

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ ТУЛЬСКОЙ ОБЛАСТИ  
Государственное учреждение Тульской области  
«Комплексный центр социального обслуживания населения № 3»  
(ГУТО КЦСОН № 3)  
г. Богородицк

**ПРИКАЗ**

от 7. апреля 2021 года

№ 359-осн.

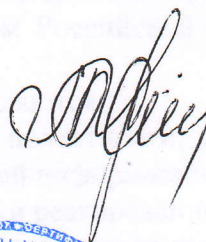
**Об утверждении Политики в отношении обработки персональных данных государственного учреждения Тульской области «Комплексный центр социального обслуживания населения № 3»**

В соответствии с п.2 ч.1, ч.2 ст. 18.1. Федерального закона от 27.07.2000 № 152-ФЗ «О персональных данных», на основании Устава ГУ ТО «Комплексный центр социального обслуживания населения №3»,

**ПРИКАЗЫВАЮ:**

1. Утвердить Политику в отношении обработки персональных данных государственного учреждения Тульской области «Комплексный центр социального обслуживания населения №3» (Приложение).
2. Опубликовать Политику государственного учреждения Тульской области «Комплексный центр социального обслуживания населения № 3» в отношении обработки персональных данных» на официальном сайте государственного учреждения Тульской области «Комплексный центр социального обслуживания населения № 3», в течение 10 дней с момента утверждения.
3. Приказ вступает в силу со дня подписания.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

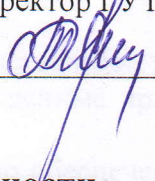


Л.М. Терехина

*Копия передана*



УТВЕРЖДАЮ  
Директор ГУ ТО КЦСОН № 3

  
Л.М. Терехина

## **Политика информационной безопасности в государственном учреждении Тульской области «Комплексный центр социального обслуживания населения №3»**

### **1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается директором ГУ ТО КЦСОН №3 и определяет мероприятия, процедуры и правила по защите информации в информационных системах ГУ ТО КЦСОН №3.

1.2. Положения настоящей Политики распространяются на следующие информационные системы ГУ ТО КЦСОН №3:

- ИС ГУ ТО КЦСОН №3.

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в ГУ ТО КЦСОН №3 относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.5. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;

- предотвращение утечек защищаемой информации;

- мониторинг событий безопасности и реагирование на инциденты безопасности;

- нейтрализация актуальных угроз безопасности информации;

- выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика разработана с учетом Положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

## **2. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

- 2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в ИС ГУ ТО КЦСОН №3. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.
- 2.2. Технологический процесс обработки персональных данных сотрудников ГУ ТО КЦСОН №3:
- 2.2.1) Сбор персональных данных
- 2.2.1.1) персональные данные получают непосредственно от субъекта, либо от его законного представителя при наличии нотариально заверенной доверенности, либо иных законных оснований;
- 2.2.1.2) источником получения персональных данных субъекта является предоставленные документы и заполненная унифицированная форма Т-2 «Личная карточка сотрудника».
- 2.2.2) Запись персональных данных в базу данных осуществляется штатными сотрудниками ГУ ТО КЦСОН №3.
- 2.2.3) Систематизация, накопление и хранение персональных данных выполняется средствами ИС ГУ ТО КЦСОН №3.
- 2.2.4) Уточнение (обновление, изменение) персональных данных осуществляется при обнаружении неточных, устаревших данных, либо по заявлению субъекта в связи с их изменением.
- 2.2.5) Обработка персональных данных предполагает сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование,

передача (предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

#### 2.2.6) Передача персональных данных

2.2.6.1) распространение персональных данных сотрудников ГУ ТО КЦСОН №3 не допускается;

2.2.6.2) предоставление персональных данных осуществляется в соответствии с законодательством Российской Федерации в следующих целях:

- сдача отчетности в Пенсионный Фонд РФ;
- налоговая отчетность;
- бухгалтерская отчетность;
- начисление заработной платы;
- предоставление субъектам справок.
- доступ к персональным данным имеют сотрудники, допущенные к обработке персональных данных в ИС ГУ ТО КЦСОН №3 и субъект персональных данных.

2.2.7) Обезличивание персональных данных в рамках данной информационной системы не предполагается.

2.2.8) Блокирование персональных данных осуществляется на основании мотивированной заявки субъекта в случае нарушения его прав или законных интересов, связанных с неправомерной обработкой его персональных данных в соответствии с законодательством РФ.

2.2.9) Удаление персональных данных, обрабатываемых средствами программного обеспечения, осуществляется при достижении цели обработки.

2.2.10) Уничтожение персональных данных производится по истечении сроков хранения документов содержащих соответствующую информацию (75 лет).

#### 2.3. Технологический процесс обработки персональных данных соискателей на вакантные должности в ГУ ТО КЦСОН №3:

2.3.1) Соискатель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые ГУ ТО КЦСОН №3 способы обработки персональных данных;
- наименование и место нахождения ГУ ТО КЦСОН №3, сведения о лицах (за исключением работников ГУ ТО КЦСОН №3), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с ГУ ТО КЦСОН №3 или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему Соискателю, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления Соискателем прав, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению ГУ ТО КЦСОН №3, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ «О персональных данных» или другими федеральными законами.

2.3.2) Соискатель вправе требовать от ГУ ТО КЦСОН №3 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.

2.3.3) Право Соискателя на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

2.3.4) Если Соискатель считает, что ГУ ТО КЦСОН №3 осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, Соискатель вправе обжаловать действия или бездействие ГУ ТО КЦСОН №3 в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.3.5) Основные обязанности ГУ ТО КЦСОН №3

2.3.5.1) При сборе персональных данных ГУ ТО КЦСОН №3 обязан предоставить Соискателю по его просьбе информацию, предусмотренную п. 1.2.1 настоящей Политики.

2.3.5.2) Если предоставление персональных данных является обязательным в соответствии с федеральными законами, ГУ ТО КЦСОН №3 обязан разъяснить Соискателю юридические последствия отказа предоставить его персональные данные.

2.3.5.3) Если персональные данные получены не от Соискателя, ГУ ТО КЦСОН №3, за исключением случаев, предусмотренных п. 1.3.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить Соискателю следующую информацию:

- наименование либо адрес ГУ ТО КЦСОН №3 или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом № 152-ФЗ «О персональных данных» права субъекта персональных данных;
- источник получения персональных данных.

2.3.6) ГУ ТО КЦСОН №3 освобождается от обязанности предоставить Соискателю сведения в случаях, если:

- ГУ ТО КЦСОН №3 уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены ГУ ТО КЦСОН №3 на основании федеральных законов или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является Соискатель;
- персональные данные сделаны общедоступными Соискателем или получены из общедоступного источника;
- ГУ ТО КЦСОН №3 осуществляет обработку персональных данных для статистических или иных исследовательских целей, либо научной или иной творческой деятельности, если при этом не нарушаются права и законные интересы Соискателя;
- предоставление Соискателю сведений, нарушает права и законные интересы третьих лиц.

2.3.7) При сборе персональных данных ГУ ТО КЦСОН №3 обязан обеспечить 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 пунктах 2, 3, 4, 8 части 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных».

2.4. Технологический процесс обработки персональных данных клиентов в ГУ ТО КЦСОН №3:

2.4.1) Сбор персональных данных

- персональные данные следует получать непосредственно у субъекта, либо у законного представителя при наличии нотариально заверенной доверенности, либо иных законных оснований;
- источником получения персональных данных субъекта является предоставленные документы.

2.4.2) Запись персональных данных в базу данных ИС ГУ ТО КЦСОН №3 осуществляется штатными сотрудниками ГУ ТО КЦСОН №3.

2.4.3) Уточнение (обновление, изменение) персональных данных осуществляется при обнаружении неточных, устаревших данных, либо по заявлению субъекта в связи с их изменением.

2.4.4) Обработка персональных данных предполагает сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

2.4.5) Передача персональных данных

- распространение персональных данных клиентов ГУ ТО КЦСОН №3 не допускается;
- предоставление персональных данных осуществляется в соответствии с законодательством Российской Федерации;
- доступ к персональным данным имеют сотрудники, допущенные к обработке персональных данных в ИС ГУ ТО КЦСОН №3 и субъект персональных данных.

2.4.6) Обезличивание персональных данных в рамках данной информационной системы не предполагается.

2.4.7) Блокирование персональных данных осуществляется на основании мотивированной заявки субъекта в случае нарушения его прав или законных интересов, связанных с неправомерной обработкой его персональных данных в соответствии с законодательством РФ.

2.4.8) Удаление персональных данных, обрабатываемых средствами программного обеспечения, осуществляется при достижении цели обработки.

2.4.9) Уничтожение персональных данных производится по истечении сроков хранения документов содержащих соответствующую информацию (5 лет).

### **3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ИС.**

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ГУ ТО КЦСОН №3, допущенному к работе с ресурсами ИС ГУ ТО КЦСОН №3 присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

3.2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе.

3.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

3.4. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ИС для сотрудника ГУ ТО КЦСОН №3, и предоставления ему (или изменения его) прав доступа к ресурсам ИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИС ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИС);
- заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ИС.

3.5. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

- положение о разграничении прав доступа в ИС (при необходимости, Приложение № 2 к настоящей Политике);
  - Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ИС ГУ ТО КЦСОН №3.
- 3.6. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись и первичный пароль. Дает ознакомиться с инструкцией Пользователя ИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ИС.
- 3.7. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИС при разборе инцидентов безопасности.
- 3.8. В качестве модели разграничения доступа к ресурсам ИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ИС приведено в Приложении к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.
- 3.9. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ИС и сопоставляемые им роли, утверждаются руководителем ГУ ТО КЦСОН №3, Администратор обеспечивает оперативное обновление и актуальность данного перечня.
- 3.10. Перечень помещений, в которых разрешена работа с ресурсами ИС, расположены технические средства ИС, а также перечень лиц, утверждается руководителем ГУ ТО КЦСОН №3. Администратор обеспечивает оперативное обновление и актуальность данного перечня.
- 3.11. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети ГУ ТО КЦСОН №3 на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.
- 3.12. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе.

#### **4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ.**

4.1. Информационные потоки в ГУ ТО КЦСОН №3 разделены на две группы: основные потоки получения и передачи информации, непосредственно входящие в технологический процесс работы ГУ ТО КЦСОН №3 и дополнительные вспомогательные потоки обеспечения информацией и повышения эффективности работы.

В первую группу входят следующие основные информационные потоки:

- обмен электронными документами;
- прием и выдача документов клиентам;
- отправка отчетных форм.

Во вторую группу входят следующие вспомогательные информационные потоки:

- получение информационно-правовой справочной информации с использованием справочных систем;
- получение информации с использованием глобальной электронной сети Интернет.

#### 4.2. Основные информационные потоки

##### 4.2.1) Обмен электронными документами.

*Данный информационный поток обеспечивает обмен электронными платежными документами между ГУ ТО КЦСОН №3 осуществляется в соответствии с действующим законодательством, нормативными актами вышестоящих организаций, внутренними документами ГУ ТО КЦСОН №3.*

##### 4.2.2) Прием и выдача документов клиентов.

Данный информационный поток обеспечивает обмен документами между ГУ ТО КЦСОН №3 и клиентами как на бумажном носителе, так и в электронном виде по каналам связи с использованием сети Интернет.

Работа специалистов ГУ ТО КЦСОН №3 на данном участке регламентируется действующим законодательством, нормативными актами вышестоящих организаций, внутренними документами ГУ ТО КЦСОН №3.

Для обеспечения информационной безопасности программно-аппаратные средства ИС обеспечивают:

- парольный вход;
- проверку целостности программного и информационного обеспечения;
- криптографическую защиту передаваемой информации;

##### 4.2.3) Отправка отчетных форм.

Данный информационный поток обеспечивает обмен документами между ГУ ТО КЦСОН №3 и вышестоящими контролирующими организациями, как на бумажном носителе, так в электронной форме.

В первом случае доставка документов осуществляется Почтой России.

Во втором случае предусмотрено использование специально защищенной системы связи.

#### 4.3. Вспомогательные информационные потоки

##### 4.3.1) Получение информационно-правовой справочной информации с использованием справочных систем.

Данный информационный поток обеспечивает получение информационно-правовой справочной информации специальных программ всеми пользователями внутренней компьютерной сети ГУ ТО КЦСОН №3.

##### 4.3.2) Получение информации с использованием глобальной электронной сети Интернет.

Данный информационный поток обеспечивает работу в сети Интернет ограниченному числу сотрудников ГУ ТО КЦСОН №3, которым для выполнения служебных обязанностей данная услуга необходима.

Для обеспечения информационной безопасности используются следующие программно-организационные средства:

- использование файрвола для защиты извне внутренней компьютерной сети банка;
- мониторинг и сканирование антивирусными программами;
- регулярный анализ администратором сети протоколов соединений с целью выявления внешних сетевых нежелательных подключений и атак

### **5. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

5.1. В ИС ГУ ТО КЦСОН №3 разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.2. Перечень разрешенного программного обеспечения в ИС ГУ ТО КЦСОН №3 определен в Приложении к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением. Пользователям запрещена установка любого ПО в ИС ГУ ТО КЦСОН №3.



5.4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

5.5. Администратор ежемесячно проводит проверку соответствия состава программного обеспечения в ИС ГУ ТО КЦСОН №3 списку разрешенного ПО. В случае выявления стороннего программного обеспечения, созывается группа реагирования на инцидент информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

## **6. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, ГАРАНТИРОВАННО УНИЧТОЖЕНИЕ ИНФОРМАЦИИ.**

6.1. В качестве машинных носителей информации рассматриваются:

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках),
- съемные машинные носители информации,
- портативные вычислительные устройства, имеющие встроенные носители информации.

6.2. Под использованием машинных носителей информации в ИС ГУ ТО КЦСОН №3 понимается их подключение к инфраструктуре ИС ГУ ТО КЦСОН №3 с целью обработки/приема/передачи информации между информационной системой и носителями информации.

6.3. Данные правила обязательны для применения во всех подразделениях ГУ ТО КЦСОН №3, в которых обрабатывается информация ограниченного доступа (в том числе персональные данные), не содержащая сведения, составляющие государственную тайну.

6.4. Использование машинных носителей информации

6.4.1) В ИС ГУ ТО КЦСОН №3 допускается использование только учетных машинных носителей информации, которые являются собственностью ГУ ТО КЦСОН №3 и подлежат регулярной ревизии и контролю.

6.4.2) Машинные носители информации предоставляются сотрудникам ГУ ТО КЦСОН №3 по инициативе начальника структурного подразделения в случаях:

- необходимости выполнения вновь принятым сотрудником своих должностных обязанностей;
- возникновения у сотрудника ГУ ТО КЦСОН №3 производственной необходимости.

6.4.3) При использовании сотрудниками машинных носителей информации необходимо:

- использовать машинные носители информации исключительно для выполнения служебных обязанностей.

- ставить в известность Ответственного за защиту информации в ГУ ТО КЦСОН №3 о любых фактах нарушения требований настоящих правил.

- бережно относиться к машинным носителям информации.
- обеспечивать физическую безопасность машинных носителей информации.
- извещать Ответственного за защиту информации о фактах утраты (кражи) машинных носителей информации.

- перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ.

6.4.4) При использовании машинных носителей информации запрещено:

- использовать машинные носители информации в личных целях.
- передавать носители информации другим лицам (за исключением администраторов информационной безопасности).
- оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;

- выносить машинные носители информации из служебных помещений для работы с ними на дому и т. д.

- ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

#### 6.5. Хранение и учёт машинных носителей информации

6.5.1) Все находящиеся на хранении и в обращении машинные носители информации в ИС ГУ ТО КЦСОН №3 подлежат обязательному учёту. На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать.

6.5.2) Регистрацию машинных носителей информации осуществляет Ответственный за защиту информации в Журнале регистрации, учета и выдачи машинных носителей информации (далее – Журнал регистрации) путем занесения регистрационного или иного номера с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

6.5.3) Учет выдачи машинных носителей информации ведётся Ответственным за обработку и защиту информации в Журнале регистрации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего средство его роспись.

6.5.4) Сотрудники ГУ ТО КЦСОН №3 получают учтенный машинный носитель от Ответственного за обработку и защиту информации для выполнения работ на конкретный срок. При получении делаются соответствующие записи в Журнале регистрации. По окончании работ пользователь сдает машинный носитель для хранения Ответственному за защиту информации, о чем делается соответствующая запись в журнале регистрации.

6.5.5) При поступлении нового машинного носителя информации, который будет использоваться в ИС ГУ ТО КЦСОН №3, Ответственный за защиту информации регистрирует его в Журнале регистрации. Перед использованием новый машинный носитель информации в обязательном порядке должен пройти антивирусную проверку (при наличии технической возможности).

*6.5.6) При передаче средств вычислительной техники (далее – СВТ) ИС ГУ ТО КЦСОН №3 сторонним организациям для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ.*

6.5.7) В случае возврата машинного носителя информации в Журнале регистрации Ответственным за защиту информации проставляется отметка о возврате с указанием даты времени возврата, личных подписей передающей и принимающей стороны.

6.5.8) В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные машинные носители информации изымаются.

6.5.9) Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

#### 6.6. Ликвидация машинных носителей информации и уничтожение (стирание) информации на машинных носителях.

6.6.1) В случае утраты или уничтожения машинных носителей информации немедленно ставятся в известность начальник соответствующего структурного подразделения и Ответственный за защиту информации. На утраченные носители составляется акт. Соответствующие отметки вносятся в Журнал регистрации.

6.6.2) Машинные носители информации, пришедшие в негодность или отслужившие установленный срок, должны быть уничтожены без возможности восстановления с составлением Акта уничтожения машинных носителей информации и последующей регистрацией в Журнале регистрации. Уничтожение машинных носителей осуществляется комиссией.

6.6.3) В ГУ ТО КЦСОН №3 обеспечивается уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации:

6.6.4) Уничтожение (стирание) информации на машинных носителях исключает возможность восстановления защищаемой информации при передаче машинных носителей ме

ду пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

6.6.5) В ИС ГУ ТО КЦСОН №3 используются следующие меры по уничтожению (стиранию) информации на машинных носителях, исключая возможность восстановления защищаемой информации:

- перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, - удаление записи о файлах,
- обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

6.6.6) Ответственный за обработку и защиту информации обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесением в Журнал регистрации.

## **7. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ)**

7.1. В ГУ ТО КЦСОН №3 обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

7.2. Управление взаимодействием ИС ГУ ТО КЦСОН №3 с внешними информационными системами включает:

- предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям;
- определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учетных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к информационной системе авторизованными (уполномоченными) пользователями из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

7.3. Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. N 977.

## **8. ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА.**

8.1. Удаленный доступ к ИС ГУ ТО КЦСОН №3 осуществляется на основании заявок, подписанных руководителем подразделения. Форма заявки на предоставление доступа к ИС ГУ ТО КЦСОН №3 приведена в Приложении.

8.2. В заявках на предоставление доступа к ИС ГУ ТО КЦСОН №3 с упрощенной аутентификацией указывается обоснование необходимости предоставления доступа, список

пользователей, которым необходимо предоставить доступ, и срок предоставления доступа.

8.4. Удаленный доступ к системе электронной почты предоставляется пользователям ИС автоматически при создании учетной записи электронной почты.

8.5. В заявках на предоставление доступа к ИС общего доступа с усиленной аутентификацией указывается обоснование необходимости предоставления доступа, список пользователей, которым необходимо предоставить доступ, срок предоставления доступа, а также сведения об используемых средствах защиты информации.

8.6. В случае отсутствия у пользователя сертификата ключа аутентификации, выданного удостоверяющим центром, пользователь обязан получить его в установленном порядке перед подачей заявки на предоставление доступа к ИС общего доступа с усиленной аутентификацией.

8.7. Удаленный доступ к ИС с ограниченным доступом предоставляется сторонним пользователям при наличии соглашения об информационном взаимодействии между сторонним пользователем и абонентом, содержащего обязательства по выполнению требований законодательства Российской Федерации к обеспечению защиты обрабатываемой информации.

8.8. Заявка на предоставление удаленного доступа к ИС с ограниченным доступом должна содержать:

- наименование и реквизиты стороннего пользователя;
- наименование ИС, к которой предполагается доступ;
- сведения о соглашении между сторонним пользователем и абонентом;
- характеристику предполагаемого информационного взаимодействия информационных систем;
- структуру и состав информационной системы стороннего пользователя;
- схему подключения информационной системы стороннего пользователя к ИС с ограниченным доступом с указанием информационных потоков;
- состав программного и аппаратного обеспечения (в том числе средств защиты информации), с помощью которых предполагается обеспечить подключение;
- сведения о сотрудниках стороннего пользователя, для которых запрашивается право доступа к ИС;
- сведения о соответствии информационной системы стороннего пользователя требованиям, установленным для ИС, к которой предоставляется доступ (сведения об аттестате соответствия требованиям информационной безопасности при подключении к государственным информационным системам);
- сведения о должностном лице, ответственном за организацию подключения.

8.9. Порядок прекращения удаленного доступа к ИС:

8.9.1) Удаленный доступ пользователей к ИС ГУ ТО КЦСОН №3 прекращается на основании заявок, направляемых абонентом ГУ ТО КЦСОН №3, или по истечении срока, указанного в заявке на предоставление удаленного доступа.

8.9.2) Удаленный доступ пользователей к системе электронной почты прекращается автоматически при блокировке учетной записи пользователя.

8.9.3) ГУ ТО КЦСОН №3 имеет право без предварительного уведомления приостановить (прекратить) удаленный доступ пользователей к ИС ГУ ТО КЦСОН №3 в случае возникновения угрозы обеспечения целостности и сохранности информации в ИС ГУ ТО КЦСОН №3.

## **9. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ.**

9.1. В ГУ ТО КЦСОН №3 в качестве средства выявления уязвимостей используются сканеры уязвимостей OWASP ZAP, 4MOSAn Vulnerability Management, Secunia Personal Software Inspector и SQLMAP.

9.2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИС ГУ ТО КЦСОН №3 производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

9.3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИ-ИБ.

9.4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

9.5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

9.6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя ГУ ТО КЦСОН №3.

#### ***10. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.***

10.1. Администратором ИБ должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

10.2. Администратором ИБ должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

10.3. При контроле установки обновлений администратор ИБ должен осуществлять проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком.

10.4. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации должен проводиться не реже 1 раза в 6 месяцев.

#### ***11. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ.***

11.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ИС ГУ ТО КЦСОН №3 фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

11.2. В случае добавления новых ТС, ПО и СрЗИ в состав ИС ГУ ТО КЦСОН №3 или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

11.3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

11.4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ИС ГУ ТО КЦСОН №3 является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

11.5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

11.6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю ГУ ТО КЦСОН №3, который принимает решение об организации самостоятельной сертификации используемого СрЗИ, либо об обновлении используемого СрЗИ до актуальной версии, либо о замене используемого СрЗИ на другое аналогичное сертифицированное СрЗИ.

## **12. ПЕРЕЧЕНЬ НЕШТАТНЫХ СИТУАЦИЙ.**

12.1. Разглашение информации ограниченного доступа сотрудниками ГУ ТО КЦСОН №3, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача информации по незащищенным каналам связи;
- обработка информации на незащищенных технических средствах обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;
- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с информацией.

12.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение информации;
- несанкционированное копирование информации;

12.3. Несанкционированный доступ к защищаемой информации:

- несанкционированное подключение технических средств к средствам и системам ИС ГУ ТО КЦСОН №3;
- использование закладочных устройств;
- использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС ГУ ТО КЦСОН №3;
- использование злоумышленником уязвимостей программного обеспечения ИС;
- использование злоумышленником программных закладок;
- заражение ИС злоумышленником программными вирусами;
- хищение носителей информации;
- нарушение функционирования технических средств обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

12.4. Дефекты, сбои, отказы, аварии технических средств и систем ИС;

12.5. Дефекты, сбои, отказы программного обеспечения ИС;

12.6. Сбои, отказы и аварии систем обеспечения ИС;

12.7. Природные явления, стихийные бедствия:

- термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
- механические факторы (повреждения зданий, землетрясения и т. д.);
- электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

12.8. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

12.9. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

12.10. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

12.11. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбой, отказы и аварии средств и систем ИС а также меры по замене/ремонту вышедших из строя средств и систем;

12.12. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации;
- в случае нарушения корректной работы технических средств в ИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

**- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств и носителей информации.**

**ЗАЯВКА**  
**на внесение изменений в списки пользователей**  
**и наделение пользователей полномочиями доступа**  
**к ресурсам ИС ГУТО КЦСОН №3**

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) ИС  
(нужное подчеркнуть)

\_\_\_\_\_

(должность с указанием подразделения)

\_\_\_\_\_

(фамилия имя и отчество сотрудника)  
предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)  
(нужное подчеркнуть)

для решения задач:

\_\_\_\_\_

(список задач согласно формуляров задач)

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

(наименование заказывающего подразделения)

«\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(фамилия)

Согласовано      Администратор безопасности

«\_\_» \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(фамилия)



### Положение о разграничении прав доступа в ИС ГУТО КЦСОН №3

Исходя из характера и режима обработки защищаемой информации в ИС ГУТО КЦСОН №3 определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ИС приведен в таблице.

Роль	Описание параметров доступа к ПДн для данной роли	Разрешенные действия
Администратор	<ul style="list-style-type: none"><li>- Обладает полной информацией о системном и прикладном программном обеспечении.</li><li>- Обладает полной информацией о технических средствах и конфигурации.</li><li>- Имеет доступ ко всем техническим средствам обработки информации и данным.</li><li>- Обладает правами конфигурирования и административной настройки технических средств.</li></ul>	<ul style="list-style-type: none"><li>- сбор</li><li>- систематизация</li><li>- накопление</li><li>- хранение</li><li>- уточнение</li><li>- использование</li><li>- уничтожение</li></ul>
Администратор безопасности	<ul style="list-style-type: none"><li>- Обладает правами Администратора.</li><li>- Обладает полной информацией об.</li><li>- Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов.</li><li>- Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).</li></ul>	<ul style="list-style-type: none"><li>- сбор</li><li>- систематизация</li><li>- накопление</li><li>- хранение</li><li>- уточнение</li><li>- использование</li><li>- уничтожение</li></ul>
Оператор	<ul style="list-style-type: none"><li>- Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.</li></ul>	<ul style="list-style-type: none"><li>- сбор</li><li>- систематизация</li><li>- накопление</li><li>- хранение</li><li>- уточнение</li><li>- использование</li><li>- уничтожение</li></ul>

Список разрешенного программного обеспечения в ИС ГУ ТО КЦСОН №3

№ п/п	Наименование ПО	Тип ПО
	Astra Linux	Операционные системы
	Microsoft Windows	Операционные системы
	Microsoft Office	Офисные пакеты
	LibreOffice	Офисные пакеты
	1С Предприятие	Программное обеспечение бухгалтерского и кадрового учета
	1С Бухгалтерский учет	Программное обеспечение бухгалтерского и кадрового учета
	Парус	Программное обеспечение бухгалтерского и кадрового учета
	Налогоплательщик ЮЛ	Программное обеспечение бухгалтерского и кадрового учета
	КРИСТА	Программное обеспечение бухгалтерского и кадрового учета
	СЭД УФК	Программное обеспечение бухгалтерского и кадрового учета
	АС «Клиент-Сбербанк»	Программное обеспечение бухгалтерского и кадрового учета
	Крипто-Про CSP	Средства криптографической защиты информации
	Rutoken Drivers	Средства криптографической защиты информации
	Континент-АП	Средства криптографической защиты информации
	VipNet Client	Средства криптографической защиты информации
	Eset nod 32 Antivirus	Антивирусное программное обеспечение
	Kaspersky Antivirus	Антивирусное программное обеспечение
	Internet Explorer	Интернет браузеры
	Mozilla Firefox	Интернет браузеры
	Opera	Интернет браузеры
	Google Chrome	Интернет браузеры
	Yandex Browser	Интернет браузеры
	7Zip	Программное обеспечение для архивирования файлов и папок (архиваторы)
	WinRAR	Программное обеспечение для архивирования файлов и папок (архиваторы)
	ABBYY Fine Reader	Прикладное ПО
	Adobe Flash Player	Прикладное ПО
	Adobe Acrobat Reader	Прикладное ПО
	Foxit Reader	Прикладное ПО
	Гарант	Справочно-правовые системы
	Консультант Плюс	Справочно-правовые системы

№ п/п	Наименование ПО	Тип ПО
	ИС АСП	Информационные системы персональных данных
	ИС РСЭП ТО	Информационные системы персональных данных
	АЛЬКОНА	Информационные системы персональных данных
	Прочее специализированное ПО, необходимое для обработки массивов данных, для достижения целей поставленных руководством министерства труда и социальной защиты Тульской области.	

\*Внесение изменений в список разрешенного программного обеспечения или установка и использование неуказанных в списке программных продуктов возможно только при письменном согласовании с ответственным сотрудником сектора программно-информационного обеспечения.

План обеспечения непрерывности функционирования ИС ГУ ТО КЦСОН №3

№ п/п	Тип нештатной ситуации	Кому и в какие сроки докладываются в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
	Обнаружение несанкционированно скопированной или измененной конфиденциальной информации	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
	Обнаружение подключения технических средств к средствам и системам объекта информатизации	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	3 часа
	Подключение технических средств к средствам и системам ГИС в текущий момент времени	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа
	Обнаружение закладочных устройств	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	Сразу после получения информации об инциденте	1 день

**ЗАДАНИЕ**  
**на внесение изменений в списки пользователей ИС**

Администратору безопасности информации

\_\_\_\_\_ (фамилия и инициалы исполнителя)

**Произвести изменения в списках пользователей**

Директор ГУ ТО КЦСОН №3  
\_\_\_\_\_ Терехина Л.М.

«\_\_» \_\_\_\_\_ 20\_\_ г.

*Обратная сторона заявки*

Присвоено **имя** \_\_\_\_\_ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

Наименование задач

Администратор безопасности \_\_\_\_\_

Имя учетной записи, и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя ИС ознакомлен

Пользователь \_\_\_\_\_

(подпись, фамилия)

«\_\_» \_\_\_\_\_ 20\_\_ года