# МИНИСТЕРСТВО ОБРАЗОВАНИЯ ПЕНЗЕНСКОЙ ОБЛАСТИ

# П Р И К А З

16.03.2015 № 193/01-04

г. Пенза

**Об определении лица, ответственного за управление (администрирование) системой защиты информации государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»**

В целях выполнения требований Федерального закона от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспертному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», п р и к а з ы в а ю:

1. Определить заместителя директора регионального центра обработки информации государственного автономного образовательного учреждения дополнительного профессионального образования «Институт регионального развития Пензенской области» Голоба Олега Эдуардовича лицом, ответственным за управление (администрирование) системой защиты информации государственной информационной системы «Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (по согласованию).

2. Утвердить прилагаемую инструкцию лица, ответственного за управление (администрирование) системой защиты информации государственной информационной системы Пензенской области

«Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (далее – администратор безопасности).

3. Настоящий приказ разместить (опубликовать) на официальном сайте Министерства образования Пензенской области в информационно – телекоммуникационной сети «Интернет».

4. Контроль за исполнением настоящего приказа оставляю за собой.

Министр А.Н. Фомин

Утверждено
приказом Министерства образования
Пензенской области
от 26032015 № 193/01-04

# Инструкция администратора безопасности

## 1. Общие положения

1.1. Инструкция администратора безопасности (далее - Инструкция) определяет обязанности, права и ответственность работника, назначенного ответственным за управление (администрирование) системой защиты информации государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования».

1.2. В своей деятельности администратор безопасности руководствуется законодательством Российской Федерации, иными нормативными правовыми актами Российской Федерации сфере обработки и защиты информации, в том числе персональных данных (далее – защищаемая информация), нормативными актами Министерства образования Пензенской области, а также настоящей Инструкцией.

1.3. Администратор безопасности назначается приказом Министерства образования Пензенской области и обеспечивает в пределах своих функциональных обязанностей безопасность защищаемой информации, обрабатываемой, передаваемой и хранимой в государственной информационной системе Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (далее - РИС ГИА).

## 2. Обязанности администратора безопасности

Администратор безопасности при эксплуатации РИС ГИА обязан:

2.1 Соблюдать требования законодательных и нормативных документов по обеспечению безопасности защищаемой информации.

2.2 Выполнять и принимать меры к выполнению требований организационно-распорядительной документации по организации обработки и защиты информации в РИС ГИА.

2.3 Осуществлять установку, настройку и сопровождение технических средств защиты РИС ГИА.

2.4. Осуществлять организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в РИС ГИА, контроль действий пользователей РИС ГИА при их работе с персональными идентификаторами и паролями доступа, в том числе:

– создавать, присваивать, уничтожать персональные идентификаторы и пароли доступа к техническим средствам и информационным ресурсам РИС ГИА;

– хранить, выдавать, инициализировать, блокировать средства аутентификации (пароли, аппаратные идентификаторы) и принимать меры в случае утраты или компрометации средств аутентификации;

– вести, надежно хранить и в установленном порядке уничтожать журнал учета выдачи первичных паролей к РИС ГИА;

– надежно хранить и вести учет аппаратных средств аутентификации (при наличии) по журналу учета аппаратных средств;

– надежно хранить и в установленном порядке уничтожать журнал учета аппаратных средств аутентификации;

– обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены и изменять свой собственный пароль не реже 1 раза в месяц. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере индивидуальных аппаратных идентификаторов;

– выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов (при наличии).

2.5. Осуществлять и контролировать разграничение доступа пользователей к ресурсам и информации РИС ГИА путем настройки программно-технических средств и средств защиты информации:

– управлять учетными записями (заведение, активацию, блокирование, уничтожение) пользователей РИС ГИА, в том числе внешних пользователей, при этом осуществлять блокирование учетной записи при превышении времени неиспользования более 90 дней, максимальное количество неуспешных попыток аутентификации до блокировки до 5 попыток, блокирование сеанса доступа в РИС ГИА после установленного времени бездействия (неактивности) пользователя 15 минут или по его запросу;

– обеспечивать актуальность, сохранность и конфиденциальность матрицы доступа к ресурсам РИС ГИА;

– вести учет технических средств удаленного доступа (в случае использования удаленного доступа через сеть Интернет к ресурсам РИС ГИА) с документальным оформлением в журнале учета разрешенных средств удаленного доступа, а также осуществлять выдачу, хранение технических средств удаленного доступа, установку и настройку программного обеспечения, его обновление, антивирусную защиту технических средств удаленного доступа и контролировать использование технических средств удаленного доступа к РИС ГИА;

– вести учет мобильных технических средств (в случае использования мобильных технических средств для доступа к ресурсам РИС ГИА) с документальным оформлением в журнале учета разрешенных мобильных технических средств и контролировать использование мобильных технических средств для доступа к РИС ГИА.

2.6. Вести учет, хранение и выдачу машинных носителей информации, в том числе:

– организовывать и контролировать процедуру уничтожения (стирания) или обезличивания персональных данных при передаче между пользователями, в сторонние организации для ремонта или утилизации, а также факт уничтожения машинного носителя информации;

– участвовать в составе комиссии по проверке наличия и состояния машинных носителей информации;

– в случае выхода из строя, порчи или утраты машинного носителя персональных данных докладывать об инциденте ответственному за организацию обработки персональных данных.

2.7. Контролировать проведение резервного копирования технических средств РИС ГИА.

2.8. Осуществлять настройку журналов регистрации событий информационной безопасности в программном обеспечении РИС ГИА и средств защиты информации в части касающейся, фиксировать информацию о событиях безопасности в РИС ГИА, не подлежащую автоматической регистрации в журнале событий информационной безопасности РИС ГИА.

Вести, надежно хранить журнал событий информационной безопасности государственной информационной системы РИС ГИА.

2.9. Осуществлять установку, конфигурирование и обеспечивать централизованное управление средствами антивирусной защиты в РИС ГИА, в том числе:

– установку и обновление лицензионных ключей средств антивирусной защиты, обновлений базы признаков вредоносных компьютерных программ (вирусов);

– принимать меры по локализации и удалению вредоносного программного обеспечения (далее – ПО), выявлению источника и способа проникновения вредоносного ПО;

– восстановление работоспособности программных средств и информационных массивов программных средств, поврежденных вредоносным ПО;

– ограничение доступа пользователей на АРМ к настройкам установленных средств антивирусной защиты;

– контроль за работой пользователей РИС ГИА по применению на непосредственных АРМ средств антивирусной защиты,

– немедленно оповещать ответственного за организацию обработки персональных данных, ответственного за защиту информации в РИС ГИА об обнаружении вредоносного ПО на серверном или телекоммуникационном оборудовании.

2.10. Осуществлять исполнение мероприятий по выявлению (поиску), анализу и устранению уязвимостей в РИС ГИА (с разработкой плана устранения выявленных уязвимостей):

– осуществлять мониторинг наличия обновлений, выпускаемых разработчиками ПО, используемого в РИС ГИА, и средств защиты информации в части касающейся;

– проводить обновление ПО средств защиты информации, ПО аппаратных средств в случае выявления уязвимостей, связанных с устаревшими версиями ПО;

– проводить оценку изменений в ПО на условия изменения конфигурации РИС ГИА и системы защиты информации;

– выполнять необходимые настройки, проводить тестирование работоспособности после установки обновлений ПО и вносить необходимые изменения в эксплуатационную документацию;

– проводить контроль установки обновлений ПО (проводить проверку соответствия версии общесистемного, прикладного и специального ПО, установленного в РИС ГИА, а также ПО средств защиты информации и выпущенного разработчиком, наличия отметок в Техническом паспорте и в эксплуатационной документации);

– не реже 1 раза в полгода проводить контроль на соответствие техническому паспорту РИС ГИА состава технических средств, ПО и средств защиты информации;

– осуществлять проверку наличия и сроков действия лицензий на установленное ПО РИС ГИА и ПО системы защиты информации (далее – СЗИ), сертификатов соответствия на примененные в РИС ГИА и СЗИ аппаратные средства;

– ежемесячно проводить контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

– немедленно уведомлять ответственного за организацию обработки персональных данных, ответственного за защиту информации в РИС ГИА при получении информации о прекращении поддержки разработчиком используемого ПО в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки;

– проводить проверку технического состояния аппаратных средств, журналов планово-профилактического обслуживания аппаратных средств РИС ГИА за период контроля защищенности РИС ГИА, перечня событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств, конфигурацию соединений и установки аппаратных средств, условия их эксплуатации;

– осуществлять контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ, в случае выявления сбоев, отказов или несоответствия настройкам, организовывать восстановление ПО и СЗИ;

– участвовать в организованной ответственным за организацию обработки персональных данных проверке состояния и актуальности организационно-распорядительной документации по обеспечению безопасности защищаемой информации.

2.11. Контролировать выполнение требований к размещению устройств вывода информации в контролируемых зонах, расположение технических устройств и физический доступ к ним.

2.12. Проводить анализ планируемых изменений в конфигурацию РИС ГИА и СЗИ и принимать решение о необходимости внесения изменений в конфигурацию РИС ГИА и СЗИ, осуществлять проверку корректности изменения конфигурации и при необходимости совместно с ответственным за организацию обработки персональных данных организовать актуализацию документации по вопросам обеспечения безопасности защищаемой информации, а также контроль эффективности обеспечения безопасности защищаемой информации в РИС ГИА, в том числе персональных данных.

2.13. Проводить анализ событий информационной безопасности (далее - ИБ), подтверждать/опровергать является ли событие ИБ инцидентом ИБ, оформлять отчет об инциденте и предоставлять его ответственному за организацию обработку персональных данных, ответственному за защиту информации в РИС ГИА и в случае необходимости пользователям РИС ГИА.

Проводить в составе комиссии анализ выявленного инцидента ИБ.

Принимать меры по устранению последствий инцидента (проводить процедуру смены паролей пользователями, пересматривать и обновлять с учетом содержания инцидента матрицу доступа к ресурсам РИС ГИА, организовать переустановку ПО РИС ГИА и СЗИ с дистрибутивных носителей используемого ПО, удалять вредоносное ПО, организовать восстановление данных из резервных копий, организовать устранение уязвимостей, проверить состав конфигурации РИС ГИА и системы защиты информации и при необходимости восстановить конфигурацию в соответствии с эксплуатационной документацией).

Формировать перечень мероприятий, направленных на предупреждение повторного возникновения инцидента.

2.14. Обеспечивать управление программным обеспечением РИС ГИА, в том числе:

- формировать и согласовывать с ответственным за защиту информации в РИС ГИА перечень программного обеспечения и (или) его компонентов, запрещенных к использованию в РИС ГИА;

- устанавливать (инсталлировать) программное обеспечение и (или) его компоненты, обновления программного обеспечения РИС ГИА в соответствии с инструкцией по управлению программным обеспечением РИС ГИА и эксплуатационной документацией;

- осуществлять контроль за установкой компонентов программного обеспечения РИС ГИА (состав компонентов, параметры установки, конфигурация компонентов);

- обеспечивать контроль установленного (инсталлированного) в РИС ГИА программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в РИС ГИА, на предмет отсутствия программного обеспечения, запрещенного к установке;

- вносить изменения в технический паспорт РИС ГИА и в эксплуатационную документацию в соответствии с порядком управления конфигурацией РИС ГИА и ее системы защиты информации.

2.15. Для реализации возложенных на администратора безопасности обязанностей в РИС ГИА обеспечивается выделение для него автоматизированного рабочего места.

## 3. Права администратора безопасности

3.1. Администратор безопасности РИС ГИА имеет право:

– привлекать к работам, связанным с обеспечением безопасности информации, системных администраторов РИС ГИА;

– требовать от пользователей РИС ГИА выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности РИС ГИА;

– докладывать ответственному за организацию обработки персональных данных, ответственному за защиту информации, о нарушениях или невыполнении пользователями требований обеспечению безопасности информации;

– вносить предложения по модернизации и совершенствованию системы защиты информации в РИС ГИА ответственному за организацию обработки персональных данных;

– останавливать обработку информации в РИС ГИА в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации.

–

## 4. Ответственность

4.1. Работник, назначенный ответственным за управление (администрирование) системой защиты информации РИС ГИА, несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией, в соответствии с действующим законодательством Российской Федерации.