Бюджетное учреждение Воронежской области
«Краснолипьевский центр реабилитации и социализации»

ПРИКАЗ

03.02.2025 № 49/ОД

Об обеспечении безопасности помещений, в которых ведется работа с государственными информационными системами Воронежской области в БУ ВО «Краснолипьевский ЦРС»

С целью организации работ по обеспечению безопасности помещений, в которых ведется обработка персональных данных в государственных информационных системах, располагаются средства криптографической защиты информации, и сохранности материальных носителей информации ограниченного доступа, в том числе машинных носителей информации в БУ ВО «Краснолипьевский ЦРС» в целях выполнения требований постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных ~ системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказа ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания 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»

п р и к а з ы в а ю :

1. Утвердить список лиц, допущенных к обработке персональных данных, в соответствии с приложением 1 к настоящему приказу.

2. Назначить ответственного за порядок и организацию режима безопасности помещений, в которых ведется обработка персональных данных и (или) размещаются средства криптографической защиты информации.

3. Утвердить Инструкцию по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации в соответствии с приложением № 2 к настоящему приказу.

4. Утвердить Порядок доступа сотрудников в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе (приложение 3 к настоящему приказу).

5. Утвердить Перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах (приложение 4).

6. Вести ежегодную актуализацию списков, указанных в пункте 1 и 5 настоящего приказа.

7. Администратору информационной безопасности – технику-программисту Шпилевому Александру Владимировичу:

- осуществлять поэкземплярный учет материальных (отчуждаемых машинных) носителей информации ограниченного доступа, не содержащей сведения, составляющей государственную тайну, путем ведения соответствующего журнала;

- довести до сотрудников, допущенных к обработке информации ограниченного доступа, не составляющей государственную тайну, положения

утвержденных организационно-распорядительных документов под роспись.

8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.В.Аралов

С приказом ознакомлены:

Малыхина Е.Ю.
Измайлова Л.Н.
Шпилевой А.В.

Приложение № 1
к приказу
БУ ВО «Краснолипьевский ЦРС»
от 03.02.2025 № 49/ОД

Список лиц,
допущенных к обработке персональных данных

№ п/п	№ кабинета	Наименование ИС[1]	Должность	ФИО
	Каб. директора	АС ДОУ - ГИС «Автоматизированная система документационного обеспечения управления Воронежской области» ГИС ЕИС - ГИС «Единая информационная система персонифицированного учета граждан в органах социальной защиты населения Воронежской области» и защищенной корпоративной сети передачи данных» ЕЦИС - ГИС «Единая централизованная информационная система Воронежской области по бюджетному (бухгалтерскому) учету и отчетности» КАСИБ - ГИС «Комплексная автоматизированная система исполнения бюджета» WEB-Торги КС - ГИС «Региональная информационная система в сфере закупок Воронежской области «Программный комплекс для автоматизации государственных (муниципальных) закупок»	Директор	Аралов Валерий Викторович
	Каб. Отдел кадров	ГИС ЕИС - ГИС «Единая информационная система персонифицированного учета граждан в органах социальной защиты населения Воронежской области» и защищенной корпоративной сети передачи данных»	Инспектор по кадрам	Малыхина Евгения Юрьевна
	Каб. Отдел кадров	ГИС ЕИС - ГИС «Единая информационная система персонифицированного учета граждан в органах социальной защиты населения Воронежской области» и защищенной корпоративной сети передачи данных»	Специалист по социальной работе	Измайлова Любовь Николаевна

[1] АС ДОУ - ГИС «Автоматизированная система документационного обеспечения управления Воронежской области»
ГИС ЕИС - ГИС «Единая информационная система персонифицированного учета граждан в органах социальной защиты населения Воронежской области» и защищенной корпоративной сети передачи данных»
СГИО - ГИС «Система гарантированного информационного обмена»
ЕЦИС - ГИС «Единая централизованная информационная система Воронежской области по бюджетному (бухгалтерскому) учету и отчетности»
КАСИБ - ГИС «Комплексная автоматизированная система исполнения бюджета»
WEB-Торги КС - ГИС «Региональная информационная система в сфере закупок Воронежской области «Программный комплекс для автоматизации государственных (муниципальных) закупок»
АИС «Контингент ВО» (подсистема КДНиЗП) - ГИС «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным и дополнительным общеобразовательным программам и программам среднего профессионального образования Воронежской области»

Приложение № 2
к приказу
БУ ВО «Краснолипьевский ЦРС»
от 03.02.2025 № 49/ОД

ИНСТРУКЦИЯ
по организации хранения, учета и работы с материальными носителями информации ограниченного доступа, в том числе с машинными носителями информации

1 Общие положения

1.1 Настоящая Инструкция определяет правила при хранении и учета материальных носителей информации ограниченного доступа (в том числе персональные данные), включая машинные носители информации в бюджетное учреждение Воронежской области «Краснолипьевский центр реабилитации и социализации» (далее – учреждения).

1.2 Действие настоящей Инструкции распространяется на сотрудников учреждения, допущенных к обработке информации ограниченного доступа.

2 Порядок хранение материальных носителей информации

2.1 Хранение материальных носителей информации должно происходить в порядке, исключающем их утрату или неправомерное использование.

2.2 При хранении материальных носителей, в том числе на бумажных носителях, содержащих информацию ограниченного доступа, должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

2.3 Хранение персональных данных (далее - ПДн) субъектов ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки в соответствии со сроками хранения, определяемыми законодательством Российской Федерации и нормативными документами учреждения.

2.4 При уходе в отпуск, нахождении в служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте он обязан передать документы и иные носители, содержащие информацию ограниченного доступа, лицу, на которое приказом или распоряжением директора учреждения будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, документы и иные носители, содержащие информацию ограниченного доступа, передаются другому

работнику, имеющему доступ к информации ограниченного доступа по указанию руководителя отдела.

2.5 При увольнении работника, имеющего доступ к информации ограниченного доступа, документы и иные носители, содержащие информацию ограниченного доступа, сдаются работником своему непосредственному руководителю.

2.6 Режим конфиденциальности ПДн снимается в случаях их обезличивания и по истечении срока их хранения, если иное не определено законом.

3 Порядок учета машинных носителей информации

3.1 Все машинные носителей информации, используемые в информационных системах (далее - **ИС ОИ**) для хранения и обработки информации ограниченного доступа должны быть учтены.

3.2 Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

3.3 Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

3.4 Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации.

3.5 Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства ИС ОИ нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

3.6 Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с

указанием пользователя, или группы пользователей, которым разрешен доступ к машинным носителям информации.

3.7 Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

3.8 Маркировка машинных носителей информации (технических средств), дополнительно должна включать в себя информацию о возможности использования машинного носителя информации вне ИС ОИ.

3.9 Учет машинных носителей информации, осуществляется работниками, осуществляющих обработку информации ограниченного доступа (в том числе ПДн).

3.10 Ежегодно необходимо проводить инвентаризацию всех носителей информации, на которых хранится и обрабатывается информация ограниченного доступа. Результаты инвентаризации должны документироваться.

4 Порядок работы с материальными носителями информации ограниченного доступа

4.1 При работе с материальными носителями информации ограниченного доступа необходимо соблюдать требования данной Инструкции.

4.2 При потере или краже материального носителя информации ограниченного доступа незамедлительно ставить в известность директора учреждения. Отметки об утрате вносятся в журнал.

4.3 При передаче информации ограниченного доступа необходимо передавать минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.

4.4 В случае увольнения или перевода работника в другой отдел, предоставленные документы, содержащие сведения ограниченного доступа, изымаются.

4.5 При работе с материальными носителями информации ограниченного доступа запрещается:

- использовать документы, содержащие информацию ограниченного доступа в личных целях;

- передавать документы, содержащие информацию ограниченного доступа, третьим лицам без соответствующего разрешения директора;

- хранить документы, содержащие информацию ограниченного доступа, с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить документы, содержащие информацию ограниченного доступа, из

служебных помещений для работы с ними на дому и т. д.

4.6 Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

5. Порядок уничтожения (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

5.1 При передаче машинных носителей информации между пользователями, в сторонние организации для ремонта или утилизации должно обеспечиваться уничтожение (стирание) информации на машинных носителях, а также контроль уничтожения (стирания) информации.

5.2 Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

5.3 Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

5.4 Процедуры уничтожения информации и контроля осуществляются администратором информационной безопасности с использованием встроенных механизмов средств защиты информации (далее - СрЗИ) от несанкционированного доступа (далее - НСД) в соответствии с эксплуатационной документацией на СрЗИ. Должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

- очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти.

5.5 Действия по удалению защищаемой информации и уничтожению машинных носителей информации должны регистрироваться и контролироваться администратором информационной безопасности.

6. Порядок доступа к машинным носителям информации

6.1 На рабочих местах, где ведется обработка информации ограниченного доступа, определяют должностные лица, имеющие физический доступ к машинным носителям информации, а именно к следующим:

- съемным машинным носителям информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

- портативным вычислительным устройствам, имеющим встроенные носители

информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

-машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

- бумажным носителям информации.

6.2 Предоставление физического доступа к машинным носителям информации осуществляется только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

7. Контроль использования интерфейсов ввода (вывода)

7.1 В БУ ВО «Краснолипьевский ЦРС» разрешено использование интерфейсов средств вычислительной техники (далее - СВТ), которые могут использоваться для ввода (вывода) информации, исключительно для работы с учтенными машинными носителями информации.

7.2 Доступ к использованию интерфейсов ввода (вывода) СВТ ИС разрешен лицам, допущенным к данному СВТ и администраторам ИС.

7.3 Контроль использования интерфейсов ввода (вывода) осуществляется встроенными механизмами средства защиты от НСД.

Приложение 1 к Инструкции
Типовая форма журнала учета
машинных носителей

УТВЕРЖДАЮ

« » 20 г.

ЖУРНАЛ
/
учета машинных носителей информации ограниченного доступа

Начат . 20___ г.

Ответственный за организацию и обеспечение безопасности ПДн:

№ п/п	Рег./Инв. №	Вид носителя, учетный номер носителя	Кол-во носителей	Датам № акта уничтожения	Ф.И.О. ответственного пользователя	Наименование структурного подразделения	Каб.	Дата передачи носителя	Ф.И.О. передавшего	Ф.И.О. получившего	Роспись

ЛИСТ ОЗНАКОМЛЕНИЯ

п.п.	Должность	Фамилия Имя Отчество	Дата и подпись
1.	директор	В.В.Аралов	03.02.25
2.	Инспектор по кадрам	Е.Ю.Малыхина	03.02.2025
3.	Специалист по социальной работе	Л.Н.Измайлова	03.02.2025
4.	Техник-программист	А.В.Шпилевой	03.02.2025 Шпилевой

Приложение № 3
к приказу
БУ ВО «Краснолипьевский ЦРС»
от 03.02.2025 № 49/ОД

Порядок доступа работников в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе

1. Общие положения

1.1 Настоящий Порядок доступа работников БУ ВО «Краснолипьевский ЦРС» (далее - учреждение) в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе (далее - Порядок) устанавливает единые требования к доступу работников учреждения в служебные помещения.

1.2 Настоящий Порядок обязателен для применения и исполнения всеми работниками учреждения, работающими в служебных помещениях, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе.

2. Требования к служебным помещениям, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе

2.1 В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения БУ ВО «Краснолипьевский ЦРС», в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе обеспечивается:

- использование служебных помещений строго по назначению;
- наличие на входах в служебные помещения дверей, оборудованных запорными устройствами, уплотняющими прокладками;
- содержание дверей служебных помещений в нерабочее время в закрытом на запорное устройство состоянии;
- остекление окон в здании учреждения, содержание их в нерабочее время в закрытом состоянии;
- доступ в служебные помещения только работников учреждения.

2.2 Доступ в служебные помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе работников допускается только для выполнения поручений и получения информации, необходимой для исполнения служебных обязанностей в соответствии с должностной инструкцией, иных лиц - в случаях, установленных законодательством.

2.3 Работникам запрещается передавать ключи от служебных помещений в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе третьим лицам.

3. Контроль за соблюдением требований к доступу работников в служебные помещения в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе

3.1. Текущий контроль за содержанием служебных помещений, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе осуществляет лицо, ответственное за соблюдение требований к ограничению доступа в служебные помещения.

3.2. Работники, обнаружившие попытку проникновения посторонних лиц в служебные помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе, немедленно сообщают об этом лицу, ответственному за соблюдение требований к ограничению доступа в служебные помещения.

Приложение № 4
к приказу
БУ ВО «Краснолипьевский ЦРС»
от 03.02.2025 № 49/ОД

Перечень работников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах

№ п/п	Должность	ФИО
1	директор	Аралов Валерий Викторович
2	Инспектор по кадрам	Малыхина Евгения Юрьевна
3	Специалист по социальной работе	Измайлова Любовь Николаевна

Ответственный за порядок и организацию режима безопасности помещений, в которых ведется обработка персональных данных и (или) размещаются средства криптографической защиты информации: директор Аралов Валерий Викторович