МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
ГОРОДА ТЮМЕНИ
«ЦЕНТР КУЛЬТУРЫ И ТВОРЧЕСТВА «ТЮМЕНЬ»

ул. 50 лет Октября, 82, корпус 2, г.Тюмень, 625013; тел./факс: (3452) 41-12-55; E-mail: tzkit@obl72.ru;
ОКПО 95843474; ОГРН 1067203329160; ИНН/КПП 7202150964/720301001

№_____ от_____ на_____ от_____

П Р И К А З

«01» апреля 2025 г. № 37-ОД-р

Об организации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных муниципального учреждения культуры города Тюмени «ЦКиТ «Тюмень»

Во исполнение Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», в рамках реализации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных,

ПРИКАЗЫВАЮ:

1. Утвердить:
   1.1. Положение об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных МАУК «ЦКиТ «Тюмень» (Приложение №1).
   1.2. Перечень ИСПДн в МАУК «ЦКиТ «Тюмень» (Приложение №2).
   1.3. Перечень организаций, которым передаются ПДн МАУК «ЦКиТ «Тюмень» (Оператор) (Приложение №3).
   1.4. Инструкцию администратора информационной безопасности (Приложение №4).
   1.5. Инструкцию пользователя ИСПДн (Приложение №5).
2. Предоставить права администратора в ИСПДн МАУК «ЦКиТ «Тюмени» следующим сотрудникам:

- Заместителю директора Коваленко Надежде Дмитриевне

- Главному бухгалтеру Овсянниковой Наталье Викторовне
- Начальнику отдела кадровой политики Баевой Елене Владимировне

3. Назначить администратором информационной безопасности ИСПДн МАУК «ЦКиТ «Тюмень» Шумкова Юрия Александровича.
4. Администратору безопасности информации в своей деятельности руководствоваться инструкцией администратора безопасности информации.
5. Помощника директора Гайнутдинову Н.Н. ознакомить работников, перечисленных в п. 2 настоящего приказа, под роспись.
6. Заместителя директора Коваленко Н.Д. ознакомить всех сотрудников, которые являются пользователями ИСПДн, с Инструкцией пользователя ИСПДн.
7. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Трифонов С.В.

Приложение №1

УТВЕРЖДЕНО
Приказом директора
МАУК «ЦКиТ «Тюмень»
от « 01 » апреля 2025 г. № 37-ОД-Ф

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных, обрабатываемых в информационных системах Муниципального автономного учреждения культуры города Тюмени «Центр культуры и творчества «Тюмень»

1. Общие положения

1.1. Данное Положение об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных в Муниципальном автономном учреждении культуры города Тюмени «Центр культуры и творчества «Тюмень» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).
1.2. Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации а также порядок обезличивания ПДн.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации

Настоящий порядок определяет действия персонала муниципального автономного учреждения культуры города Тюмени «ЦКиТ «Тюмень» (далее – Учреждение) в части обеспечения безопасности ПДн при их обработке в ИСПДн.
2.1. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн заведующим Учреждения назначается администратор информационной безопасности, который также осуществляет контроль за выполнением необходимых мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн.
2.2. Администратор информационной безопасности ведет перечень ИСПДн Учреждения. Перечень ИСПДн утверждается заведующим Учреждения.
2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.
2.5. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.
2.6. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;
- выполнять требования по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;

2.7. Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;
- вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

2.8. Лицо, ответственное за защиту персональных данных в МАДОУ д/с №? г. Тюмени - Администратор информационной безопасности – физическое лицо, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации, определяющий уровень доступа и ответственность лиц, участвующих в обработке ПДн, отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн в подразделениях. Назначается приказом заведующим Учреждения.

2.9. Администратор информационной безопасности (при его отсутствии замещающее его лицо) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;
- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:
  - реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
  - вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;
  - своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
  - контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;
  - проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
  - контролировать своевременное (не реже чем один раз в год) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
  - обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
  - осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
  - настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
  - сопровождать подсистемы обеспечения целостности информации в ИСПДн;
  - периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
  - восстанавливать программную среду, программные средства и настройки СЗИ при сбоях совместно с лицами, ответственными за техническое обеспечение;
  - периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:
    - ✓ проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
    - ✓ сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;
    - ✓ контролировать соответствие документально утвержденного состава

аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;
- ✓ обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);
- ✓ присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- ✓ поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;
- ✓ в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать заведующему Учреждения о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.10. Администратор информационной безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.2. Резервному копированию подлежат базы данных ПДн, а также прикладное программное обеспечение, предназначенное для работы с этими базами данных в случае, если оно подвергается модификации со стороны разработчиков ИСПДн.

3.3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере.

3.4. Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других ИСПДн, хранящихся на сервере, при отсутствии допуска к работе в этих ИСПДн.

3.5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.

3.6. Раз в месяц администратор информационной безопасности создает резервную копию баз данных и программного обеспечения ИСПДн на отчуждаемый носитель, хранящийся у администратора информационной безопасности в закрывающемся на ключ хранилище.

3.7. Резервное копирование баз данных на файловый сервер должно осуществляться еженедельно администратором информационной безопасности.

3.8. Восстановление программного обеспечения производится путем его инсталляции с

использованием эталонных дистрибутивов либо полного восстановления системы с образа диска.
3.9. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению. Работа с использованием неисправных технических средств запрещается.
3.10. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.
3.11. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.
3.12. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств на отчуждаемый носитель.
3.13. Ответственность за проведение резервного копирования ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИСПДн.

4. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации.

5.1. Пользователи должны продемонстрировать администратору информационной безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор информационной безопасности должен вести список пользователей, допущенных к информационным системам персональных данных.
5.2. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.
5.3. Рекомендуется прохождение администратором информационной безопасности специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

6. Правила антивирусной защиты

6.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства.
6.2. Установка, начальная настройка и удаление средств антивирусного контроля на

компьютерах осуществляется администратором информационной безопасности.
6.3. Администратор информационной безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.
6.4. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.
6.5. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.
Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).
Настройку средств антивирусной защиты выполняет администратор информационной безопасности.
Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
6.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.
6.7. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.
6.8. 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 и т.п.) пользователь самостоятельно (или вместе с администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.
В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:
- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.
6.9. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора информационной безопасности.
6.10. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора информационной безопасности и всех пользователей данной ИСПДн.

7. Правила парольной защиты и доступа к информации к ИСПДн

7.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.
7.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.
7.3. Личные пароли должны создаваться пользователями объекта вычислительной техники самостоятельно.;

- при смене пароля новое значение должно отличаться от предыдущих;

- пользователь не имеет права сообщать личный пароль другим лицам.

7.4. Все пароли Учреждения заносятся в базу данных паролей, распределяясь по подразделениям, администратором информационной безопасности в день создания или смены пароля.
7.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.
7.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.
7.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) администратора информационной безопасности.
7.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.
7.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора информационной безопасности.
7.10. Доступ к базе данных на сервере Srv /Asrock core i5 , 800 Гб, осуществляется администратором информационной безопасности через учетные пользовательские записи.
7.11. Доступ к информации (файлам, папкам и др. материалам), расположенной на сервере, открывается администратором информационной безопасности. Перечень информации (файлам, папкам и др. материалам), к которой необходимо открыть доступ зависит от занимаемой должности пользователя. Перечень информации, к которой предоставляется доступ в зависимости от занимаемой должности утверждается приказом заведующего Учреждения.
7.12. Удаленный доступ пользователям осуществляется при помощи программ AnyDesk и TeamViewer.

8. Правила обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн

8.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.
8.2. Все изменения программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, должны производиться администратором информационной безопасности на основании заявки администратора ИСПДн, направляемой ответственному за обработку персональных данных.
8.3. Изменение конфигурации программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников ***запрещено***.
8.4. Процедура внесения изменений в конфигурацию программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, инициируется заявкой администратора ИСПДн.
8.5. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);
- обновление(замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения

определенной задачи программ);

- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

8.6. Заявку администратора ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается администратору информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке самостоятельно или с привлечением сотрудников, ответственных за техническое обеспечение учреждения.

8.7. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности.

8.8. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт-дисков и т.п.), прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

8.9. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также на совместимость с установленным программным обеспечением и операционной системой.

8.10. После установки (обновления) ПО, администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера, проверить работоспособность ПО и правильность их настройки.

8.11. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта администратор информационной безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

9. Управление учетными записями пользователей

9.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

9.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.9.5, ***запрещена.***

9.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой администратора ИСПДн.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;

- имя пользователя (учетной записи) данного сотрудника;

- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

9.4. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн.
9.5. После получения утвержденной заявки администратор информационной безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в заявке. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в год.

10. Порядок контроля соблюдения условий использования средств защиты информации

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).
10.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.
10.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором информационной безопасности.
10.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за обработку персональных данных;
- администратор информационной безопасности.

10.5. Пользователю ИСПДн категорически запрещается:

- отключать СЗИ;
- производитьобработку конфиденциальной информации в случае неработоспособности средств ее защиты (СЗИ);
- менять настройки СЗИ.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения

11.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.
11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.
Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается заведующим Учреждения и передаётся на пост охраны.
11.3. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в сейф (металлический шкаф).
11.4. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время организация, осуществляющая охрану Учреждения, сообщает о случившемся заведующему хозяйством, или ответственному лицу, который сдавал Учреждение на пульт охраны.
11.5. Помещения вскрываются заведующим хозяйством или ответственным лицом, который сдал офис на пульт охраны в присутствии представителя организации, осуществляющей охрану Учреждения с составлением акта.

12. Порядок стирания защищаемой информации и уничтожения носителей

защищаемой информации

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.
12.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).
12.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.
12.4. Бумажные и прочие сгораемые носители уничтожают путем сжигания или с помощью любых бумагорезательных машин.
12.5. По факту уничтожения или стирания носителей составляется акт.
12.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: администраторы ИСПДн, ответственный за обработку в ИСПДн, администратор информационной безопасности.

13. Обезличивание персональных данных

13.1. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных
13.2. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
13.3. Способы обезличивания при условии дальнейшей обработки персональных данных:
- метод введения идентификаторов;
- метод изменения состава или семантики;
- обобщение (понижение точности некоторых сведений);
- метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

13.4. Для обезличивания персональных данных используются способы обезличивания, определенные приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» в соответствии с рекомендациями по использованию этих методов.
13.5. Решение о необходимости обезличивания персональных данных принимает руководитель Организации.
13.6. Руководители подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных,

обоснование такой необходимости и способ обезличивания.

13.7. Сотрудники подразделений, обслуживающих базы данных с персональными данными, осуществляют непосредственное обезличивание выбранным способом.

13.8. Порядок работы с обезличенными персональными данными:

13.8.1. Обезличенные персональные данные не подлежат разглашению.

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

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

Приложение №2
к приказу от 01.04.2025 № 37-ОД-8

Перечень ИСПДн в МАУК «ЦКиТ «Тюмень»

Название ИСПДн	Местонахождение (место доступа)	Наличие подключений к СООП и сетям МИО (Интернет)	Режим обработки ПДн	Разграничение доступа пользователей	Размещение ресурса	Заводской (инв.) номер ПЭВМ, за которым работает сотрудник
1С: ЗиКГУ 3.1	Каб №204, каб №205	Имеется	Многопользовательский	С разграничением прав пользования	ПО	
1С:БГУ 2.0	КАБ №205, КАБ №206	Имеется	Многопользовательский	С разграничением прав пользования	ПО	
БАРС. МОНИТОРИНГ. КУЛЬТУРА	Каб №204, КАБ №205, КАБ №206	Имеется	Многопользовательский	С разграничением прав пользования	Web - клиент	
Клиент-Банк	КАБ №205, КАБ №206	Имеется	Многопользовательский	С разграничением прав пользования	Web – клиент	
СБИС	Каб №204, КАБ №205, КАБ №206	Имеется	Многопользовательский	С разграничением прав пользования	Web - клиент	

Приложение №3
к приказу от 01.04.2025 № 37-ОД-8

Перечень организаций, которым передаются ПДн МАУК «ЦКиТ «Тюмень» (Оператор)

№ п/п	Перечень организаций, которым Оператор передает ПДн	Способ передачи ПДн	Перечень передаваемых ПДн	Основания для передачи ПДн
1	ПАО «Сбербанк» Адрес: индекс, город, улица, дом	Персональные данные вносятся в реестры банка. Потом реестры с помощью программы Клиент Банк подписываются электронной подписью и передаются с использованием сети Интернет непосредственно в ПАО «Сбербанк» для перечисления сотрудникам заработной платы на банковскую карточку (передача ПДн происходит по мере необходимости) согласно Законодательству РФ	- Фамилия, - Имя, - Отчество, - Дата рождения, - Лицевой счет в банке, - размер заработной платы -паспортные данные	1. Договор между МАУК «ЦКиТ «Тюмень» 2. Согласие субъекта на передачу ПДн
2	ПАО «ВТБ» Адрес: индекс, город, улица, дом	Персональные данные вносятся в реестры банка. Потом реестры с помощью программы Клиент Банк подписываются электронной подписью и передаются с использованием сети Интернет непосредственно в ПАО «ВТБ» для перечисления сотрудникам заработной платы на банковскую карточку (передача ПДн происходит по мере необходимости) согласно Законодательству РФ	- Фамилия, - Имя, - Отчество, - Дата рождения, - Лицевой счет в банке, - размер заработной платы -паспортные данные	1. Договор между МАУК «ЦКиТ «Тюмень» 2. Согласие субъекта на передачу ПДн
4	Отделение СФР Адрес: индекс, город, улица, дом	Персональные данные выгружаются из программы 1С: ЗиКГУ 3.1 (или формируются в другой программе для сдачи отчетности), подписываются отправляемые данные ЭЦП и передаются в СФР через Интернет	- ФИО, - Дата рождения, - № страхового свидетельства, - ИНН, - Паспортные данные, - Сумма начисления заработной платы - Адрес места жительства, - сведения о трудовой деятельности, - данные о счетах,	1. Трудовой кодекс РФ 2. Федеральный закон «Об обязательном пенсионном страховании в РФ» от 15.12.2001 г. №167-ФЗ

			открытых в банке, - о состоянии здоровья, - сведения о детях, их возрасте, -наименование структурного, - подразделения; занимаемая должность; - реквизиты документа, удостоверяющего личность, - суммы начисленных пособий	
6	Инспекция Федеральной налоговой службы Адрес: индекс, город, улица, дом	Персональные данные заносятся в программ СБИС, подвергаются корректировке и проверке, после чего подписываются ЭЦП и отправляются в ИФНС через Интернет	- ФИО, - ИНН, - Дата рождения, - Гражданство, - Паспортные данные - Адрес места жительства, - Сведения о доходах за отчетный период, - Сумма НДФЛ База по начислению страховых взносов -СНИЛС	1. Налоговый кодекс 2. В целях исполнения трудового договора
7	Военкомат Адрес: индекс, город, улица, дом	Персональные данные заносятся в формы, утвержденные Военкоматом, распечатываются на бумажном носителе и лично передаются ответственным лицам	- ФИО, - Дата рождения, - Семейное положение, - Сведения о детях, - Сведения об образовании, - Место работы и должность - отношение к воинской обязанности, воинское звание, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах	ст. 4 Закона от 28.03.1998 №53 ФЗ

Приложение №4
к приказу от 01.04.2025 № 37-ОД-Р

Инструкция администратора информационной безопасности

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность администратора безопасности информации в информационных системах персональных данных (далее - ИСПДн).
1.2. Администратор безопасности информации назначается в соответствии с приказом главного врача.
1.3. Администратор безопасности информации осуществляет контроль выполнения требований и организационных мероприятий по обеспечению защиты информации при использовании автоматизированных рабочих мест (далее – АРМ) дополнительно к своим непосредственным обязанностям.

2. Обязанности администратора безопасности информации ИСПДн

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2.2. Осуществлять установку, настройку и сопровождение средств защиты информации.
2.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.
2.4. Участвовать в приемке новых программных средств.
2.5. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении, оформленного соответствующим образом разрешения.
2.6. Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.
2.7. Вести контроль над процессом осуществления резервного копирования объектов защиты.
2.8. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.
2.9. Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
2.10. Контролировать физическую сохранность средств и оборудования ИСПДн.
2.11. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.
2.12. Контролировать исполнение пользователями парольной политики.
2.13. Реализовывать парольную политику.
2.14. Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.
2.15. Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений.
2.16. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.
2.17. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.
2.18. Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.
2.19. Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.
2.20. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
2.21. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права администратора безопасности информации ИСПДн

3.1. Администратор безопасности информации имеет право инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.2. Администратор безопасности информации имеет право обращаться к ответственному за организацию обработки персональных данных и/или ответственному за эксплуатацию ИСПДн с требованием прекращения работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по защите.

4. Ответственность администратора безопасности информации ИСПДн

4.1. На администратора безопасности информации ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн.

4.2. Администратор безопасности информации ИСПДн несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение №5
к приказу от 01.04.2025 № 37-ОД-Р

Инструкция пользователя ИСПДн

1 Общие положения

1.1. Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа информационных системах персональных данных (далее - ИСПДн).
1.2. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
1.3. Пользователем является каждый сотрудник **Муниципального Автономного учреждения культуры города Тюмени «Центр культуры и творчества «Тюмень»** (далее – Учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.4. Пользователь отвечает за правильность функционирования ИСПДн, входа в систему и все действия при работе в ИСПДн.
1.5. Пользователь в своей работе руководствуется настоящей инструкцией и регламентирующими документами Учреждения.
1.6. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2 Должностные обязанности

2.1. Допуск пользователей для работы на **АРМ** (автоматизированное рабочее место) осуществляется в соответствии со списком лиц, допущенных к работе с персональными данными.
2.2. В процессе первичной регистрации пользователя руководитель отдела, в котором работает пользователь, заявляет Администратору информационной системы перечень необходимых для работы пользователя ресурсов, перечень персональных данных, состав необходимого общесистемного программного обеспечения для решения поставленных задач.
2.3. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору информационной безопасности по телефону +7 952 685 24 69. (Шумков Юрий Александрович)
2.4. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Шумкову Юрию Александровичу по телефону +7 952 685 24 69.
2.5. Пользователь обязан:

- Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
- Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн.
- Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.
- Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет.
- При работе со съемными носителями пользователь должен каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ.

- В случае обнаружения вирусов на машинных (съемных) носителях информации (съемных носителях, жестком магнитном диске, твердотельном носителе) пользователь обязан немедленно сообщить Администратору информационной безопасности.
- В случае оставления рабочей станции без визуального контроля доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо комбинацией клавиш Win + L.
- Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.6. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.
- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
- Отключать (блокировать) средства защиты информации.
- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.
- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
- Самостоятельно вносить изменения в аппаратно-программную конфигурацию ИСПДн, изменять месторасположение средств отображения информации. 2.7. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

3 Правила работы в сетях общего доступа и (или) международного обмена

3.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2 При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования механизмов защиты.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (порно сайты, сайты, содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к Сети.