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

ИНСТРУКЦИЯ АДМИНИСТРАТОРА
информационной безопасности
ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения»

СОДЕРЖАНИЕ

1. Общие положения

1.1.Обязанности Администратора информационной безопасности возлагаются на программиста ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения».

1.1. Администратор информационной безопасности отвечает за поддержание необходимого уровня безопасности информационных ресурсов подлежащих защите, а также правильность использования и нормальное функционирование средств защиты информации (СЗИ), подготовку сотрудников по вопросам безопасной обработки информации в информационных систем ГАОУДПО Республики Мордовия «Мордовский республиканский центр повышения квалификации специалистов здравоохранения». (далее – ИС).

1.2. Администратор информационной безопасности в своей работе руководствуется настоящей Инструкцией, а также руководящими и нормативными документами ФСТЭК России и ФСБ России в области обеспечения безопасности информации.

1.3. Администратор информационной безопасности является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИС и ее ресурсов на этапах ее эксплуатации и модернизации.

1.4. Администратор информационной безопасности в вопросах защиты информации взаимодействует с ответственным за обеспечение защиты информации ограниченного доступа (персональные данные, коммерческая тайна, служебная информация).

1.5. Методическое руководство работой Администратора информационной безопасности осуществляется ответственным за обеспечение защиты информации ГБУЗ Республики Мордовия «Детская поликлиника №1», назначенным из числа руководителей в соответствии с указом Главы Республики Мордовия № 193-УГ от 13.06.2018 г. «О мерах по защите информации ограниченного доступа в Республике Мордовия».

1.6. Администратор информационной безопасности должен иметь специальное рабочее место, размещенное таким образом, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.7. Рабочее место Администратора информационной безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или др.), а так же средствами контроля за техническими средствами защиты.

1.8. Требования Администратора информационной безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИС.

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

2. Функции администратора информационной безопасности

2.1. Администратор информационной безопасности осуществляет настройку и сопровождение системы защиты информации (СЗИ), при этом:

– осуществляет установку (инсталляцию) компонентов программного обеспечения, в том числе определяет компоненты, подлежащие установке, настройку параметров установки компонентов, контроль за установкой компонентов программного обеспечения.

– реализует полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов на основе утвержденного руководством списка сотрудников, участвующих в обработке информации;

– назначает пароли к информационным ресурсам и вводит в базу данных системы защиты описание полномочий доступа пользователей к защищаемым ресурсам;

– своевременно удаляет описание пользователя из базы данных при увольнении или перемещении сотрудника;

– периодически инициирует смену паролей пользователями для доступа в ИС.

2.2. Осуществляет настройку и сопровождение подсистемы управления доступом:

– назначает и следит за периодической сменой паролей пользователей;

– определяет перечень съемных носителей информации, разрешенных к использованию в ИС.

2.3. Осуществляет настройку и сопровождение подсистемы обнаружения вторжений:

– по мере необходимости производит обновления баз решающих правил.

2.4. Осуществляет настройку и сопровождение подсистемы регистрации и учета:

– периодически производит контроль состояния модулей сбора информации, устраняет возникающие ошибки и сбои, производить выгрузку журнала регистрации событий.

– проводит регулярный анализ журналов СЗИ, для своевременного выявления фактов несанкционированного доступа к защищаемым ресурсам, ошибок, сбоев и других инцидентов.

– своевременно информирует руководство о несанкционированных действиях персонала и организует расследование попыток НСД.

2.5. Сопровождает подсистемы обеспечения целостности рабочего программного обеспечения и СЗИ НСД:

– проводит периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий пользователей;

– осуществляет восстановление системы защиты от НСД при сбоях;

– проводит контроль соответствия общесистемной программной среды эталону;

– обеспечивает поддержание установленного порядка и соблюдение требований инструкции по антивирусной защите;

– производит периодический (не реже одного раза в неделю) контроль

целостности программной и информационной частей межсетевых экранов, посредством сохранения файлов микропрограмм и конфигураций на локальный компьютер с последующим расчетом контрольных сумм.

2.6. Производит настройку и сопровождение подсистемы защиты от вирусов и программно-математических воздействий (ПМВ):

– производит настройку автоматической проверки на наличие вредоносных программ;

– следит за обновлениями баз данных, на признаки вредоносных компьютерных программ (вирусов).

– следит за исполнением пользователями требований инструкции по проведению антивирусного контроля.

2.7. Проводит анализ уязвимостей (при помощи установленных в ИС средств анализа защищенности), связанных с недостатками операционных систем, с ошибками в конфигурации прикладного ПО ИС, ошибками конфигурирования сетевого оборудования, которые могут быть использованы нарушителем для реализации атаки на систему. Проверка производится при изменении программной и/или аппаратной среды ИС, при выявлении фактов НСД, а также периодически не реже одного раза в месяц. При выявлении уязвимостей, представляющих угрозу безопасности ИС, администратор информационной безопасности принимает необходимые меры по их устранению. При необходимости, администратор информационной безопасности вправе потребовать от пользователей ИС приостановить обработку информации до устранения угроз безопасности.

2.8. Проводит периодическое (не реже одного раза в три месяца) регламентное тестирование функций межсетевого экранирования в соответствии с утвержденным Регламентом, так же ограничивает посредством средств межсетевого экранирования возможности удаленного подключения к компонентам ИС (при наличии средств межсетевого экранирования).

2.9. Участвует в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Должностные обязанности администратора информационной безопасности

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций по защите информации и распоряжений, регламентирующих порядок действий по защите ПДн.

3.2. Обеспечивать функционирование и поддерживать работоспособность средств защиты информации, обеспечивать установку, настройку и своевременное обновление элементов ИС:

– программного обеспечения ИС (операционные системы, прикладное и специальное ПО);

– аппаратных средств;

– аппаратных и программных средств защиты информации.

3.3. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИС.

3.4. В случае отказа работоспособности технических средств и программного обеспечения ИС, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.5. Не допускать использования, хранения и размножения в ИС программных продуктов и носителей информации, непосредственно не связанных со служебной деятельностью.

3.6. Проводить периодическое резервное копирование обрабатываемых данных на учтенные носители информации.

3.7. Реагировать на поступающие в информационную систему незапрашиваемые электронные сообщения (письма, документы) и иной информации, не относящейся к функционированию информационной системы (защита от спама).

3.8. Пресекать действия пользователей, которые могут привести к компрометации паролей и (или) персональных идентификаторов.

3.9. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля операторами ИС.

3.10. Информировать ответственного за обеспечение защиты информации ограниченного доступа (персональные данные, коммерческая тайна, служебная информация) о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИС.

3.11. Контролировать работу пользователей ИС в части обеспечения безопасности информации и неизменности настроек СЗИ, выполнения парольной политики, проведения антивирусного контроля, работы в сетях общего пользования и (или) международного обмена.

3.12. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

3.13. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

3.14. Присутствовать при выполнении технического обслуживания элементов ИС (в т.ч. ' обновлении баз данных), сторонними физическими лицами и организациями.

3.15. Контролировать неизменность перечня установленного программного обеспечения в ИС.

3.16. Пресекать действия пользователей, которые пытаются установить на компьютеры новое оборудование и ПО, не связанное с исполнением должностных обязанностей.

3.17. Своевременно анализировать журналы учета событий, регистрируемых ОС и средствами защиты, с целью выявления возможных нарушений и попыток НСД.

3.18. Своевременно отключать службы удаленного администрирования при отсутствии потребности удаленного управления сетевыми объектами ИС.

3.19. Не допускать использования для каналов удаленного управления нестандартных сетевых портов.

4. Организация антивирусной защиты

4.1. Настоящий раздел Инструкции определяет требования к организации защиты ИС от разрушающего воздействия компьютерных вирусов.

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

4.3. Администратор информационной безопасности несет ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля.

4.4. В ИС запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

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

4.6. Администратор информационной безопасности ежедневно осуществляет установку пакетов обновлений вирусных баз, осуществляет контроль их подключения к антивирусному пакету и проверку жесткого диска и съемных носителей на наличие вирусов.

4.7. Полный антивирусный контроль рабочих станций ИС 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.

4.8. Непосредственно после установки (изменения) системного и прикладного программного обеспечения, должна быть выполнена антивирусная проверка.

4.9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) администратор информационной безопасности должен провести внеочередной антивирусный контроль.

4.10. В случае обнаружения в результате антивирусной проверки зараженных компьютерными вирусами файлов администратор информационной безопасности обязан приостановить работу и провести необходимые антивирусные мероприятия.

4.11. В случае обнаружения не поддающегося лечению вируса, администратор информационной безопасности обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность системы. В случае отказа – произвести восстановление соответствующего программного обеспечения.

5. Организация парольной защиты

5.1. Администратор информационной безопасности осуществляет организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИС, а также контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями.

Пароли должны формироваться с учетом следующих требований:

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

– Пароль должен состоять не менее чем из 6 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, 123456 и т.п.).

– Запрещается использования заводских, паролей для ограничения доступа к службам удаленного администрирования коммутационного и серверного оборудования, используемого в составе ИС.

– Запрещается выбирать пароли, которые уже использовались ранее.

5.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

5.4. 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 информационной безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.5. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 5.4 настоящей Инструкции.

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

5.7. Администратор информационной безопасности осуществляет повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования.

5.8. Администратор информационной безопасности осуществляет контроль использования учетных записей пользователей. При приеме на работу нового сотрудника, для него создают новую учетную запись и предоставляют необходимые права доступа. При увольнении сотрудника аналогичным образом осуществляется блокировка или удаление учетных записей сотрудника в информационной системе.

6. Опломбирование ПЭВМ

6.1. Администратор информационной безопасности осуществляет опломбирование ПЭВМ для предотвращения вскрытия.

6.2. Пломбы, используемые для контроля вскрытия должны располагаться таким образом, чтобы исключить вскрытие без повреждения пломбы и обеспечить возможность визуального контроля за состоянием пломбы.

6.3. При опечатывании (опломбировании) системного блока пломбами следует размещать их на разрыв на боковые панели корпуса вместе с несъёмными частями корпуса. На печатях (пломбах) должны быть указаны дата опломбирования, фамилия и подпись администратора информационной безопасности.

7. Регистрация событий информационной безопасности

7.1. Администратор информационной безопасности определяет перечень событий безопасности, подлежащих регистрации. Перечень определяется на этапе проектирования ИС, модифицируются в процессе ее использования.

События безопасности, подлежащие регистрации, должны определяться Администратором информационной безопасности с учетом способов реализации угроз безопасности для ИС.

При достижении предельного размера, журнал может переписать старые данные новыми, или прекратить регистрацию событий. Для этого администратор информационной безопасности должен архивировать журналы событий информационной безопасности в течение 3 лет.

События безопасности, а также сроки хранения должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС.

7.2. Для каждого регистрируемого типа событий безопасности Администратор информационной безопасности определяет состав и содержание информации о событиях безопасности.

Состав и содержание информации о событиях безопасности должны обеспечивать возможность идентификации в соответствии с методическим

документом «Меры защиты информации в государственных информационных системах» утвержденным ФСТЭК России 11 февраля 2014 года:

- типа события безопасности.
- даты и времени события безопасности.
- идентификационной информации источника события безопасности.
- результата события безопасности.
- субъекта доступа.

7.3. Администратор информационной безопасности обеспечивает регистрацию установленных в пункте 7.1 настоящей Инструкции событий безопасности, а также устанавливает состав и содержание регистрируемой информации в соответствии с пунктом 7.2 настоящей Инструкции с использованием средств защиты информации, установленных в ИС.

Объем памяти для хранения информации о событиях безопасности рассчитывается Администратором информационной безопасности с учетом типов событий безопасности, их состава, содержания, прогнозируемой частоты возникновения, а также срока их хранения.

7.4. Просмотр журналов событий в ИС осуществляется Администратором информационной безопасности при возникновении инцидента информационной безопасности или, в случае отсутствия инцидентов, не реже одного раза в две недели.

В случае обнаружения сбоев в системе регистрации событий, Администратор информационной безопасности:

- выясняет причину сбоя (переполнение журнала, отсутствие связи с базой данных и т.д.).
- устраняет причину сбоя путем изменения параметров регистрации в соответствии с пунктами 7.2 и 7.3 настоящей инструкции.

7.5. В ИС Администратором информационной безопасности используются следующие методы защиты информации о событиях безопасности:

- логическое ограничение доступа к местам хранения журналов событий;
- управление журналами событий. доступ к управлению журналами должен быть разрешен только для привилегированных пользователей ИС.

Контроль реализации методов защиты осуществляется Администратором информационной безопасности не реже одного раза в год.

8. Организация парольной защиты BIOS

8.1. Администратором информационной безопасности должен быть установлен пароль администратора на BIOS (Supervisor Password) для исключения вхождения лиц, не ответственных за администрирование АРМ в режим конфигурирования BIOS.

8.2. Пароль может состоять только из букв английского алфавита, причем верхний и нижний регистры не различаются, и цифр. Максимальная длина пароля – восемь символов.

8.3. Также рекомендуется определить в BIOS установки, исключающие возможность загрузки операционной системы, отличной от установленной на

жестком диске: отключается возможность загрузки с гибкого диска, привода CD-ROM, исключаются прочие нестандартные виды загрузки ОС, включая сетевую загрузку.

9. Разграничения прав доступа пользователей

9.1. Администратором информационной безопасности должно быть обеспечено разделение полномочий пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями).

10. Контроль интерфейсов ввода вывода

10.1. Администратор информационной безопасности осуществляет контроль использования интерфейсов ввода-вывода.

10.2. В случае необходимости администратор информационной безопасности может применять следующие меры, исключающие возможность использования запрещенных интерфейсов ввода-вывода:

- опечатывание интерфейсов ввода (вывода);
- использование механических запирающих устройств;
- удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);
- применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

С инструкцией ознакомлен:

_____	_____	_____	_____
Ф.И.О.	Должность	Подпись	Дата