими отделениями, специалистом по персоналу, экономистом, архивариусом в специальный пенал, который затем опечатывается.

3.5. Опечатанный специальный пенал с ключами передается на хранение дежурному по режиму/сторожу-вахтеру (далее – работники вахты) и хранится в помещении вахты.

3.6. Дубликат ключа от замка входной двери служебного помещения хранится у работников вахты в отдельном опечатанном пенале.

3.7. В случае утраты ключа от запираемых сейфов или металлических шкафов, а также входной двери служебного помещения немедленно ставится в известность администрация учреждения и осуществляется замена замка или его секрета.

3.8. Хранение носителей конфиденциальной информации и персональных данных в запираемых сейфах и металлических шкафах, от которых утрачены ключи, до замены замка или его секрета запрещается.

4. ОБЯЗАННОСТИ СПЕЦИАЛИСТОВ, ОТВЕТСТВЕННЫХ ЗА СОХРАННОСТЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ ПО КАДРОВОМУ ДЕЛОПРОИЗВОДСТВУ

4.1. Организовывать работу по обеспечению сохранности конфиденциальной информации и персональных данных в служебном помещении строго в соответствии с настоящим Положением.

4.2. Нести персональную ответственность за сохранность доверенных им сведений.

4.3. Не допускать действий, которые могут повлечь утрату конфиденциальных документов или разглашение конфиденциальной информации.

4.4. Знать и соблюдать требования локальных актов учреждения о режиме защиты конфиденциальной информации и персональных данных.

4.5. Незамедлительно сообщать уполномоченным лицам об утрате документов, содержащих конфиденциальную информацию или персональные данные, о фактах посягательств на незаконный сбор сведений, составляющих конфиденциальную информацию или персональные данные.

4.6. Оформлять письменные объяснения об известных им обстоятельствах при проведении разбирательств по фактам нарушения требований внутренних нормативных актов учреждения о режиме защиты конфиденциальной информации и персональных данных, а также по фактам утраты и хищения документов, содержащих конфиденциальную информацию учреждения.

ПОРЯДОК
доступа работников учреждения, посетителей в помещения бюджетного
учреждения социального обслуживания Вологодской области «Социально-
реабилитационный центр для несовершеннолетних «Росток» города
Череповца» (далее - учреждение), в которых ведется обработка
персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий порядок определяет правила ограничения доступа сотрудников (работников) учреждения, посетителей в помещения учреждения, где ведется обработка персональных данных.

1.2. Ограничение доступа в помещения устанавливается с целью исключения фактов неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2. ПРАВИЛА ДОСТУПА В ПОМЕЩЕНИЯ,
В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Доступ в помещения сотрудников, посетителей разрешается только в рабочее время работника, ведущего обработку персональных данных.

2.2. Уборка помещений должна производиться в присутствии сотрудника, ведущего обработку персональных данных, с соблюдением мер исключаяющих доступ посторонних лиц к персональным данным.

2.3. Обслуживание технических средств, находящихся в помещении, должно производиться под наблюдением работника, ведущего обработку персональных данных.

2.4. Ключи от помещений сдаются сотруднику службы режима/вахтеру.

2.5. Ключи от помещений выдаются сотрудником службы режима/вахтером только работникам, работающим в данных помещениях.

2.6. При необходимости доступа в помещения (при проведении аварийных работ, срабатывании пожарной, охранной сигнализаций) вскрытие помещений осуществляется в присутствии ответственного за организацию обработки персональных данных в учреждении и (или) сотрудника службы режима.

2.7. Для хранения материальных носителей персональных данных помещения оборудуются сейфами и (или) специальными шкафами, закрываемыми на ключ.

2.8. В помещениях должна соблюдаться «политика чистого стола». После завершения работы с документами, содержащими персональные данные, их необходимо убрать со стола в защищенное место. Отключить технические средства, участвующие в обработке персональных данных.

2.9. Категорически запрещен бесконтрольный доступ и бесконтрольное нахождение посетителей учреждения в данные помещения.

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их
представителей на получение информации, касающейся обработки его
персональных данных, обращений уполномоченного органа по защите прав
субъектов персональных данных в бюджетном учреждении социального
обслуживания Вологодской области «Социально-реабилитационный центр для
несовершеннолетних «Росток» города Череповца» (далее — Правила,
учреждение)
(новая редакция)

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Персональные данные - любая информация, прямо или косвенно относящаяся к определенному или определяемому физическому лицу (субъект персональных данных).

1.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

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

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

1.6. 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.

1.7. Заявитель - субъект персональных данных (физическое лицо) или его представитель.

1.8. Запрос - обращение заявителя в учреждение с правами и без прав юридического лица в письменной форме или в форме электронного документа, заявление или жалоба, а также устное обращение заявителя либо обращение уполномоченного органа по защите прав субъектов персональных данных.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящие Правила определяют порядок рассмотрения в учреждении запросов субъектов персональных данных или их представителей на получение также обращений уполномоченного органа по защите прав субъектов

персональных данных.

2.2. Настоящие Правила разработаны в соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных»; от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудовым кодексом Российской Федерации, постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными правовыми актами и инструкциями в области защиты информации в учреждении.

3. ПРАВА ЗАЯВИТЕЛЯ НА ДОСТУП К ЕГО ПЕРСОНАЛЬНЫМ ДАННЫМ

3.1. Заявитель имеет право на получение информации, касающейся обработки его персональных данных, содержащей:

- 1) подтверждение факта обработки персональных данных учреждением;
- 2) правовые основания и цели обработки персональных данных;
- 3) применяемые способы обработки персональных данных;
- 4) наименование и место нахождения учреждения, осуществляющего обработку персональных данных;
- 5) сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора на основании законодательства РФ;
- 6) обрабатываемые персональные данные, относящиеся к заявителю, источник их получения, если иной порядок предоставления таких данных не предусмотрен Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 7) сроки обработки персональных данных, сроки их хранения;
- 8) порядок осуществления заявителем прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 9) информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
- 10) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению учреждения, если обработка поручена или будет поручена такому лицу;
- 11) иные сведения, предусмотренные нормативными правовыми актами в области защиты персональных данных.

3.2. Право заявителя на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.3. Заявитель вправе требовать от учреждения уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.4. Сведения, указанные в пункте 3.1 настоящих Правил, должны быть предоставлены заявителю учреждения в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

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

3.6. В случае если сведения, указанные в пункте 3.1 настоящих Правил, а также обрабатываемые персональные данные, были предоставлены для ознакомления заявителю по его запросу, заявитель вправе обратиться повторно в учреждение или направить повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого является заявитель, как выгодоприобретатель либо поручитель.

3.7. Заявитель вправе обратиться повторно в учреждение или направить повторный запрос в целях получения сведений, указанных в пункте 3.1 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 3.6 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 3.5 настоящих Правил, должен содержать обоснование направления повторного запроса.

3.8. Учреждение вправе отказать заявителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 3.6, 3.7 настоящих Правил. Такой отказ должен быть мотивированным, обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на учреждении.

4. ПРАВА УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАССМОТРЕНИИ ОБРАЩЕНИЯ ЗАЯВИТЕЛЯ

4.1. Уполномоченный орган по защите прав субъектов персональных данных имеет право:

- запрашивать у учреждения информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
- проводить проверки соблюдения обязательных требований в сфере обработки персональных данных;
- требовать от органов мэрии уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки персональных

данных, осуществляемой с нарушением требований федеральных законов.

4.2. Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу необходимую информацию в течение тридцати дней с даты получения такого запроса.

4.3. Учреждение обязано принять необходимые меры по устранению нарушений, выявленных в ходе проведения проверки соблюдения обязательных требований в сфере обработки персональных данных и выполнения требований уполномоченного органа по защите прав субъектов персональных данных.

5. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ УЧРЕЖДЕНИЯ ПРИ ОБРАЩЕНИИ ЗАЯВИТЕЛЯ

5.1. Все запросы заявителей в учреждение на получение информации, касающейся обработки его персональных данных, подлежат регистрации и учету.

5.2. Должностные лица учреждения обязаны сообщить заявителю информацию о наличии персональных данных, относящихся к нему, а также предоставить возможность ознакомления с ними в течение тридцати дней со дня обращения заявителя либо от даты получения запроса.

5.3. В случае отказа в предоставлении заявителю информации о наличии персональных данных о нем должностные лица учреждения обязаны представить в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения заявителя, либо от даты получения запроса.

5.4. Предоставление информации о наличии персональных данных заявителя осуществляется безвозмездно.

5.5. Должностные лица учреждения обязаны при предоставлении заявителем информации подтверждающей, что его персональные данные являются неполными, неточными или неактуальными, внести в них необходимые изменения в срок, не превышающий 7-ми рабочих дней со дня поступления информации.

5.6. Должностные лица учреждения обязаны при предоставлении заявителем информации, подтверждающей, что его персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие персональные данные в срок, не превышающий 7-ми рабочих дней со дня поступления информации.

5.7. Должностные лица учреждения обязаны уведомить о внесенных изменениях в его персональные данные и принятых мерах заявителя и третьих лиц, которым персональные данные этого заявителя были переданы.

ПРАВИЛА

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в БУ СО ВО «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – Правила, учреждение) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ «О персональных данных» (далее – Федеральный закон о персональных данных), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом о персональных данных.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информация – сведения (сообщения, данные) независимо от формы их представления.

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Убытки – расходы, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено.

Моральный вред – физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо

посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

Оценка возможного вреда – определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

3. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Вред субъекту персональных данных возникает в результате неправомерного действия или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

- неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
- неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
- неправомерное изменение персональных данных является нарушением целостности персональных данных;
- нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации;
- нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
- обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;
- неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
- принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

3.3. Субъекту персональных данных может быть причинён вред в форме:

- убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;
- морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права

гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законодательством.

3.4. В оценке возможного вреда учреждение исходит из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

- низкий уровень возможного вреда – последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;
- средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;
- высокий уровень возможного вреда – во всех остальных случаях.

4. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА, А ТАКЖЕ СООТНЕСЕНИЯ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ ОПЕРАТОРОМ МЕР

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в учреждении за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении 1, прилагаются.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», определяется лицом, ответственным в учреждении за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых Оператором мер

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
1	Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации и локальными актами по обеспечению безопасности персональных данных
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2	Порядок и условия применения средств защиты информации;	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты ИСПД
		Целостность	+		
		Доступность	-		
		Конфиденциальность	-		
3	Состояние учета машинных носителей персональных данных;	Убытки и моральный вред	-	низкий	В соответствии с принятыми организационными мерами
		Целостность	+		
		Доступность	-		

		Конфиденциальность	-		
4	Соблюдение правил доступа к персональным данным;	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами
		Целостность	+		
		Доступность			
		Конфиденциальность	+		
5	Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг средств защиты информации на наличие фактов доступа к ПД
		Целостность	-		
		Доступность	+		
		Конфиденциальность	-		
6	Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;	Убытки и моральный вред	-	низкий	Применение резервного копирования
		Целостность	+		
		Доступность	-		
		Конфиденциальность	-		
7	Осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред	-	низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность	-		
		Конфиденциальность	-		

РУКОВОДСТВО
по порядку использования и организации работы со средствами
криптографической защиты информации, не содержащей сведений,
составляющих государственную тайну в бюджетном учреждении социального
обслуживания Вологодской области «Социально-реабилитационный центр для
несовершеннолетних «Росток» города Череповца»
(далее – Руководство, учреждение)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Руководство разработано в соответствии с Федеральными законами от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», 06.04.2011 № 63-ФЗ «Об электронной подписи», приказом ФАПСИ при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», приказом ФСБ Российской Федерации от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)», Методических рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных ФСБ России 31.03.2015 № 149/7/2/6-432.

1.2. Настоящее Руководство устанавливает единые требования в учреждении по обеспечению безопасности функционирования криптосредств для защиты информации, не содержащей сведений, составляющих государственную тайну, определяет функциональные обязанности ответственного пользователя криптосредств и пользователя криптосредств, порядок учета, выдачи, хранения, уничтожения криптосредств, действия при компрометации криптосредств.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система - система, состоящая из сотрудников и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида, в составе: вычислительная техника (компьютер), устройства ввода/вывода (монитор, принтер, МФУ) и передачи информации.

Электронный документ - документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись - информация в электронной форме, которая присоединена к

другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Криптосредство - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну.

Шифровальные (криптографические) средства:

а) средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;

г) средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (криптоключи) - сохраняемая в тайне, закрытая информация, используемая криптографическим алгоритмом при шифровании/расшифровании сообщений, постановке и проверке цифровой подписи.

Ответственный пользователь криптосредств - сотрудник учреждения, назначенный ответственным за обеспечение функционирования и безопасности криптосредств в учреждении.

Пользователь криптосредств - сотрудник учреждения, наделенный правом применения средства криптографической защиты для выполнения возложенных на него обязанностей.

Конфиденциальность - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Безопасность информации - состояние защищенности информации, характеризуемое способностью сотрудников, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от третьих лиц, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий. Защищаемую информацию.

Криптографическая (шифровальная) защита - защита информации от ее несанкционированного доступа и модификации посторонних лиц при помощи алгоритмов криптографического преобразования.

Доступ к информации - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых автоматизированными системами.

Компрометация криптосредства - хищения, утрата, разглашение, несанкционированное копирование и другие действия, в результате которых криптосредства могут стать доступными третьим лицам, не имеющим право использовать криптосредства.

Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников, обслуживающего персонала и посетителей, а также транспортных, технических и иных материальных ценностей.

3. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ

3.1. Ответственным пользователем криптосредств в учреждении является заместитель директора.

3.2. Директор определяет сотрудников учреждения, допущенных к работе с криптосредствами, в соответствии с возложенными на них функциональными обязанностями.

3.3. Директор учреждения принимает необходимые меры по размещению, специальному оборудованию, организации охраны и соблюдению установленного режима информационной безопасности в помещениях, где используются криптосредства и хранятся ключевые документы к ним.

4. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

Ответственный пользователь криптосредств обязан:

- организовывать получение криптосредств, ключевых документов, эксплуатационной и технической документации к ним у удостоверяющих центров;
- вести учет криптосредств, ключевых документов, эксплуатационной и технической документации с использованием регистрационных номеров;
- осуществлять контроль сроков действия сертификатов соответствия по требованиям безопасности информации на криптосредства;
- обеспечивать надежное хранение криптосредств, ключевых документов, резервных ключевых документов, эксплуатационной и технической документации к криптосредствам;
- вести учет сотрудников, допущенных к работе с криптосредствами;
- организовывать централизованное уничтожение (утилизацию) криптосредств, не пригодных для дальнейшего использования или надобность в использовании которых миновала;
- осуществлять контроль установки и ввода в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией;
- не разглашать третьим лицам информацию об используемых в учреждении криптосредствах, ключевых документах, резервных ключевых документах, местах их

установки и хранения, организации информационной безопасности, содержания эксплуатационной и технической документации к криптосредствам;

- контролировать соблюдение требований настоящего Руководства и условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- инициировать разбирательства по фактам нарушения правил использования криптосредств, нарушений информационной безопасности и участвовать в их проведении.

5. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

5.1. Пользователь криптосредств обязан:

- обеспечивать надежное хранение криптосредств, исключив доступ к ним третьих лиц, возможность компрометации криптосредств;

- соблюдать требования по использованию криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах, эксплуатационной и технической документации к криптосредствам, мерах защиты, местах установки и хранения криптосредств;

- осуществлять хранение криптосредств, ключевых документов, эксплуатационной и технической документации в хранилище (сейфе, металлическом шкафу). Доставать их из хранилища только при необходимости использования в работе;

- убирать криптосредство в хранилище при отсутствии необходимости его использования и по окончании рабочего дня;

- не оставлять бесконтрольно криптосредства на рабочих местах и в автоматизированных рабочих местах;

- не допускать снятия копий с ключевых документов;

- не допускать вывод ключевых документов на дисплей (монитор) или печатающее устройство (принтер, МФУ);

- не допускать записи на ключевой носитель посторонней информации;

- не допускать установки ключевых документов на другие автоматизированные рабочие места;

- сообщать о попытках третьих лиц получить сведения об используемых криптосредствах, ключевых документах, эксплуатационной и технической документации к криптосредствам директору учреждения, ответственному пользователю криптосредств;

- уведомлять директора учреждения, ответственного пользователя криптосредств о фактах утраты или порчи криптосредств, ключевых документов, эксплуатационной и технической документации к криптосредствам, ключей от помещений, хранилищ и о других фактах, которые могут привести к нарушению информационной безопасности;

- сдать криптосредства, эксплуатационную и техническую документацию к криптосредствам, ключевые документы ответственному пользователю криптосредств при увольнении или прекращении исполнения обязанностей, связанных с использованием криптосредств.

5.2. Пользователи криптосредств несут персональную ответственность за сохранность криптосредств и полученной документации.

6. ПОРЯДОК УЧЕТА И ВЫДАЧИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Ответственный пользователь криптосредств ведет журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее – журнал поэкземплярного учета), в который заносятся все получаемые от удостоверяющих центров криптосредства и документы, а также информация об изъятии и уничтожении криптосредств, форма журнала прилагается (приложение 1).

Единицей поэкземплярного учета ключевых документов считается носитель с ключевой информацией. Если один и тот же ключевой носитель многократно используется для записи ключевой информации, то его каждый раз следует регистрировать отдельно.

6.2. Ответственный пользователь криптосредств выдает пользователю криптосредств все необходимые для работы экземпляры криптосредств, при необходимости выдает эксплуатационную и техническую документацию и ключевые документы под расписку в журнале поэкземплярного учета. Делает отметку о выданных криптосредствах, эксплуатационной и технической документации.

7. РАЗМЕЩЕНИЕ, СПЕЦИАЛЬНОЕ ОБОРУДОВАНИЕ, ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕННЫ КРИПТОСРЕДСТВА ИЛИ ХРАНЯТСЯ КЛЮЧЕВЫЕ ДОКУМЕНТЫ К НИМ

7.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, ключевых документов.

7.2. Помещения, где установлены криптосредства или хранятся ключевые документы к ним, должны быть оборудованы средствами охранной и пожарной сигнализаций, препятствующими неконтролируемому проникновению в помещения.

7.3. Входные двери должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

7.4. По окончании рабочего дня помещения и установленные в них хранилища, должны быть закрыты. Находящиеся в пользовании ключи от кабинетов должны быть сданы сотрудникам службы режима учреждения.

8. ПОРЯДОК УНИЧТОЖЕНИЯ КРИПТОСРЕДСТВ

8.1. Крип토средства, непригодные для дальнейшего использования, или надобность в использовании которых миновала, уничтожаются (утилизируются).

8.2. Уничтожение ключевой информации может производиться путем физического уничтожения ключевого носителя, на котором она расположена, или путем стирания (разрушения) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

8.3. Ключевую информацию стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение

соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим криптосредствам, а также указаниями удостоверяющего центра.

8.4. Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

8.5. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

8.6. Факт уничтожения криптосредств оформляется актом (образец заполнения, приложение 2) и соответствующей записью в журнале поэкземплярного учета.

В акте указываются криптосредства, ключевые документы, резервные ключевые документы, эксплуатационная и техническая документация к криптосредствам, подлежащие уничтожению, их количество.

Исправления в акте не допускаются.

9. ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ

Сотрудники, допущенные к работе с криптосредствами, несут персональную ответственность за несоблюдение требований, указанных в настоящем руководстве, в соответствии с законодательством Российской Федерации.

Журнал поэкземплярного учета криптосредств, эксплуатационной
и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного о письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение 2
к Руководству

ОБРАЗЕЦ ЗАПОЛНЕНИЯ

АКТ уничтожения средств криптографической защиты информации

Комиссия

_____ полное наименование учреждения (организации)

в составе председателя:

_____ (должность, Фамилия И.О.)

и членов комиссии:

_____ (должность, Фамилия И.О.)

в соответствии с п. 8.6. Руководства по порядку использования и организации работы со средствами криптографической защиты информации, не содержащей сведений, составляющих государственную тайну в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца», утвержденного приказом учреждения от _____ № _____

составила настоящий акт о том, что средство криптографической защиты информации (далее - СКЗИ) «КриптоПро CSP» версии 4.0.9944 (серийные номера дистрибутивов 385C1-011143/**/*** и 385C2-011135/**/***) выведено из эксплуатации, удалено с автоматизированного рабочего места с помощью стандартных средств операционной системы и утилиты очистки следов установки продуктов «КриптоПро CSP» *cspclean.exe*.

Произведено уничтожение дистрибутива, эксплуатационной и технической документации к СКЗИ «КриптоПро CSP» версии 4.0.9944 путем физического уничтожения информации.

Настоящий акт составлен в 2-х экземплярах на 1 листе каждый.

Председатель комиссии: _____

Члены комиссии:

**Инструкция пользователя информационных
систем персональных данных в бюджетном учреждении социального
обслуживания Вологодской области «Социально-реабилитационный центр для
несовершеннолетних «Росток» города Череповца»
(далее – Инструкция)**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана для обеспечения защиты персональных данных в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – учреждение).

1.2. Персональные данные (ПДн) относятся к категории информации ограниченного распространения.

1.3. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (далее - ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.4. Работа с персональными данными строится на принципах:

- персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под подпись;
- контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. ОБЯЗАННОСТИ РАБОТНИКОВ, ИМЕЮЩИХ ДОСТУП К ПДн

2.1. Сотрудники (работники), получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных немедленно информировать непосредственного руководителя и лицо, ответственное за организацию обработки и защиты персональных данных в учреждении.

2.2. Персональные данные не подлежат разглашению (распространению).

Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3. В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, учреждения, в том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности учреждения, полученные в течение срока работы.

2.4. Работники при работе с персональными данными обязаны:

2.4.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

2.4.2. Выполнять требования ответственного за организацию обработки и защиты персональных данных, ответственного пользователя криптосредств, касающиеся защиты информации;

2.4.3. Знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;

2.4.4. Хранить в тайне свой пароль доступа в автоматизированную систему, либо ключевой носитель, а также информацию о системе защиты, установленной в ИСПДн;

2.4.5. Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

2.4.6. Контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления непосредственному руководителю, ответственному пользователю криптосредств в учреждении;

2.4.7. Немедленно ставить в известность непосредственного руководителя, ответственного пользователя криптосредств в учреждении;

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;

- при подозрении на факты совершения в его отсутствие попыток несанкционированного доступа (НСД) к защищенной ИСПДн;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

- в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов персонального компьютера (ПК) или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты;

- необходимости обновления программного обеспечения, антивирусных баз;

- модернизации аппаратных средств или изменении конфигурации ИСПДн;

- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

- резервном копировании информации и другое.

2.5. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

2.6. Компьютерное оборудование (персональный компьютер, ноутбук), используемое для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, не имеющими отношения к конкретно обрабатываемой информации работниками.

2.7. Запрещается:

- вынос компьютерного оборудования (персональный компьютер, ноутбук) на котором проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т.п. без согласования с ответственным пользователем криптосредств;

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения ограниченного распространения;

- использовать сведения ограниченного распространения при подготовке открытых публикаций, докладов, научных работ и т.д.;

- выполнять работы с документами ограниченного распространения на дому, выносить их из служебных помещений, копировать, фотографировать или производить выписки из таких документов без разрешения директора учреждения;

- накапливать ненужные для работы персональные данные;

- передавать или принимать без расписки документы ограниченного распространения;

- оставлять на рабочих столах, в столах и незакрытых сейфах, документы ограниченного распространения, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенной без присмотра свое компьютерное оборудование (персональный компьютер, ноутбук) не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры, для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt> и выбрать опцию <Завершение сеанса> или нажать комбинацию клавиш Win+L);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность непосредственного руководителя и ответственного пользователя криптосредств.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Пользователь информационной системы имеет право:

3.1. Знакомиться с документами, определяющими правила и порядок работы в информационной системе.

3.2. Вносить на рассмотрение предложения по совершенствованию работы, связанной с исполнением обязанностей в соответствии с настоящей инструкцией и функционированию информационной системы.

3.3. Требовать обеспечения организационно - технических условий, необходимых для исполнения обязанностей в соответствии с настоящей инструкцией.

4. ОТВЕТСТВЕННОСТЬ

Пользователь информационной системы несет ответственность:

4.1. За разглашение информации конфиденциального характера и персональных данных, нарушение порядка обращения с документами и машинными носителями информации и содержащими такую информацию, а также за нарушение режима защиты, обработки и порядка использования этой информации.

4.2. За нарушение функционирования информационной системы и компьютерного оборудования; оборудования, входящего в состав информационной системы, вследствие ненадлежащего исполнения своих обязанностей.

4.3. За несвоевременное уведомление непосредственного руководителя подразделения, ответственного за организацию обработки и защиты персональных данных, ответственности пользователя криптосредств в учреждении информации о случаях нарушения правил пользования ресурсами информационной системы и случаев несанкционированного доступа к информации, обрабатываемой в информационной системе.

4.4. За ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией - в пределах, установленных действующим законодательством Российской Федерации.

4.5. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных
данных в бюджетном учреждении социального обслуживания Вологодской
области «Социально-реабилитационный центр для несовершеннолетних «Росток»
города Череповца»

1. Настоящими правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее - учреждение) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие правила разработаны в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.

3. В настоящих правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в учреждении организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверки осуществляются лицом, ответственным за организацию обработки и защиты персональных данных в учреждении, либо комиссией, образуемой приказом директора учреждения. В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в учреждении проводятся в соответствии с ежегодно разрабатываемым Планом мероприятий по проведению внутреннего контроля деятельности учреждения или на основании поступившего в учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение семи рабочих дней с момента поступления соответствующего заявления.

7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

8. Должностное лицо, ответственное за организацию обработки персональных данных в учреждении, (комиссия) имеет право:

- запрашивать у сотрудников учреждения информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить директору учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить директору учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными должностному лицу, ответственному за организацию обработки персональных данных в учреждении, (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору учреждения докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

11. Директор учреждения, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Порядок обработки персональных данных без использования средств автоматизации в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца»
(далее – Порядок)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), постановления Правительства Российской Федерации от 15.09.2008 № 687 «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации в бюджетном учреждении социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – учреждение).

1.2. Обработка персональных данных (далее - ПД) считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПД, как использование, уточнение, распространение, уничтожение ПД в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека, при этом ПД могут быть, как извлеченными из информационной системы персональных данных (далее ИСПД) так и не связанными с ИСПД, но их обработка соответствует характеру действий, совершаемых с ПД с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск ПД, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях ПД.

1.3. Материальный носитель, содержащий ПД - материальный носитель (документы, книги и журналы учета, договоры, иные носители информации, содержащие ПД) с зафиксированной на нем в любой форме информацией, содержащей ПД субъектов ПД в виде текста, фотографии и (или) их сочетания.

1.4. С учетом большого объема (массовости) документов, содержащих персональные данные, и строго регламентированного порядка их хранения, пометка конфиденциальности на них не ставится.

1.5. Ответственным за реализацию мер, обеспечивающих в учреждении сохранность ПД и исключение несанкционированного к ним доступа, является лицо, ответственное за организацию и защиту обработки персональных данных в учреждении, назначаемое приказом директора учреждения.

1.6. Сотрудники учреждения, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе лица, осуществляющие такую обработку по договору с учреждением) должны быть проинформированы о факте обработки ими ПД, обработка которых осуществляется в учреждении без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами, а также локальными

нормативными актами учреждения, под подпись, по форме листа информирования согласно приложению 1 к настоящему Порядку.

2. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. ПД должны обособляться от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков).

2.2. При фиксации ПД на материальных носителях не допускается фиксации на одном материальном носителе ПД, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПД необходимо использовать отдельный материальный носитель для каждой из категорий.

2.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПД (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПД, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта ПД, источник получения ПД, сроки обработки ПД, перечень действий с ПД, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПД;

- типовая форма должна предусматривать поле, в котором субъект ПД может поставить отметку о своем согласии на обработку ПД, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПД;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПД, содержащихся в документе, имел возможность ознакомиться со своими ПД, содержащимися в документе, не нарушая нрав и законных интересов иных субъектов ПД;

- типовая форма должна исключать объединение полей, предназначенных для внесения ПД, цели обработки которых заведомо не совместимы.

2.4. Уничтожение или обезличивание части ПД, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПД с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.5. Уточнение ПД при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПД.

2.6. Непосредственный руководитель подразделения, в котором обрабатываются ПД, принимает все необходимые организационные и технические меры, исключающие возможность несанкционированного доступа к материальным носителям ПД лиц, не допущенных к их обработке. Материальные носители с ПД хранятся в запирающихся на ключ помещениях, металлических шкафах, имеющих запираемые блок-секции.

2.7. Хранение ПД субъекта может осуществляться не дольше, чем этого

требуют цели обработки, если иное не предусмотрено федеральными законами.

2.8. Помещениями, определяющими места хранения персональных данных граждан на бумажных носителях, являются: архив, кабинет отделения консультативной и методической помощи (по вопросам организации отдыха детей и их оздоровления), кабинеты отделения профилактики и безнадзорности несовершеннолетних, кабинеты отделения социальной реабилитации учреждения, кабинет юрисконсульта.

Помещениями, определяющими места хранения персональных данных сотрудников (работников), является кабинет специалиста по персоналу, специалиста по охране труда.

2.9. Места хранения материальных носителей ПД, обработка которых осуществляется в различных целях, расположены отдельно и определены приложением 2 к настоящему Порядку.

2.10. Перечень должностей сотрудников учреждения, осуществляющих обработку персональных данных без использования средств автоматизации, определен приложением 3 к настоящему Порядку.

3. ПОРЯДОК УНИЧТОЖЕНИЯ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПРИ ДОСТИЖЕНИИ ЦЕЛЕЙ ОБРАБОТКИ ИЛИ ПРИ НАСТУПЛЕНИИ ИНЫХ ЗАКОННЫХ ОСНОВАНИЙ

3.1. Материальные носители с ПД при достижении целей обработки, или при наступлении иных законных оснований (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению в соответствии с законодательством.

3.2. Уничтожение документов, содержащих ПД, осуществляется способом, не позволяющим в дальнейшем ознакомиться с ПД.

Отобранные к уничтожению материальные носители измельчаются механическим или ручным способом до степени, исключающей возможность прочтения текста, или сжигаются.

3.3. После уничтожения материальных носителей членами комиссии подписывается Акт об уничтожении материальных носителей, содержащих персональные данные, делается запись в журналах их учета и регистрации, а также в номенклатурах структурных подразделений проставляется соответствующая отметка.

4. ОБЯЗАННОСТИ РАБОТНИКА, ДОПУЩЕННОГО К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. При работе с материальными носителями, содержащими ПД, работник (сотрудник) обязан исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними (в том числе другими работниками своего структурного подразделения).

4.2. При выносе материальных носителей, содержащих ПД, за пределы помещения, в котором проводится обработка ПД, по служебной необходимости, работник и его непосредственный руководитель должен принять все возможные меры, исключающие утрату (утерю, хищение) таких материальных носителей.

4.3. При утрате (утере, хищении) документов, содержащих ПД, работник обязан немедленно доложить о таком факте своему непосредственному руководителю. Руководитель подразделения должен сообщить о факте утраты (утере, хищении) материальных носителей, содержащих ПД, ответственному за организацию

и защиту обработки персональных данных в учреждении.

По каждому такому факту назначается служебное расследование.

4.4. Ответственность за неисполнение или ненадлежащее выполнение требований настоящего Порядка возлагается на сотрудников (работников) и их непосредственных руководителей.

Приложение 1
к Порядку

**Уведомление о факте обработки персональных данных
без использования средств автоматизации**

Я, _____,
(фамилия, имя, отчество)
работающий(ая) в должности _____

(должность, наименование структурного подразделения)
проинформирован(а):

- о факте обработки мною персональных данных, обработка которых осуществляется в БУ СО ВО «СРЦН «Росток» г. Череповца (далее - Оператор) без использования средств автоматизации*;
- о категориях обрабатываемых персональных данных;
- о правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов власти, органов исполнительной власти субъектов Российской Федерации, а также локальными нормативными актами Оператора.

* Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Я предупрежден(а) о том, что в случае нарушения установленного законодательством Российской Федерации порядка сбора, хранения, использования или распространения персональных данных я несу ответственность, предусмотренную ст. 13.11 КоАП РФ «Нарушение законодательства Российской Федерации в области персональных данных».

(дата)

(подпись)

(расшифровка подписи)

**Места хранения материальных носителей
персональных данных при их обработке,
осуществляемой без использования средств автоматизации**

№ п/п	Персональные данные, обработка которых осуществляется без использования средств автоматизации	Место хранения	Должность ответственного сотрудника за обеспечение сохранности материальных носителей
1.	Обработка с целью оказания социальных услуг - персональные данные граждан, находящихся на социальном сопровождении, ТЖС	Металлические шкафы, находящиеся в помещениях № 29, 30, 31 в соответствии с экспликацией	Заведующий отделением профилактики безнадзорности несовершеннолетних
2.	Обработка с целью организации отдыха и оздоровления детей - персональные данные граждан.	Металлические шкафы, находящиеся в помещении № 10 в соответствии с экспликацией	Заведующий отделением консультативной и методической помощи
3.	Обработка с целью оказания социальных услуг - персональные данные несовершеннолетних, законных представителей (усыновителей), опекунов, поступивших в учреждение	Металлические шкафы, находящиеся в помещениях № 61, 62, 64 в соответствии с экспликацией	Заведующий отделением социальной реабилитации
4.	Обработка с целью оказания социально-правовых услуг - персональные данные граждан	Металлические шкафы, находящиеся в помещении № 21 в соответствии с экспликацией	Юрисконсульт
5.	Обработка с целью исполнения прав и обязанностей сторон трудовых отношений - персональные данные сотрудников (работников) учреждения, кандидатов	Металлические шкафы, находящиеся в помещениях № 59 в соответствии с экспликацией	Специалист по персоналу
6	Обработка с целью соблюдения трудового законодательства по вопросам медицинского обследования – персональные данные сотрудников учреждения	Металлические шкафы, находящиеся в помещениях № 15 в соответствии с экспликацией	Специалист по охране труда
7	Персональные данные граждан, сотрудников учреждения	Помещения № 4, 37 в соответствии с экспликацией	Архивариус

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ
сотрудников учреждения, осуществляющих обработку персональных данных
без использования средств автоматизации

1. Директор
2. Заместитель директора (по направлениям деятельности)
3. Заведующий отделением (по направлениям деятельности)
4. Специалист по персоналу
5. Экономист
6. Специалист по социальной работе (по направлениям деятельности)
7. Специалист по работе с семьей
8. Юрисконсульт
9. Специалист по охране труда
10. Архивариус
11. Документовед
12. Воспитатель
13. Младший воспитатель
14. Дежурный по режиму
15. Сторож-вахтер

ПОЛИТИКА

конфиденциальности персональных данных официального сайта бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца»

Настоящая Политика конфиденциальности персональных данных (далее – Политика конфиденциальности) действует в отношении всей информации, которую официальный сайт бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – «сайт», учреждение) расположенный на доменном имени rostok.gov35.ru (а также его субдоменах), может получить о Пользователе во время использования сайта (а также его субдоменов), его программ и его продуктов.

1. ОПРЕДЕЛЕНИЕ ТЕРМИНОВ

В настоящей Политике конфиденциальности используются следующие термины:

«Администрация сайта» (далее – Администрация) – уполномоченные сотрудники на управление сайтом, которые организуют и (или) осуществляют обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

«Обработка персональных данных» - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

«Конфиденциальность персональных данных» - обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

«Сайт» - это совокупность связанных между собой веб-страниц, размещенных в сети Интернет по уникальному адресу (URL): rostok.gov35.ru а также его субдоменах.

«Субдомены» - это страницы или совокупность страниц, расположенные на доменах третьего уровня, принадлежащие сайту, а также другие временные страницы, внизу которых указана контактная информация Администрации.

«Пользователь сайта» (далее Пользователь) – лицо, имеющее доступ к сайту, посредством сети Интернет и использующее информацию, материалы и продукты сайта.

«Cookies» — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя, который веб-клиент или веб-браузер каждый раз пересылает веб-серверу в HTTP-запросе при попытке открыть страницу соответствующего сайта.

«IP-адрес» — уникальный сетевой адрес узла в компьютерной сети, (Internet Protocol Address «адрес Интернет-протокола»), построенной на основе протоколов TCP/IP.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Использование сайта Пользователем означает согласие с настоящей Политикой конфиденциальности и условиями обработки персональных данных Пользователя.

2.2. В случае несогласия с условиями Политики конфиденциальности Пользователь должен прекратить использование сайта.

2.3. Настоящая Политика конфиденциальности применяется к сайту, не контролирует и не несет ответственность за сайты третьих лиц, на которые Пользователь может перейти по ссылкам, доступным на сайте.

2.4. Администрация не проверяет достоверность персональных данных, предоставляемых Пользователем.

3. ПРЕДМЕТ ПОЛИТИКИ КОНФИДЕНЦИАЛЬНОСТИ

3.1. Настоящая Политика конфиденциальности устанавливает обязательства Администрации по неразглашению и обеспечению режима защиты конфиденциальности персональных данных, которые Пользователь предоставляет по запросу Администрации при регистрации на сайте или при подписке на информационную e-mail рассылку.

3.2. Персональные данные, разрешённые к обработке в рамках настоящей Политики конфиденциальности, предоставляются Пользователем путём заполнения форм на сайте и включают в себя следующую информацию:

- фамилию, имя, отчество Пользователя;
- контактный телефон Пользователя;
- адрес электронной почты (e-mail)
- место жительства Пользователя (при необходимости)
- фотографию (при необходимости)

3.3. Защищает данные, которые автоматически передаются при посещении страниц:

- - IP адрес;
- - информация из cookies;
- - информация о браузере
- - время доступа;
- - реферер (адрес предыдущей страницы).

3.3.1. Отключение cookies может повлечь невозможность доступа к частям сайта, требующим авторизации.

3.3.2. Осуществляет сбор статистики об IP-адресах своих посетителей. Данная информация используется с целью предотвращения, выявления и решения технических проблем.

3.4. Любая иная персональная информация неоговоренная выше (история посещения, используемые браузеры, операционные системы и т.д.) подлежит

надежному хранению и нераспространению, за исключением случаев, предусмотренных в п. 5.2. настоящей Политики конфиденциальности.

4. ЦЕЛИ СБОРА ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ

Персональные данные Пользователя Администрация может использовать в целях:

- идентификации Пользователя, зарегистрированного на сайте для его дальнейшей авторизации;
- предоставления Пользователю доступа к персонализированным данным сайта;
- установления с Пользователем обратной связи, включая направление уведомлений, запросов, касающихся использования сайта, обработки запросов и заявок от Пользователя;
- определения места нахождения Пользователя для обеспечения безопасности, предотвращения мошенничества;
- подтверждения достоверности и полноты персональных данных, предоставленных Пользователем;
- создания учетной записи для использования частей сайта, если Пользователь дал согласие на создание учетной записи;
- уведомления Пользователя по электронной почте;
- предоставления Пользователю эффективной технической поддержки при возникновении проблем, связанных с использованием сайта;
- предоставления Пользователю с его согласия специальных предложений, новостной рассылки и иных сведений от имени сайта.

5. СПОСОБЫ И СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ

5.1. Обработка персональных данных Пользователя осуществляется без ограничения срока, любым законным способом, в том числе в информационных системах персональных данных с использованием средств автоматизации или без использования таких средств.

5.2. Персональные данные Пользователя могут быть переданы уполномоченным органам государственной власти Российской Федерации только по основаниям и в порядке, установленным законодательством Российской Федерации.

5.3. При утрате или разглашении персональных данных Администрация вправе не информировать Пользователя об утрате или разглашении персональных данных.

5.4. Администрация принимает необходимые организационные и технические меры для защиты персональной информации Пользователя от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий третьих лиц.

5.5. Администрация совместно с Пользователем принимает все необходимые меры по предотвращению убытков или иных отрицательных последствий, вызванных утратой или разглашением персональных данных Пользователя.

6. ПРАВА И ОБЯЗАННОСТИ СТОРОН

6.1. Пользователь вправе:

6.1.1. Принимать свободное решение о предоставлении своих персональных данных, необходимых для использования сайта, и давать согласие на их обработку.

6.1.2. Обновить, дополнить предоставленную информацию о персональных данных в случае изменения данной информации.

6.1.3. Пользователь имеет право на получение у Администрации информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами. Пользователь вправе требовать от Администрации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Для этого достаточно уведомить Администрацию по указанному E-mail адресу.

6.2. Администрация обязана:

6.2.1. Использовать полученную информацию исключительно для целей, указанных в разделе 4 настоящей Политики конфиденциальности.

6.2.2. Обеспечить хранение конфиденциальной информации в тайне, не разглашать без предварительного письменного разрешения Пользователя, а также не осуществлять продажу, обмен, опубликование, либо разглашение иными возможными способами переданных персональных данных Пользователя, за исключением п. 5.2 настоящей Политики Конфиденциальности.

6.2.3. Принимать меры предосторожности для защиты конфиденциальности персональных данных Пользователя согласно порядку, обычно используемого для защиты такого рода информации в существующем деловом обороте.

6.2.4. Осуществить блокирование персональных данных, относящихся к соответствующему Пользователю, с момента обращения или запроса Пользователя, или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных на период проверки, в случае выявления недостоверных персональных данных или неправомерных действий.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Администрация, не исполнившая свои обязательства, несёт ответственность за убытки, понесённые Пользователем в связи с неправомерным использованием персональных данных, в соответствии с законодательством Российской Федерации, за исключением случаев, предусмотренных пп. 5.2 и 7.2 настоящей Политики Конфиденциальности.

7.2. В случае утраты или разглашения Конфиденциальной информации Администрация не несёт ответственность, если данная конфиденциальная информация:

7.2.1. Стала публичным достоянием до её утраты или разглашения.

7.2.2. Была получена от третьей стороны до момента её получения Администрацией сайта.

7.2.3. Была разглашена с согласия Пользователя.

7.3. Пользователь несет полную ответственность за соблюдение требований законодательства Российской Федерации, в том числе законов о рекламе, о защите авторских и смежных прав, об охране товарных знаков и знаков обслуживания, но, не ограничиваясь перечисленным, включая полную ответственность за содержание и форму материалов.

7.4. Пользователь признает, что ответственность за любую информацию (в том числе, но, не ограничиваясь: файлы с данными, тексты и т. д.), к которой он может иметь доступ как к части сайта, несет лицо, предоставившее такую информацию.

7.5. Пользователь соглашается, что информация, предоставленная ему как часть сайта, может являться объектом интеллектуальной собственности, права на который

защищены и принадлежат другим Пользователям, партнерам или рекламодателям, которые размещают такую информацию на сайте.

Пользователь не вправе вносить изменения, передавать в аренду, передавать на условиях займа, продавать, распространять или создавать производные работы на основе такого содержания (полностью или в части), за исключением случаев, когда такие действия были письменно прямо разрешены собственниками такого содержания в соответствии с условиями отдельного соглашения.

7.6. В отношении текстовых материалов (статей, публикаций, находящихся в свободном публичном доступе на сайте) допускается их распространение при условии, что будет дана ссылка на источник.

7.7. Администрация не несет ответственности перед Пользователем за любой убыток или ущерб, понесенный Пользователем в результате удаления, сбоя или невозможности сохранения какого-либо содержания и иных коммуникационных данных, содержащихся на сайте или передаваемых через него.

7.8. Администрация не несет ответственности за любые прямые или косвенные убытки, произошедшие из-за: использования либо невозможности использования сайта, либо отдельных сервисов; несанкционированного доступа к коммуникациям Пользователя; заявления или поведение любого третьего лица на сайте.

7.9. Администрация не несет ответственность за какую-либо информацию, размещенную пользователем на сайте, включая, но, не ограничиваясь: информацию, защищенную авторским правом, без прямого согласия владельца авторского права.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. До обращения в суд с иском по спорам, возникающим из отношений между Пользователем и Администрацией, обязательным является предъявление претензии (письменного предложения или предложения в электронном виде о добровольном урегулировании спора).

8.2. Получатель претензии в течение 30 календарных дней со дня получения претензии, письменно или в электронном виде уведомляет заявителя претензии о результатах рассмотрения претензии.

8.3. При не достижении соглашения спор будет передан на рассмотрение Арбитражного суда.

8.4. К настоящей Политике конфиденциальности и отношениям между Пользователем и Администрацией применяется действующее законодательство Российской Федерации.

9. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

9.1. Администрация вправе вносить изменения в настоящую Политику конфиденциальности без согласия Пользователя.

9.2. Новая Политика конфиденциальности вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики конфиденциальности.

9.3. Все предложения или вопросы касательно настоящей Политики конфиденциальности следует сообщать на электронную почту, указанную в контактах на сайте.

ПОЛОЖЕНИЕ ОБ АНТИВИРУСНОЙ ЗАЩИТЕ
в бюджетном учреждении социального обслуживания «Социально-
реабилитационный центр для несовершеннолетних «Росток»
города Череповца»
(далее – Положение)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет требования к организации защиты средств информатизации от разрушающего воздействия компьютерных вирусов, порядок организации работ по антивирусной защите средств информатизации в бюджетном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее - учреждение), устанавливает ответственность пользователей и должностных лиц учреждения по антивирусной защите средств информатизации.

1.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

1.3. Средства антивирусной защиты информации устанавливаются на всех средствах вычислительной техники, используемых в учреждении.

1.4. К использованию в учреждении допускается только лицензионное антивирусное программное обеспечение в соответствии с требованиями действующего законодательства Российской Федерации.

2. ПОРЯДОК УСТАНОВКИ АНТИВИРУСНОГО
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1. Антивирусная защита средств информатизации учреждения осуществляется посредством специального антивирусного программного обеспечения.

2.2. Установка, настройка и регулярное обновление антивирусного программного обеспечения осуществляется бюджетным учреждением в сфере информационных технологий Вологодской области «Центр информационных технологий» (далее – БУ ИТ ВО ЦИТ), которому учреждением переданы обеспечивающие функции в сфере информационных технологий (оснащение программным обеспечением), в соответствии с правовыми актами Вологодской области.

2.3. Установка и настройка средств антивирусного программного обеспечения осуществляются в соответствии с эксплуатационной документацией, поставляемой в комплекте с ним.

2.4. Антивирусное программное обеспечение настраивается таким образом, чтобы обеспечить следующие условия:

– обязательный входной контроль на наличие программных вирусов во всех поступающих электронных носителях информации в автоматическом режиме;

- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов в автоматическом режиме;
- блокирование сетевых атак из сети «Интернет» в автоматическом режиме;

3. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

3.1. Пользователям, работающим со средствами информатизации учреждения, запрещается отключать средства антивирусной защиты информации во время работы.

3.2. Проведение мероприятий по антивирусной защите средств информатизации учреждения включает следующее:

- при загрузке персонального компьютера (ноутбука) в автоматическом режиме выполняется обновление антивирусных баз и проводится антивирусный контроль всех дисков и файлов персонального компьютера;
- периодическая проверка в автоматическом режиме на предмет отсутствия программных вирусов жестких магнитных дисков;
- обязательная проверка съемных носителей информации перед началом работы с ними;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

3.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках), необходимо провести внеплановую проверку средств информатизации учреждения (жестких магнитных дисков и съемных носителей информации) на наличие программных вирусов.

3.4. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан приостановить работу, сообщить об этом непосредственному руководителю и ответственному пользователю криптосредств в учреждении.

Ответственный пользователь криптосредств сообщает (подаёт заявку) об этом факте в БУ ИТ ВО «ЦИТ», которое проводит работу по удалению вируса и определяет возможность дальнейшего использования персонального компьютера.

МОДЕЛЬ УГРОЗ
безопасности персональных данных
информационных систем персональных данных
бюджетного учреждения социального обслуживания Вологодской области
«Социально-реабилитационный центр для несовершеннолетних «Росток»
города Череповца»

СОДЕРЖАНИЕ

Определения.....	3
Обозначения и сокращения.....	8
ВВЕДЕНИЕ.....	9
1. ОПИСАНИЕ АКТИВОВ, ПОТЕНЦИАЛЬНО ПОДВЕРЖЕННЫХ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	10
2. ОПИСАНИЕ КАНАЛОВ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	11
3. УРОВЕНЬ ИСХОДНОЙ СТЕПЕНИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	18
4. ОСНОВНЫЕ ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
5. ПЕРЕЧЕНЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	18
6. ОПИСАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	20

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в

ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой

системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанному в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки — электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» — комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных — лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка — код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить или модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие — несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

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

Ресурс информационной системы — именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники — совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации — совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящий документ разработан в рамках выполнения работ по защите информации в информационной системе бюджетного учреждения социального обслуживания Вологодской области «Социально-реабилитационный центр для несовершеннолетних «Росток» города Череповца» (далее – Учреждение).

Документ предназначен для уточнения методов и способов защиты информации, применяемых для обеспечения безопасности персональных данных при их обработке в рассматриваемой информационной системе персональных данных.

В результате предварительного обследования информационной системы определено:

- необходимость обработки персональных данных в информационной системе Учреждения;
- перечень персональных данных, подлежащих защите;
- условия расположения информационной системы (ее отдельных компонентов);
- конфигурация и топологии автоматизированной системы, систем связи в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- режим обработки персональных данных в информационной системе в целом и в отдельных компонентах;
- участие персонала в обработке персональных данных;
- угрозы безопасности персональных данных применительно к конкретным условиям функционирования информационной системы;
- класс информационной системы;
- уровень защищенности системы;

Документ разработан с учетом результатов проведенного предварительного обследования информационной системы и на основе документов:

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации №1119 от 1 ноября 2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.);
- Методика определения актуальных угроз безопасности персональных данных при их

обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.);

- Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости (утверждены директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23 декабря 2009 г.).

Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю над выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Настоящий документ подлежит периодическому пересмотру и актуализации с учетом изменений состава и условий функционирования информационной системы.

1. ОПИСАНИЕ АКТИВОВ, ПОТЕНЦИАЛЬНО ПОДВЕРЖЕННЫХ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основными активами, потенциально подверженными угрозам информационной безопасности в информационной системе Учреждения, являются информационные активы к которым, в свою очередь, относятся:

1. Целевая информация: персональные данные.
2. Технологическая информация:
 - защищаемая управляющая информация (конфигурационные файлы, настройки системы защиты и пр.);
 - защищаемая технологическая информация (аутентификационная информация и др.);
 - документация на средства защиты информации, на технические и программные компоненты;
 - информационные активы на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию информационной системы (программное обеспечение, конфигурационные файлы, настройки системы защиты и пр.).
3. Программное обеспечение:
 - программные информационные активы, содержащие общее и прикладное программное обеспечение, резервные копии программного обеспечения, программное обеспечение средств защиты информации.
4. Технические средства:

- основные технические средства и системы, осуществляющие обработку конфиденциальной информации (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно - цифровой информации);

вспомогательные технические средства и системы - технические средства и системы, их коммуникации, не предназначенные для обработки конфиденциальной информации, но размещенные в служебных помещениях, в которых производится обработка конфиденциальной информации (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, средства электронной оргтехники).

2. ОПИСАНИЕ КАНАЛОВ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учитывая результаты проведенной классификации информационных систем как информационных систем персональных данных (классы информационных систем Учреждения - ИСПДн - «Единая централизованная информационная система бюджетного (бухгалтерского) учета и отчетности Вологодской области «Смета»» класса КЗ (специальная, локальная, многопользовательская с разграничением прав доступа, не имеющая подключение к сетям связи общего пользования), ИСПДн «Электронный социальный регистр населения Вологодской области» (специальная, локальная, многопользовательская с разграничением прав доступа, не имеющая подключение к сетям связи общего пользования), «Банки данных семей и детей, находящихся на социальном сопровождении (специальная, локальная, многопользовательская, не имеющая подключение к сетям связи общего пользования)), предполагается, что значимыми каналами реализации угроз информационной безопасности являются:

- Побочные электромагнитные излучения и наводки от основных технических средств и систем;
- Акустические каналы;
- Визуально - оптические каналы;
- Материально-вещественные.

3. УРОВЕНЬ ИСХОДНОЙ СТЕПЕНИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Под уровнем исходной защищенности информационной системы понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик информационной системы.

Уровень исходной защищенности информационной системы применяется, как показатель

оценки возможности реализации угроз.

3.1 Параметры ИСПДн

В таблице 3.1 представлены характеристики уровня исходной защищенности для ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца»

Таблица 3.1 – Параметры ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца»

Структура ИСПДн	Локальная информационная система
Подключение ИСПДн к сетям общего пользования и (или) сетям международного информационного обмена	информационная система не имеет подключения к сетям связи общего пользования и/или сетям международного информационного обмена
Режим обработки ПДн	многопользовательский
Режим разграничения прав доступа пользователей	с разграничениями прав доступа
Местонахождение технических средств ИСПДн	в пределах Российской Федерации
Категория ПДн, обрабатываемых в ИСПДн	Иная категория ПД, обрабатывающая ПД сотрудников оператора
Объем ПДн, обрабатываемых в ИСПДн	Менее 1000
Заданные характеристики безопасности ПДн	специальная информационная система

В таблице 3.2 представлены характеристики уровня исходной защищенности для ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца».

Таблица 3.2 – Параметры ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца».

Структура ИСПДн	Локальная информационная система
Подключение ИСПДн к сетям общего пользования и (или) сетям международного информационного обмена	информационная система не имеет подключения к сетям связи общего пользования и/или сетям международного информационного обмена
Режим обработки ПДн	многопользовательский
Режим разграничения прав доступа пользователей	с разграничениями прав доступа
Местонахождение технических средств ИСПДн	в пределах Российской Федерации
Категория ПДн, обрабатываемых в ИСПДн	Специальная категория ПД

Объем ПДн, обрабатываемых в ИСПДн	Более 100000
Заданные характеристики безопасности ПДн	Специальная информационная система

3.2 Исходный уровень защищенности ИСПДн

В таблице 3.3 представлены характеристики ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца».

Таблица 3.3 – Характеристики ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца» .

Технические и эксплуатационные характеристики		Уровень защищенности
Позиции	Характеристики ИСПДн	
1. По территориальному размещению	локальная ИСПДн, развернутая в пределах одного здания	высокий
2. По наличию соединения с сетями общего пользования	ИСПДн, не имеющая выход в сеть общего пользования	высокий
3. По встроенным (легальным) операциям с записями баз персональных данных	запись, удаление, сортировка	средний
4. По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	База ПДн едина	средний
6. По уровню (обезличивания) ПДн	ИСПДн, в которых предоставляемые пользователю данные, не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	низкий
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

По итогам оценки характеристик ИСПДн было определено, что ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца» имеет средний уровень исходной защищенности.

В таблице 3.4 представлены характеристики ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца».

Таблица 3.4– Характеристики ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца».

Технические и эксплуатационные характеристики		Уровень защищенности
Позиции	Характеристики ИСПДн	
1. По территориальному размещению	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации	средний
2. По наличию соединения с сетями общего пользования	ИСПДн, не имеющая вход в сеть общего пользования	высокий
3. По встроенным (легальным) операциям с записями баз персональных данных	запись, удаление, сортировка	средний
4. По разграничению доступа к персональным данным	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	средний
5. По наличию соединений с другими базами ПДн иных ИСПДн	База ПДн едина	средний
6. По уровню (обезличивания) ПДн	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	средний
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	ИСПДн, предоставляющая часть ПДн	средний

По итогам оценки характеристик ИСПДн было определено, что ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца» имеет средний уровень исходной защищенности.

4. ОСНОВНЫЕ ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источниками угроз являются субъекты, действия которых нарушают характеристики безопасности активов информационной системы Учреждения. Этими субъектами могут быть нарушители информационной безопасности.

Под нарушителем здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности конфиденциальной информации при их обработке техническими средствами в информационной системе.

С точки зрения наличия права легального доступа в помещения, в которых размещены технические средства обработки конфиденциальной информации, обеспечивающие доступ к ресурсам информационной системы, выделяются два типа нарушителей:

- нарушители, не имеющие доступа к информационной системе, - внешние нарушители;
- нарушители, имеющие доступ к информационной системе, включая пользователей информационной системы, реализующие угрозы непосредственно в информационной системе, - внутренние нарушители.

5. ПЕРЕЧЕНЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

I. Угрозы утечки видовой информации

Угроза 1: Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных

Угроза 2: Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных

Угроза 3: Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных

II. Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.

Угроза 4: Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)

Угроза 5: Съём наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций

III. Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации

Угроза 6: Съём информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)

Угроза 7: Съём информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)

IV. Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации

Угроза 8: Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)

V. Угрозы, реализуемые при физическом доступе

Угроза 9: Кража ПЭВМ

Угроза 10: Вывод из строя узлов ПЭВМ, каналов связи

Угроза 11: Кража элементов (жесткий диск) ПЭВМ

Угроза 12: Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ

Угроза 13: Кража ключей от помещений, сейфов

Угроза 14: Кража носителей ключевой информации

Угроза 15: Кража индивидуальных устройств идентификации

VI. Угрозы, возникающие при использовании съемных носителей персональных данных

Угроза 16: Кража съемных носителей ПДн

Угроза 17: Использование не учтенных носителей ПДн

Угроза 18: Утрата съемных носителей ПДн

VII. Угрозы внедрения программных закладок

Угроза 19: Компьютерные вирусы

Угроза 20: Несанкционированная модификация или уничтожение защищаемой информации

Угроза 21: Несанкционированный перенос защищаемой информации на твердую копию

Угроза 22: Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн

Угроза 23: Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB- винчестер и т. д.)

Угроза 24: Несанкционированное отключение средств защиты

VIII. Угрозы несанкционированного доступа по каналам связи

Угроза 25: Перехват информации, передаваемой по локальной сети

Угроза 26: Перехват информации, передаваемой по сетям международного обмена

Угроза 27: Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.

Угроза 28: Подбор паролей через локальную вычислительную сеть организации или сети международного обмена

Угроза 29: Несанкционированный доступ через сети международного обмена

Угроза 30: Несанкционированный доступ через локальную вычислительную сеть организации

Угроза 31: Несанкционированный удаленный запуск приложений

Угроза 32: Подмена доверенного объекта сети

Угроза 33: Внедрение ложного объекта

Угроза 34: Навязывание ложного маршрута

IX. Угрозы непреднамеренных действий внутренних нарушителей

Угроза 35: Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке

Угроза 36: Непреднамеренное отключение средств защиты

Угроза 37: Утрата ключей от помещений, сейфов

Угроза 38: Утрата носителей ключевой информации

Угроза 39: Утрата индивидуальных устройств идентификации

Х. Угрозы неатропогенного характера

Угроза 40: Сбой системы электроснабжения

Угроза 41: Стихийное бедствие

6. ОПИСАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При описании угроз информационной безопасности необходимо учитывать вероятность реализации, возможность реализации и опасность угроз информационной безопасности.

Вероятность реализации угрозы считается:

- **маловероятной** в случае отсутствия объективных предпосылок для осуществления угрозы;
- **низкой** в случае присутствия объективных предпосылок для реализации угрозы и принятыми мерами, существенно затрудняющими реализацию угрозы;
- **средней** в случае присутствия объективных предпосылок для реализации угрозы и недостаточно принятыми мерами обеспечения безопасности конфиденциальной информации;
- **высокой** в случае присутствия объективных предпосылок для реализации угрозы и не принятыми мерами обеспечения безопасности конфиденциальной информации.

Возможность реализации угрозы зависит от вербальных показателей вероятности реализации угрозы и степени защищенности информационной системы и принимает следующие значения: низкая, средняя, высокая, очень высокая возможности.

Опасность угрозы считается:

- **низкая** (реализация угрозы не может привести к негативным последствиям для субъектов персональных данных);
- **средняя** (реализация угрозы может привести к негативным последствиям для субъектов персональных данных);
- **высокая** (реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных).

В информационной системе Учреждения опасность угроз информационной безопасности может принимать не все значения из вышеприведенных. Приняты и реализованы единые организационные требования по защите информационных систем персональных данных, вне зависимости от класса информационной системы и места ее расположения.

Описание угроз безопасности информационных систем персональных данных:

В таблице 6.1 представлены актуальные угрозы безопасности для ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца», а также способы их противодействия.

В таблице 6.2 представлены актуальные угрозы безопасности для ИСПДн ЕЦИС «Смета», а также способы их противодействия.

Таблица 6.1 – Модель угроз ИСПДн «Система персональных данных получателей социально-правовых услуг БУ СО ВО «СРЦН «Росток» г. Череповца»

Наименование угрозы	Уровень исходной защищенности	Опасность угрозы	Вероятность реализации угрозы	Актуальность угрозы	Рекомендации по противодействию угрозе	
					Технические	Организационные
Угрозы утечки видовой информации						
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	средний	низкая	средняя	актуальная		Рабочие места расположены специфично; Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	средний	низкая	низкая	не актуальна		Рабочие места расположены специфично; Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	средний	средняя	низкая	актуальная	Жалюзи;	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;

Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.						
Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации						
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Использование сетевых фильтров	
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	средний	низкая	низкая	Не актуальная	Экранирование и защита цепей заземления	

Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации						
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Защита помещений от проникновения высокочастотного излучения	Удаление от границ охраняемой территории;
Угрозы, реализуемые при физическом доступе						
Кража ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана	Охрана; Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Вывод из строя узлов ПЭВМ, каналов связи	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана;	Охрана; Обязанности администратора ИСПДн;
Кража элементов (жесткий диск) ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана;	Охрана; Инструкция пользователя ИСПДн; Инструкция ответственного за обработку ПДн
Несанкционированный доступ к информации при	средний	низкая	низкая	не актуальная		Порядок резервирования и восстановления работоспособности

техническом обслуживании (ремонте, модернизации) ПЭВМ						ТС и ПО, баз данных и СЗИ	
Кража ключей от помещений, сейфов	средний	средняя	низкая	актуальная		Охрана; Инструкция пользователя ИСПДн	
Угрозы, возникающие при использовании съемных носителей персональных данных							
Использование не учтенных носителей ПДн	средний	средняя	средняя	актуальная	Контроль доступа к внешним устройствам;	Инструкция администратора ИСПДн; Обязанности администратора ИСПДн;	
Угрозы внедрения программных закладок							
Компьютерные вирусы	средний	средняя	низкая	актуальная	Средства антивирусной защиты;	Инструкция об антивирусной защите	
Несанкционированная модификация или уничтожение защищаемой информации	средний	средняя	низкая	актуальная	Резервирование обрабатываемой информации;		
Несанкционированный перенос защищаемой информации на твердую копию	средний	средняя	низкая	актуальная	Регистрация печати конфиденциальных документов;		
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	средний	средняя	низкая	актуальная	Идентификация и аутентификация Контроль доступа к	Обязанности администратора ИСПДн;	

						информации, хранящейся в БД; Регистрация действий пользователей;	Разрешительная система доступа;
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB-винчестер и т. д.)	средний	низкая	маловероятно	не актуальная			
Несанкционированное отключение средств защиты	средний	низкая	маловероятно	не актуальная	Идентификация и аутентификация в СЗИ	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;	
Угрозы несанкционированного доступа по каналам связи							
Перехват информации, передаваемой по локальной сети	средний	низкая	низкая	актуальная			Инструкция пользователя ИСПДн;
Перехват информации, передаваемой по сетям международного обмена	средний	низкая	маловероятно	не актуальная			
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	средний	средняя	низкая	актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн;	

Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Несанкционированный доступ через сети международного обмена	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Internet трафика);	Обязанности администратора ИСПДн;
Несанкционированный доступ через локальную вычислительную сеть организации	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Ethernet трафика);	Обязанности администратора ИСПДн;
Несанкционированный удаленный запуск приложений	средний	низкая	низкая	не актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Подмена доверенного объекта сети	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн;
Внедрение ложного объекта	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн;
Навязывание ложного маршрута	средний	низкая	низкая	не актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн;

Угрозы непреднамеренных действий внутренних нарушителей						
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	средний	низкая	маловероятно	не актуальная	Резервирование обрабатываемой информации;	
Непреднамеренное отключение средств защиты	средний	низкая	маловероятно	не актуальная	Идентификация и аутентификация в СЗИ;	Инструкция пользователя ИСПДн;
Утрата ключей от помещений, сейфов	средний	низкая	низкая	не актуальная		Инструкция пользователя ИСПДн;
Угрозы неагропогенного характера						
Сбой системы электроснабжения	средний	средняя	низкая	актуальная	Источники бесперебойного питания; Резервирование обрабатываемой информации;	
Стихийное бедствие	средний	средняя	низкая	актуальная	Пожарная сигнализация;	

Таблица 6.2– Модель угроз ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г.Череповца».

Наименование угрозы	Уровень исходной защищенности	Опасность угрозы	Вероятность реализации угрозы	Актуальность угрозы	Рекомендации по противодействию угрозе	
					Технические	Организационные

Угрозы утечки видовой информации

Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	средний	низкая	средняя	актуальная	Рабочие места расположены специфично; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	средний	низкая	низкая	не актуальна	Рабочие места расположены специфично; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	средний	средняя	низкая	актуальная	Жалюзи; Инструкция пользователя ИСПДн;

Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.

Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Удаление от границ охраняемой территории;
---	---------	--------	--------	---------------	---

Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	средний	низкая	низкая	Не актуальная	Удаление от границ охраняемой территории;
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации					
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Использование сетевых фильтров
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	средний	низкая	низкая	Не актуальная	Экранирование и защита цепей заземления
Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации					
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Удаление от границ охраняемой территории; ; Защита помещений от проникновения высокочастотного излучения

Угрозы, реализуемые при физическом доступе						
Кража ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Инструкция пользователя ИСПДн;
Вывод из строя узлов ПЭВМ, каналов связи	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Обязанности администратора ИСПДн;
Кража элементов (жесткий диск) ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ	средний	низкая	низкая	не актуальная		Обязанности администратора ИСПДн;
Кража ключей от помещений, сейфов	средний	средняя	низкая	актуальная		Охрана; Инструкция пользователя ИСПДн;
Угрозы, возникающие при использовании съемных носителей персональных данных						
Использование не учтенных	средний	средняя	средняя	актуальная	Контроль доступа к	Обязанности администратора

носителей ПДн						внешним устройствам;	ИСПДн; Инструкция пользователя ИСПДн;
Угрозы внедрения программных закладок							
Компьютерные вирусы	средний	средняя	низкая	актуальная	Средства антивирусной защиты	Положение об антивирусной защите	
Несанкционированная модификация или уничтожение защищаемой информации	средний	средняя	низкая	актуальная	Резервирование обрабатываемой информации; Регистрация действий пользователей;		
Несанкционированный перенос защищаемой информации на твердую копию	средний	средняя	низкая	актуальная	Регистрация печати конфиденциальных документов;		
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	средний	средняя	низкая	актуальная	Идентификация и аутентификация; Контроль доступа к информации, хранящейся в ПЭВМ; Контроль доступа к информации, хранящейся в БД; Регистрация действий	Обязанности администратора ИСПДн; Разрешительная система доступа;	

						пользователей;	
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB-винчестер и т. д.)	средний	низкая	маловероятно	актуальная	Обязанности администратора ИСПДн;		
Несанкционированное отключение средств защиты	средний	низкая	маловероятно	актуальная	Идентификация и аутентификация в СЗИ	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;	
Угрозы несанкционированного доступа по каналам связи							
Перехват информации, передаваемой по локальной сети	средний	низкая	низкая	не актуальная		Инструкция пользователя ИСПДн;	
Перехват информации, передаваемой по сетям международного обмена	средний	низкая	маловероятно	не актуальная			
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	средний	средняя	низкая	актуальная		Инструкция пользователя ИСПДн;	
Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;	

Несанкционированный доступ через сети международного обмена	средний	средний	средний	актуальная	Обязанности администратора ИСПДн
Несанкционированный доступ через локальную вычислительную сеть организации	средний	средний	средний	актуальная	Обязанности администратора ИСПДн
Несанкционированный удаленный запуск приложений	средний	низкая	низкая	актуальная	Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Подмена доверенного объекта сети	средний	средний	средний	актуальная	Инструкция пользователя ИСПДн;
Внедрение ложного объекта	средний	низкий	низкий	актуальная	Инструкция пользователя ИСПДн;
Навязывание ложного маршрута	средний	низкая	низкая	актуальная	Инструкция пользователя ИСПДн;
Угрозы непреднамеренных действий внутренних нарушителей					
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	средний	низкая	маловероятно	не актуальная	Резервное копирование обрабатываемой информации
Непреднамеренное отключение средств защиты	средний	низкая	маловероятно	актуальная	Идентификация и аутентификация в СЗИ Инструкция пользователя ИСПДн;

Утрата ключей от помещений, сейфов	средний	низкая	низкая	не актуальная		Инструкция пользователя ИСПДн;
Угрозы неагропогенного характера						
Сбой системы электроснабжения	средний	средняя	низкая	актуальная	Источники бесперебойного питания; Резервирование обрабатываемой информации;	
Стихийное бедствие	средний	средняя	низкая	актуальная	Пожарная сигнализация	

Таблица 6.2 – Модель угроз ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г. Череповца».

Наименование угрозы	Уровень исходной защищенности	Опасность угрозы	Вероятность реализации угрозы	Актуальность угрозы	Рекомендации по противодействию угрозе	
					Технические	Организационные
Угрозы утечки видовой информации						
Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	средний	низкая	средняя	актуальная		Рабочие места расположены специфично; Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	средний	низкая	низкая	не актуальна		Рабочие места расположены специфично; Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	средний	средняя	низкая	актуальная	Жалюзи;	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;

Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.						
Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации						
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Использование сетевых фильтров	
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	средний	низкая	низкая	Не актуальная	Экранирование и защита цепей заземления	

Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации						
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Защита помещений от проникновения высокочастотного излучения	Удаление от границ охраняемой территории;
Угрозы, реализуемые при физическом доступе						
Кража ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана	Охрана; Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Вывод из строя узлов ПЭВМ, каналов связи	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана;	Охрана; Обязанности администратора ИСПДн;
Кража элементов (жесткий диск) ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Круглосуточная охрана;	Охрана; Инструкция пользователя ИСПДн; Инструкция ответственного за обработку ПДн
Несанкционированный доступ к информации при	средний	низкая	низкая	не актуальная		Порядок резервирования и восстановления работоспособности

техническом обслуживании (ремонт, модернизации) ПЭВМ							ТС и ПО, баз данных и СЗИ
Кража ключей от помещений, сейфов	средний	средняя	низкая	актуальная			Охрана; Инструкция пользователя ИСПДн
Угрозы, возникающие при использовании съемных носителей персональных данных							
Использование не учтенных носителей ПДн	средний	средняя	средняя	актуальная	Контроль доступа к внешним устройствам;	Инструкция администратора ИСПДн; Обязанности администратора ИСПДн;	
Угрозы внедрения программных закладок							
Компьютерные вирусы	средний	средняя	низкая	актуальная	Средства антивирусной защиты;	Инструкция об антивирусной защите	
Несанкционированная модификация или уничтожение защищаемой информации	средний	средняя	низкая	актуальная	Резервирование обрабатываемой информации;		
Несанкционированный перенос защищаемой информации на твердую копию	средний	средняя	низкая	актуальная	Регистрация печати конфиденциальных документов;		
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	средний	средняя	низкая	актуальная	Идентификация и аутентификация Контроль доступа к	Обязанности администратора ИСПДн;	

						информации, хранящейся в БД; Регистрация действий пользователей;	Разрешительная система доступа;
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB-винчестер и т. д.)	средний	низкая	маловероятно	не актуальная			
Несанкционированное отключение средств защиты	средний	низкая	маловероятно	не актуальная	Идентификация и аутентификация в СЗИ	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;	
Угрозы несанкционированного доступа по каналам связи							
Перехват информации, передаваемой по локальной сети	средний	низкая	низкая	актуальная			Инструкция пользователя ИСПДн;
Перехват информации, передаваемой по сетям международного обмена	средний	низкая	маловероятно	не актуальная			
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	средний	средняя	низкая	актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн;	

Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Несанкционированный доступ через сети международного обмена	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Internet трафика);	Обязанности администратора ИСПДн;
Несанкционированный доступ через локальную вычислительную сеть организации	средний	средний	средний	актуальная	Межсетевое экранирование (контроль Ethernet трафика);	Обязанности администратора ИСПДн;
Несанкционированный удаленный запуск приложений	средний	низкая	низкая	не актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Подмена доверенного объекта сети	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн;
Внедрение ложного объекта	средний	средний	средний	актуальная		Инструкция пользователя ИСПДн;
Навязывание ложного маршрута	средний	низкая	низкая	не актуальная	Межсетевое экранирование (контроль Internet трафика);	Инструкция пользователя ИСПДн;

Угрозы непреднамеренных действий внутренних нарушителей						
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	средний	низкая	маловероятно	не актуальная	Резервирование обрабатываемой информации;	
Непреднамеренное отключение средств защиты	средний	низкая	маловероятно	не актуальная	Идентификация и аутентификация в СЗИ;	Инструкция пользователя ИСПДн;
Утрата ключей от помещений, сейфов	средний	низкая	низкая	не актуальная		Инструкция пользователя ИСПДн;
Угрозы неагропогенного характера						
Сбой системы электроснабжения	средний	средняя	низкая	актуальная	Источники бесперебойного питания; Резервирование обрабатываемой информации;	
Стихийное бедствие	средний	средняя	низкая	актуальная	Пожарная сигнализация;	

Таблица 6.2– Модель угроз ИСПДн «Система персональных данных работников БУ СО ВО «СРЦН «Росток» г. Череповца».

Наименование угрозы	Уровень исходной защищенности	Опасность угрозы	Вероятность реализации угрозы	Актуальность угрозы	Рекомендации по противодействию угрозе	
					Технические	Организационные

Угрозы утечки видовой информации

Просмотр информации, отображаемой на дисплее монитора сотрудниками, не допущенными к обработке персональных данных	средний	низкая	средняя	актуальная		Рабочие места расположены специфично; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися в помещении, в котором ведется обработка персональных данных	средний	низкая	низкая	не актуальна		Рабочие места расположены специфично; Инструкция пользователя ИСПДн;
Просмотр информации, отображаемой на дисплее монитора посторонними лицами, находящимися за пределами помещения, в котором ведется обработка персональных данных	средний	средняя	низкая	актуальная	Жалюзи;	Инструкция пользователя ИСПДн;

Угрозы утечки информации по каналам ПЭМИН. Электромагнитные каналы утечки информации.

Перехват побочных электромагнитных излучений элементов основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
---	---------	--------	--------	---------------	--	---

Съем наводок побочных электромагнитных излучений основных технических средств и систем (ОТСС) с линий связи, технических средств и систем коммуникаций	средний	низкая	низкая	Не актуальная		Удаление от границ охраняемой территории;
Угрозы утечки информации по каналам ПЭМИН. Электрические каналы утечки информации						
Съем информационных сигналов с линий электропитания основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	Использование сетевых фильтров	
Съем информационных сигналов с цепей заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС)	средний	низкая	низкая	Не актуальная	Экранирование и защита цепей заземления	
Угрозы утечки информации по каналам ПЭМИН. Параметрические каналы утечки информации						
Перехват информации путем "высокочастотного облучения" основных технических средств и систем (ОТСС)	средний	низкая	низкая	Не актуальная	; Защита помещений от проникновения высокочастотного излучения	Удаление от границ охраняемой территории;

Угрозы, реализуемые при физическом доступе						
Кража ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Инструкция пользователя ИСПДн;
Вывод из строя узлов ПЭВМ, каналов связи	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Обязанности администратора ИСПДн;
Кража элементов (жесткий диск) ПЭВМ	средний	низкая	низкая	не актуальная	Дверной замок; Охранная сигнализация;	Охрана; Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Несанкционированный доступ к информации при техническом обслуживании (ремонте, модернизации) ПЭВМ	средний	низкая	низкая	не актуальная		Обязанности администратора ИСПДн;
Кража ключей от помещений, сейфов	средний	средняя	низкая	актуальная		Охрана; Инструкция пользователя ИСПДн;
Угрозы, возникающие при использовании съемных носителей персональных данных						
Использование не учтенных	средний	средняя	средняя	актуальная	Контроль доступа к	Обязанности администратора

носителей ПДн							внешним устройствам;	ИСПДн; Инструкция пользователя ИСПДн;
Угрозы внедрения программных закладок								
Компьютерные вирусы	средний	средняя	низкая	актуальная	Средства антивирусной защиты	Положение об антивирусной защите		
Несанкционированная модификация или уничтожение защищаемой информации	средний	средняя	низкая	актуальная	Резервирование обрабатываемой информации; Регистрация действий пользователей;			
Несанкционированный перенос защищаемой информации на твердую копию	средний	средняя	низкая	актуальная	Регистрация печати конфиденциальных документов;			
Несанкционированный доступ внешних нарушителей к ресурсам ИСПДн	средний	средняя	низкая	актуальная	Идентификация и аутентификация; Контроль доступа к информации, хранящейся в ПЭВМ; Контроль доступа к информации, хранящейся в БД; Регистрация действий	Обязанности администратора ИСПДн; Разрешительная система доступа;		

						пользователей;		
Загрузка ОС с внешних носителей (CD, DVD, USB Flash, внешний USB-винчестер и т. д.)	средний	низкая	маловероятно	актуальная			Обязанности администратора ИСПДн;	
Несанкционированное отключение средств защиты	средний	низкая	маловероятно	актуальная		Идентификация и аутентификация в СЗИ	Обязанности администратора ИСПДн; Инструкция пользователя ИСПДн;	
Угрозы несанкционированного доступа по каналам связи								
Перехват информации, передаваемой по локальной сети	средний	низкая	низкая	не актуальная			Инструкция пользователя ИСПДн;	
Перехват информации, передаваемой по сетям международного обмена	средний	низкая	маловероятно	не актуальная				
Сканирование, направленное на выявление типа ОС, открытых портов и служб, открытых соединений и др.	средний	средняя	низкая	актуальная			Инструкция пользователя ИСПДн;	
Подбор паролей через локальную вычислительную сеть организации или сети международного обмена	средний	средний	средний	актуальная			Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;	

Несанкционированный доступ через сети международного обмена	средний	средний	средний	актуальная	Обязанности администратора ИСПДн
Несанкционированный доступ через локальную вычислительную сеть организации	средний	средний	средний	актуальная	Обязанности администратора ИСПДн
Несанкционированный удаленный запуск приложений	средний	низкая	низкая	актуальная	Инструкция пользователя ИСПДн; Обязанности администратора ИСПДн;
Подмена доверенного объекта сети	средний	средний	средний	актуальная	Инструкция пользователя ИСПДн;
Внедрение ложного объекта	средний	низкий	низкий	актуальная	Инструкция пользователя ИСПДн;
Навязывание ложного маршрута	средний	низкая	низкая	актуальная	Инструкция пользователя ИСПДн;
Угрозы непреднамеренных действий внутренних нарушителей					
Непреднамеренная модификация или уничтожение информации сотрудниками, допущенными к ее обработке	средний	низкая	маловероятно	не актуальная	Резервное копирование обрабатываемой информации
Непреднамеренное отключение средств защиты	средний	низкая	маловероятно	актуальная	Идентификация и аутентификация в СЗИ
					Инструкция пользователя ИСПДн;

Утрата ключей от помещений, сейфов	средний	низкая	низкая	не актуальная		Инструкция пользователя ИСПДн;
Угрозы неагропогенного характера						
Сбой системы электроснабжения	средний	средняя	низкая	актуальная	Источники бесперебойного питания; Резервирование обрабатываемой информации;	
Стихийное бедствие	средний	средняя	низкая	актуальная	Пожарная сигнализация	