ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ ТУЛЬСКОЙ ОБЛАСТИ
«ТУЛЬСКИЙ ПСИХОНЕВРОЛОГИЧЕСКИЙ ИНТЕРНАТ»

П Р И К А З

01.03.2023 **№99-осн**

Об утверждении инструкции администратора безопасности информационных систем в ГУ ТО «Тульский психоневрологический интернат»

В целях обеспечения выполнения требований Федерального закона Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» в ГУ ТО «Тульский психоневрологический интернат»

п р и к а з ы в а ю:

1. Утвердить инструкцию администратора безопасности информационных систем в ГУ ТО «Тульский психоневрологический интернат» (Приложение №1).
2. Настоящий приказ вступает в силу со дня подписания.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор **И.Ю. Гамова**

Приложение №1
к приказу ГУ ТО «Тульский
психоневрологический интернат»
№ 99- осн
от «01»марта 2023 г.

Инструкция администратора безопасности информационных систем в ГУ ТО «Тульский психоневрологический интернат»

1. Общие положения

Настоящая Инструкция определяет основные обязанности, права и ответственность администратора безопасности информационных систем в ГУ ТО «Тульский психоневрологический интернат».

Администратор безопасности (далее АБ) является должностным лицом, ответственным за защиту информационных систем (автоматизированных систем и информационных систем персональных данных) ГУ ТО «Тульский психоневрологический интернат» (далее ИС) от несанкционированного доступа к информации, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИС.

Функции АБ ИС возлагаются на работника ГУ ТО «Тульский психоневрологический интернат».

АБ при исполнении своих функций непосредственно подчиняется директору ГУ ТО «Тульский психоневрологический интернат».

АБ в своей работе руководствуется действующим законодательством Российской Федерации в области защиты информации, локальными нормативными правовыми актами и организационно-распорядительными документами (далее ОРД) ГУ ТО «Тульский психоневрологический интернат», регламентирующими защиту конфиденциальной информации, в том числе персональных данных, положениями настоящей Инструкции.

АБ должен иметь специальное рабочее место, размещенное в помещении так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей. Рабочее место АБ должно быть оборудовано средствами физической защиты личный сейф, подключением к ИС, а также средствами контроля за техническими средствами защиты.

АБ осуществляет методическое руководство пользователями ИС в вопросах обеспечения безопасности конфиденциальной информации, в том числе персональных данных. Требования АБ к пользователям, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИС.

АБ несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИС, состояние и поддержание установленного уровня защиты ИС.

2. Обязанности

АБ обязан:

– устанавливать и настраивать средства и системы защиты информации (далее СЗИ) ИС и поддерживать их функционирование;

– восстанавливать работоспособность СЗИ от несанкционированного доступа к информации (далее НСД) в случае их отказа;

– восстанавливать работоспособность средств криптографической защиты информации (далее СКЗИ) в случае их отказа;

– контролировать эксплуатацию в ИС СЗИ и СКЗИ в соответствии с требованиями эксплуатационной и технической документации к ним;

– обеспечивать текущий, после сбоев, и периодический (не реже 1 раза в месяц) контроль наличия и работоспособности СЗИ на автоматизированных рабочих местах (далее АРМ) пользователей ИС;

– разрабатывать и обеспечивать соответствие текущим условиям обработки конфиденциальной информации, в том числе персональных данных, ОРД ГУ ТО «Тульский психоневрологический интернат»;

– контролировать наличие уведомления об обработке персональных данных и его соответствие текущим условиям обработки персональных данных, обеспечивать своевременное внесение изменений в уведомление при изменении условий обработки персональных данных;

– разрабатывать и поддерживать в актуальном состоянии разрешительную систему доступа к ИС;

– осуществлять контроль электронных журналов СЗИ от НСД на АРМ пользователей ИС, анализ электронных журналов регистрации событий информационной безопасности для предотвращения попыток НСД (не реже 1 раза в месяц);

– осуществлять контроль электронных журналов общесистемного и прикладного ПО с целью выявления инцидентов информационной безопасности (не реже 1 раза в месяц);

– поддерживать в актуальном состоянии журналы учета, ведение которых осуществляется в соответствии с требованиями законодательства Российской Федерации в области защиты информации;

– проводить мероприятия по контролю соблюдения режима защиты персональных данных;

– фиксировать результаты проведенных мероприятий по контролю соблюдения режима защиты персональных данных;

– проводить учет, регистрацию и выдачу машинных носителей информации (персональных данных), обеспечивать ведение учетной документации, уничтожение носителей установленным порядком;

– выполнять разработку, хранение и актуализацию таблиц допуска пользователей к защищаемым ресурсам с указанием разрешенных режимов работы и уровней доступа к защищаемым ресурсам;

– обеспечивать разработку, хранение и актуализацию таблиц доступа пользователей к защищаемым ресурсам с указанием идентификаторов и

аутентификаторов (паролей) пользователей;

– проводить выработку паролей с использованием вычислительной техники и специального ПО и оформление парольной документации для информационных ресурсов, не имеющих возможность обеспечить назначение пароля доступа к данному ресурсу непосредственно пользователем;

– проводить плановую смену паролей учетных записей пользователей ИС по истечении их срока действия (90 суток);

– блокировать учетную запись пользователя при выявлении факта компрометации аутентификатора;

– блокировать учетную запись пользователя при увольнении, а также при предоставлении отпуска по уходу за ребёнком до 3-х лет на основании соответствующих приказов;

– проводить инструктаж работников ГУ ТО «Тульский психоневрологический интернат» по инструкциям, регламентирующим защиту конфиденциальной информации, в том числе персональных данных, под подпись в листах ознакомления (не реже 1 раза в полгода);

– осуществлять обход АРМ с целью контроля соблюдения пользователями ИС требований инструкций, регламентирующих защиту конфиденциальной информации, в том числе персональных данных, а также утвержденной технологии обработки информации в ИС (не реже 1 раза в квартал);

– оказывать помощь пользователям ИС в части применения СЗИ и консультировать по вопросам информационной безопасности;

– представлять непосредственному руководителю отчеты о состоянии защиты ИС, нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3. Права

АБ имеет право:

– требовать от пользователей ИС выполнения установленной технологии обработки информации, инструкций, регламентирующих защиту конфиденциальной информации, в том числе персональных данных, в ИС;

– информировать непосредственное руководство о фактах нарушения установленной технологии обработки информации и требований инструкций;

– в случаях, не терпящих отлагательства, обращаться с докладами и предложениями по принятию необходимых мер по обеспечению безопасности информации непосредственно к директору ГУ ТО «Тульский психоневрологический интернат»;

– изменять пароль или блокировать учетную запись пользователя при явной или неявной компрометации;

– блокировать работу АРМ пользователей ИС в случаях нарушений установленной технологии обработки информации до устранения пользователем выявленных нарушений;

– обращаться к директору ГУ ТО «Тульский психоневрологический интернат» с предложением о приостановке обработки информации в ИС в случаях выявленных нарушений требований по защите информации до полного устранения нарушений;

– принимать участие в расследовании инцидентов информационной безопасности.

4. Ответственность

На АБ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

АБ несет ответственность за неисполнение (ненадлежащее исполнение) своих обязанностей в пределах, определенных административным, уголовным и гражданским законодательствами Российской Федерации.