УТВЕРЖДЕНО:
Приказом № 72-ОД от 26.05.2026
Директора ГАОУДПО Республики Мордовия
«Мордовский республиканский центр
повышения квалификации специалистов
здравоохранения»

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

по обеспечению защиты информации при её обработке в информационных системах ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения»

СОДЕРЖАНИЕ

1. Общие положения

Настоящая Инструкция разработана для обеспечения защиты персональных данных при их обработке в информационных системах ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения» в соответствии со следующими документами:

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 11 февраля 2013 г. № 17 г. Москва «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

– Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11 февраля 2014 г;

– Постановление Правительства Республики Мордовия от 7 мая 2018 г. № 289 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных».

1.1. Работа с информацией, подлежащей защите строится на следующих принципах:

– принцип персональной ответственности – в любой момент времени за каждый документ (независимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;

– принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах/актах (передача из рук в руки, снятие копии и т.п.).

Пользователь ИС (далее – Пользователь) осуществляет обработку персональных данных субъектов ПДн и персональных данных работников ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификаций специалистов здравоохранения».

1.2.Информации, составляющей коммерческую тайну, а также служебной информации ограниченного доступа в информационных системах ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения».

1.3. Информация, обрабатываемая в ИС ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения» является информацией, доступ к которой ограничен в соответствии с федеральными законами (далее – информация ограниченного

доступа).

1.4. Пользователем является каждый работник ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, обрабатываемым данным и средствам защиты.

1.5. Пользователь несет персональную ответственность за свои действия.

1.6. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о защите персональных данных ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», нормативными документами ФСТЭК России в области защиты информации, а также иными нормативными документами в области защиты информации утвержденными ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения».

1.7. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты информации и администратором информационной безопасности.

2. Организационные мероприятия по защите информации

2.1. Самостоятельный доступ в помещения, в которых размещены рабочие станции из состава ИС, разрешается постоянно работающим в них работникам в соответствии с утвержденными перечнями работников, имеющих право самостоятельного доступа в указанные помещения. Другие лица могут находиться в указанных помещениях только в присутствии работников, имеющих право самостоятельного доступа.

2.2. ПЭВМ, используемые для обработки информации ограниченного доступа, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора, лицами, не имеющими отношения обрабатываемой информации.

2.3. Вынос ПЭВМ, на которых проводится обработка информации ограниченного доступа, за пределы контролируемой территории объекта с целью их ремонта, замены и т.п. без согласования с ответственным за обеспечение защиты информации запрещен. При принятии решения о выносе ПЭВМ, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному.

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

2.5. Пользователю запрещается:

– передавать кому бы то ни было (в том числе родственникам) устно или письменно информацию ограниченного доступа;

– использовать информацию ограниченного доступа при подготовке открытых публикаций, докладов, научных работ и т.д.;

– выполнять работы с документами, содержащими информацию ограниченного доступа, на дому, выносить их из рабочих помещений, снимать

копии или производить выписки из таких документов без разрешения руководителя;

– копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

– накапливать ненужную для работы информацию, содержащую персональные данные;

– передавать или принимать без расписки документы, содержащие информацию ограниченного доступа;

– оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие информацию ограниченного доступа, а также оставлять незапертыми и неопечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими информацию ограниченного доступа;

– использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций, устанавливать дополнительно любые программные и аппаратные средства или изменять установленный алгоритм функционирования технических и программных средств (включая различные модемы и программы управления для любых Bluetooth контроллеров и устройств);

– несанкционированно открывать общий доступ к папкам на своей рабочей станции;

– 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 связанные со служебной необходимостью и не предусмотренные должностной инструкцией;

– сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИС.

– привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за обеспечение защиты информации (администратором информационной безопасности).

– осуществлять обработку информацию ограниченного доступа в присутствии посторонних (не допущенных к данной информации) лиц;

– записывать и хранить информацию, содержащую персональные данные, на неучтенных носителях информации;

– передавать информацию ограниченного доступа по каким-либо открытым (незащищенным) каналам связи.

– оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры).

3. Должностные обязанности пользователя

3.1. Работники, получившие доступ к информации ограниченного доступа, обязаны хранить в тайне данные сведения, ставшие им известными во время работы

или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации ограниченного доступа немедленно информировать руководителя структурного подразделения, специалиста по защите информации.

3.2. 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.

– Знать и соблюдать установленные требования по режиму обработки информации ограниченного доступа, учету, хранению и пересылке носителей информации, обеспечению безопасности информации, а также руководящих и организационно-распорядительных документов

– Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него штатными должностными обязанностями

– Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС.

– Выполнять требования администратора безопасности, касающиеся защиты информации.

– Контролировать использование интерфейсов ввода (вывода) информации на машинные носители персональных данных.

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

– Хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС.

– Использовать для работы, только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и flash-накопители.).

– Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него полномочиями пользователей по доступу к информационным ресурсам, программным и техническим средствам ИС (в составе технического паспорта на конкретную ИС).

– Соблюдать требования парольной политики (раздел 4 настоящей Инструкции).

– Соблюдать требования по организации антивирусной защиты (раздел 5 настоящей Инструкции).

– Соблюдать правила при работе в сетях общего доступа и (или) международного обмена (Интернет) и других (раздел 6 настоящей Инструкции).

3.3. Обо всех выявленных нарушениях, связанных с информационной безопасностью организации, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты информации.

3.4. Для получения консультаций по вопросам работы и настройке элементов ИС необходимо обращаться к Администратору ИС.

3.5. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, или нажать одновременно комбинацию клавиш <Win><L>.

4. Организация парольной защиты

4.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в АС, а также контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями осуществляет администратор информационной безопасности.

4.2. Полная плановая смена паролей в ИС проводится не реже одного раза в 3 месяца.

4.3. Правила формирования пароля:

– Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– Пароль должен состоять не менее чем из 8 символов.

– В пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;
2) строчные буквы английского алфавита от a до z;
3) десятичные цифры (от 0 до 9);
4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

– Запрещается выбирать пароли, которые уже использовались ранее.

4.4. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.

4.5. Правила хранение пароля:

– Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

– Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

4.6. Внеплановая смена личного пароля или удаление учетной записи

пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными работниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.7. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 4.6 настоящей Инструкции.

4.8. Хранение работником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором).

4.9. Лица, использующие паролирование, обязаны четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию, своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

5. Организация антивирусной защиты

5.1. В ИС допускаются к использованию только лицензионные и сертифицированные средства антивирусной защиты, имеющие действующий сертификат соответствия ФСТЭК России.

5.2. При загрузке ОС в автоматическом режиме должен проводиться антивирусный контроль системных файлов и памяти ПЭВМ.

5.3. Полный антивирусный контроль должен проводиться не реже одного раза в месяц. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая на съемных носителях (магнитных, лазерных дисках и flash-накопителях), а также файлы, помещаемые в электронные архивы.

5.4. Установка (изменение) системного и прикладного программного обеспечения осуществляется в соответствии с настоящей «Инструкцией…» и «Перечнем используемого программного обеспечения…».

5.5. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка.

5.6. При возникновении подозрения на наличие компьютерных вирусов (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен самостоятельно или вместе с администратором информационной безопасности провести внеочередной антивирусный контроль.

5.7. В случае обнаружения в результате антивирусной проверки зараженных компьютерными вирусами файлов пользователи автоматизированных систем обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных

вирусом файлов администратора информационной безопасности;

– провести необходимые антивирусные мероприятия.

5.8. Ответственность за организацию проведения своевременного антивирусного контроля возлагается на администратора информационной безопасности. Ответственность за непосредственное проведение антивирусного контроля и соблюдение требований настоящей «Инструкции…» возлагается пользователя конкретной рабочей станции из состава ИС.

6. Порядок обращения с машинными носителями информации

6.1. Под использованием машинных носителей информации (далее – МНИ) в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

6.2. В ИС допускается использование только учтенных МНИ, которые являются собственностью Оператора и подвергаются регулярной ревизии и контролю.

6.3. К машинным носителям конфиденциальной информации предъявляются те же требования, что и для стационарных АРМ.

6.4. Машинные носители информации ограниченного доступа предоставляются по инициативе Руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым Пользователем своих должностных обязанностей;

– возникновения у Пользователя производственной необходимости.

6.5. Съемные МНИ, предназначенные для обработки информации ограниченного доступа, учитываются в журнале учета машинных носителей информации работником, назначенным Министром экономики, торговли и предпринимательства Республики Мордовия.

6.6. На съемных МНИ любым доступным способом в удобном для просмотра месте проставляются следующие реквизиты: учетный номер с пометкой «ПДн» или «КТ». Допускается также проставление других реквизитов, идентифицирующих носитель: дата регистрации, подпись работника, ответственного за его регистрации и т.д.

6.7. Учтенные МНИ передаются работникам под расписку в журнале учета машинных носителей информации в соответствие со списком, утвержденным ().

6.8. Учет несъемного носителя информации (ЖМД) производится в составе СВТ, в котором он установлен. Такое средство вычислительной техники подлежит учету.

6.9. МНИ в случае стирания с него конфиденциальной информации, не снимается с учета.

6.10. Хранение МНИ, предназначенных для обработки информации ограниченного доступа, обеспечивают работники, назначенные приказом в условиях, исключающих несанкционированный доступ к информации.

6.11. Пришедшие в негодность или отслужившие установленный срок МНИ уничтожается по акту путем сжигания (разрезания на несколько частей) в присутствии лиц, подписывающих этот акт.

6.12. Порядок учета, хранения и обращения со съемными МНИ.

6.12.1. Все находящиеся на хранении и в обращении съемные МНИ подлежат учёту.

6.12.2. Каждый съемный МНИ с записанной на нем информацией ограниченного доступа, должен иметь этикетку, на которой указывается его уникальный учетный номер (п. 6.6).

6.12.3. Учет и выдачу съемных МНИ осуществляют уполномоченные работники, на которых возложены функции хранения МНИ.

6.12.4. Пользователи получают учтенный съемный носитель от уполномоченного работника для выполнения работ на конкретный срок. По окончании работ Пользователь сдает съемный носитель для хранения уполномоченному работнику.

6.12.5. В случае увольнения Пользователя, использующего личный зарегистрированный съемный носитель, уполномоченным работником производится стирание информации посредством многократного форматирования МНИ.

6.12.6. При использовании Пользователями МНИ необходимо:

– соблюдать требования настоящей Инструкции;

– использовать МНИ исключительно для выполнения своих служебных обязанностей;

– ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции;

– бережно относится к МНИ;

– обеспечивать физическую безопасность МНИ всеми разумными способами;

– извещать администраторов ИС о фактах утраты (кражи) МНИ.

6.12.7. При использовании машинных носителей информации ограниченного доступа запрещается:

– использовать МНИ в личных целях;

– передавать МНИ другим лицам (за исключением администраторов ИС);

– хранить съемные МНИ вместе с общедоступными данными, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съёмные МНИ из служебных помещений для работы с ними на дому и т. д.

6.12.8. Любое взаимодействие (обработка, прием/передача информации), инициированное работником между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, согласованных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование МНИ.

6.12.9. В случае выявления фактов несанкционированного и/или нецелевого использования МНИ инициализируется служебная проверка, проводимая комиссией, состав и полномочия которой определяется приказом. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю для принятия мер согласно локальным нормативным актам и действующему законодательству.

6.12.10. Информация, хранящаяся на МНИ, подлежит обязательной проверке на отсутствие вредоносного ПО.

6.12.11. При отправке или передаче информации ограниченного доступа адресатам на съемные МНИ записываются только предназначенные адресатам данные. Отправка информации ограниченного доступа адресатам на съемных МНИ осуществляется в порядке, установленном для документов для служебного пользования.

6.12.12. Вынос съемных МНИ для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя подразделения.

6.12.13. В случае утраты или уничтожения МНИ либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей информации.

6.12.14. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему МНИ изымаются уполномоченным работником, на которого возложены функции хранения МНИ в ГБУЗ Республики Мордовия «Детская поликлиника №1».

7. Правила работы в сетях общего доступа и (или) международного информационного обмена

7.1. Подключение средств вычислительной техники к международным информационным сетям (МИС) общего пользования представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).

7.2. Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

– проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;

– перенос в АС разрушающего программного обеспечения (внедрение программных закладок, вирусов);

– выбор и использование законным пользователем системы неудачных паролей;

– несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.

7.3. При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

– получить информацию об адресной структуре сети;

– установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);

– получить информацию о пользователях сети;

– попытаться подключиться к информационным ресурсам сети;

– вызвать отказ в обслуживании легальных пользователей.

7.4. Кроме явных, то есть непосредственно направленных на сеть организации, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими работниками организации. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

7.5. По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам).

7.6. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) на элементах ИС, должна проводиться при служебной необходимости.

7.7. При работе в сетях общего доступа запрещается:

– Осуществлять работу при отключенных средствах защиты (к техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся: системы разграничения прав доступа, межсетевые экраны, СКЗИ, системы построения защищенных виртуальных сетей (Virtual Private Network – VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.).

– Передавать по сетям общего доступа защищаемую информацию без использования средств межсетевого экранирования и СКЗИ.

– Запрещается загружать из сетей общего доступа программное обеспечение и другие файлы.

– Запрещается посещение сайтов сомнительной репутации (содержащие нелегально распространяемое ПО и другие).

– Запрещается нецелевое использование подключения к сетям общего доступа.

7.8. Пользователь обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

– знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;,

– хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты, установленной на АС;

– материальные носители информации с записанной на них входящей документированной информации полученной в процессе работы с информационными ресурсами МИС общего пользования передавать для учета в несекретное делопроизводство;

– при пользовании электронной почтой запрещается передача сведений, содержащих информацию ограниченного доступа, без применения специальных мер

защиты.

7.9. Автоматизированные системы, имеющие подключение к МИС общего пользования, в обязательном порядке оснащаются антивирусным программным обеспечением, обновление антивирусной базы которого производится непосредственно перед каждым началом работы. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения. Автоматизированные системы, имеющие подключение к МИС общего пользования, регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.

7.10. Ведение учета рабочих станций, подключенных к МИС общего пользования, организуется администратором информационной безопасности.

7.11. Администратор информационной безопасности имеет право вносить предложения по порядку и ограничениям использования ИС, а также выдавать рекомендации и предъявлять дополнительные требования по защите информации от несанкционированного доступа.

8. Заключение

8.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует без ограничения срока.

8.2. Пользователь несет ответственность за соблюдение требований настоящей Инструкции, а также других нормативных документов в области защиты персональных данных в ГБУЗ Республики Мордовия «Детская поликлиника №1.

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

С инструкцией ознакомлен:

№	Должность	Ф.И.О.	Подпись	Дата

№	Должность	Ф.И.О.	Подпись	Дата

№	Должность	Ф.И.О.	Подпись	Дата