МИНИСТЕРСТВО ОБРАЗОВАНИЯ ПЕНЗЕНСКОЙ ОБЛАСТИ

ПРИКАЗ

26.02.2026 № 99/01-04

г. Пенза

Об утверждении и вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты информации, обрабатываемой 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»

В целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями), постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (с последующими изменениями), приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (с последующими изменениями), приказа Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», приказом Министерства образования Пензенской области от 11.11.2024 № 16-192 «О государственной информационной системе Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (с последующими изменениями), руководствуясь Положением о Министерстве образования Пензенской области, утвержденным

постановлением Правительства Пензенской области от 05.08.2008 № 485-пП (с последующими изменениями), п р и к а з ы в а ю:

1. Утвердить и ввести в действие комплект организационно – распорядительной документации по организации обработки и защиты информации, обрабатываемой 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), в соответствии с приложениями к настоящему приказу:

1.1. Правила обработки персональных данных в РИС ГИА в Министерстве образования Пензенской области согласно приложению № 1 к настоящему приказу.

1.2. Правила рассмотрения запросов субъектов персональных данных или их представителей в Министерстве образования Пензенской области согласно приложению № 2 к настоящему приказу.

1.3. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве образования Пензенской области согласно приложению № 3 к настоящему приказу.

1.4. План внутреннего контроля обработки и защиты персональных данных в Министерстве образования Пензенской области согласно приложению № 4 к настоящему приказу.

1.5. План мероприятий по защите информации в РИС ГИА согласно приложению № 5 к настоящему приказу.

1.6. Инструкция о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Министерстве образования Пензенской области согласно приложению № 6 к настоящему приказу.

1.7. Инструкция пользователя РИС ГИА согласно приложению № 7 к настоящему приказу.

1.8. Положение о порядке организации и проведении работ по защите информации, обрабатываемой в РИС ГИА согласно приложению № 8 к настоящему приказу.

1.9. Инструкция по идентификации и аутентификации пользователей РИС ГИА согласно приложению № 9 к настоящему приказу.

1.10. Инструкция по управлению доступом к РИС ГИА согласно приложению № 10 к настоящему приказу.

1.11. Инструкция по защите машинных носителей информации в Министерстве образования Пензенской области согласно приложению № 11 к настоящему приказу.

1.12. Инструкция по управлению событиями информационной безопасности РИС ГИА согласно приложению № 12 к настоящему приказу.

1.13. Инструкция по антивирусной защите РИС ГИА согласно приложению № 13 к настоящему приказу.

1.14. Инструкция по контролю (анализу) защищенности информации РИС ГИА согласно приложению № 14 к настоящему приказу.

1.15. Инструкция по защите технических средств РИС ГИА согласно приложению № 15 к настоящему приказу.

1.16. Порядок по управлению изменениями в конфигурации РИС ГИА согласно приложению № 16 к настоящему приказу.

1.17. Порядок по выявлению инцидентов в РИС ГИА и реагированию на них согласно приложению № 17 к настоящему приказу.

1.18. Порядок доступа в помещения, в которых размещена РИС ГИА согласно приложению № 18 к настоящему приказу.

1.19. Инструкция по управлению программным обеспечением РИС ГИА согласно приложению № 19 к настоящему приказу.

1.20. Инструкция по обеспечению целостности РИС ГИА согласно приложению № 20 к настоящему приказу.

1.21. Положение по использованию средств криптографической защиты информации в Министерстве образования Пензенской области согласно приложению № 21 к настоящему приказу.

1.22. Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Министерстве образования Пензенской области согласно приложению № 22 к настоящему приказу.

1.23. Инструкция ответственного пользователя средств криптографической защиты информации в Министерстве образования Пензенской области согласно приложению № 23 к настоящему приказу.

1.24. Инструкция пользователя средств криптографической защиты информации в Министерстве образования Пензенской области согласно приложению № 24 к настоящему приказу.

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

3. Контроль за исполнением настоящего приказа возложить на первого заместителя Министра образования Пензенской области Денисова М.В.

Министр А.Н. Фомин

Приложение №1
Утверждёно
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-07

Правила
обработки персональных данных 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» в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящие Правила обработки персональных данных в РИС ГИА (далее – Правила) в Министерстве образования Пензенской области разработаны в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в Министерстве образования Пензенской области;

- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов Министерства образования Пензенской области по вопросам обработки и защиты персональных данных;

- определения целей обработки персональных данных в РИС ГИА в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;

- установления ответственности сотрудников Министерства образования Пензенской области, имеющих доступ к персональным данным субъектов персональных данных в РИС ГИА, за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящими Правилами и иными локальными актами Министерства образования Пензенской области.

1.2. В настоящих Правилах используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящих Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты ПДн.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ПДн	Персональные данные
Роскомнадзор	Уполномоченный орган по защите прав субъектов персональных данных
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от

Термин	Определение	Источник
персональных данных		27.06.2006 № 152-ФЗ «О персональных данных»
Безопасность информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию	ГОСТ Р 50922-2006
Доступность информации	Свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать	Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Обработка персональных данных без использования	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении	Постановление Правительства Российской Федерации от

Термин	Определение	Источник
средств автоматизации	каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Целостность информации	Свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право	Методический документ «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Настоящие Правила разработаны на основании следующих нормативных правовых актов:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»,

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

1.4. Настоящие Правила устанавливают и определяют в Министерстве образования Пензенской области:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки и защиты ПДн;

- цели обработки ПДн;

- содержание обрабатываемых ПДн;

- сроки обработки и хранения обрабатываемых ПДн;

- порядок уничтожения обработанных ПДн при достижении целей обработки или при наступлении иных законных оснований.

1.5. Правила являются обязательными для исполнения всеми пользователями РИС ГИА, имеющими доступ к ПДн.

Пользователи РИС ГИА должны быть ознакомлены с настоящими Правилами до начала работы в РИС ГИА под подпись.

Обязанность по организации ознакомления пользователей с настоящими Правилами возлагается на ответственного за организацию обработки ПДн.

1.6. Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

2. Требования к обработке и защите ПДн

2.1 Министерство образования Пензенской области при обработке ПДн руководствуется принципами и условиями, определенными нормами главы 2 Федерального закона № 152-ФЗ.

2.2. Права субъектов ПДн определены в главе 3 Федерального закона № 152-ФЗ.

2.3. При определении обязанностей Министерство образования Пензенской области при сборе ПДн и при обращении субъектов ПДн в Министерство образования Пензенской области руководствуется главой 4 Федерального закона № 152-ФЗ.

2.4. В Министерстве образования Пензенской области принимаются меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, в том числе:

- назначается приказом Министерства образования Пензенской области ответственный за организацию обработки ПДн в Министерстве образования Пензенской области и утверждается министром образования Пензенской области Инструкция ответственного за организацию обработки в Министерстве образования Пензенской области, в которой определены его права и обязанности;

- составляется перечень ПДн, обрабатываемых в РИС ГИА, который утверждается приказом Министерства образования Пензенской области;

- издаются документы, определяющие политику Министерства образования Пензенской области в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, определяющих для каждой цели обработки ПДн объем, категории и перечень обрабатываемых ПДн, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;

- обеспечивается размещение на официальном сайте Министерства образования Пензенской области Политики в отношении обработки персональных данных в Министерстве образования Пензенской области;

- применяются правовые, организационные и технические меры по обеспечению безопасности ПДн в соответствии со статьей 19 Федерального закона № 152-ФЗ «О персональных данных»;

- осуществляется внутренний контроль соответствия обработки ПДн Федеральному закону № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам, локальным актам Министерства образования Пензенской области согласно Правилам внутреннего контроля обработки персональных данных на соответствие требованиям к их защите, утвержденным в Министерстве образования Пензенской области;

- обеспечивается ознакомление пользователей РИС ГИА, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации, локальными актами оператора в сфере обработки ПДн, в том числе требованиями к защите ПДн и настоящими Правилами;

- запрещается обработка ПДн в РИС ГИА, а равно и обработка ПДн без использования средств автоматизации (при наличии смешанной обработки ПДн), лицами, не допущенными к обработке ПДн согласно приказам Министерстве образования Пензенской области «О предоставлении пользователям доступа к информационным ресурсам РИС ГИА.

2.5. Обработка ПДн осуществляется после получения согласия субъекта ПДн (за исключением случаев, предусмотренных частью 1 статьи 6 Федерального закона № 152-ФЗ «О персональных данных»), при условии выполнения требований к защите ПДн. Согласие на обработку субъект ПДн предоставляет письменно по форме **Приложения № 1** и **Приложения № 2** к настоящим Правилам.

2.6. Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, предоставляется письменно по форме **Приложения № 4** к настоящим Правилам. При необходимости оператор обязан обеспечить субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешенных субъектом ПДн для распространения.

2.7. При необходимости привлечения к обработке ПДн третьих лиц оператор ПДн может передать для обработки персональные данные субъекта ПДн третьему лицу только с согласия субъекта ПДн. В этом случае согласие на передачу субъект ПДн предоставляет письменно по форме **Приложения № 1.1**.

В случае, когда в ИСПДн обрабатываются ПДн несовершеннолетних и в соответствии с законодательством Российской Федерации требуется согласие от законного представителя оформляется согласие законного представителя на обработку ПДн несовершеннолетнего по форме **Приложения № 1.2.**

2.8. Безопасность ПДн, при их обработке в РИС ГИА обеспечивает Министерство образования Пензенской области.

2.9. При обработке ПДн соблюдаются следующие требования:

- к работе с ПДн допускаются только пользователи на основании соответствующего приказа Министерства образования Пензенской области, и подписавшие обязательство о неразглашении персональных данных по форме **Приложения № 3** к настоящему приказу;

- в целях обеспечения сохранности документов, содержащих ПДн, все операции по оформлению, формированию, ведению и хранению данной информации выполняются пользователями – сотрудниками Министерства образования Пензенской области, осуществляющими данную деятельность в связи с исполнением трудовых (служебных) обязанностей;

- на период обработки ПДн в помещении могут находиться только лица, допущенные в установленном порядке к обработке ПДн.

2.10. Особенности обработки ПДн:

1) машинные носители ПДн подлежат обязательной регистрации и учету;

2) обработка ПДн осуществляется при условии выполнения требований к защите ПДн, утвержденных:

- постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»;

- приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- локальными актами Министерства образования Пензенской области, устанавливающими принятие организационных и технических мер для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

2.11. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, проинформированы в соответствии с формой согласно **Приложению № 5** к настоящим Правилам о факте обработки ими персональных данных, обработка которых осуществляется в Министерстве образования Пензенской области без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами Российской Федерации, а также локальными правовыми актами Министерства образования Пензенской области.

3. Цели обработки ПДн

3.1 Министерство образования Пензенской области обрабатывает ПДн, содержащиеся в РИС ГИА.

Целью обработки ПДн в РИС ГИА является проведение государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования.

4. Содержание обрабатываемых ПДн

4.1. Содержание обрабатываемых ПДн определяется перечнем ПДн, утверждаемым приказом Министерства образования Пензенской области «Об утверждении перечня персональных данных, обрабатываемых в РИС ГИА.

5. Категории ПДн

5.1. В РИС ГИА обрабатываются иные категории ПДн.

6. Сроки обработки и хранения обрабатываемых ПДн

6.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн.

6.2. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.3. Основания для прекращения обработки ПДн и сроки их уничтожения определены в частях 3, 4, 5 статьи 21 Федерального закона № 152-ФЗ.

6.4. Основанием (условием) прекращения обработки ПДн также является ликвидация (реорганизация) Министерства образования Пензенской области.

6.5. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в частях 3, 4, 5 статьи 21 Федерального закона № 152-ФЗ, Министерство образования Пензенской области осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства образования Пензенской области). Обеспечивает уничтожение ПДн в срок **не более чем 6 месяцев**, если иной срок не установлен федеральными законами.

7. Порядок уничтожения ПДн

7.1. Уничтожение персональных данных осуществляется в соответствии с Положением о комиссии по уничтожению персональных данных, утверждаемым приказом Министерства образования Пензенской области.

7.2. Порядок уничтожения машинного носителя информации (в том числе персональных данных) определяется Инструкцией по защите машинных носителей информации в Министерстве образования Пензенской области, утверждаемой приказом Министерства образования Пензенской области.

8. Ответственность за нарушения при обработке ПДн

8.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, установленных настоящими Правилами, в соответствии с действующим законодательством Российской Федерации.

9. Заключительные положения

9.1. Лица, определенные приказом Министерства образования Пензенской области, как пользователи РИС ГИА, участвующие в обработке и защите ПДн, должны быть ознакомлены с настоящими Правилами.

9.2. Обязанность по организации работы по ознакомлению под подпись сотрудников Министерства образования Пензенской области с положениями нормативных правовых актов Российской Федерации в сфере обработки и защиты ПДн, локальных актов Министерства образования Пензенской области по вопросам обработки ПДн, требованиями к защите ПДн, возлагается на ответственного за организацию обработки ПДн в Министерстве образования Пензенской области.

Приложение №1
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Согласие субъекта персональных данных на обработку персональных данных

Я, _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

зарегистрированный (ая) по адресу: _____

_____

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие Министерству образования Пензенской области, зарегистрированному по адресу: 440034, г. Пенза, ул. Маркина, стр. 2, (далее – Оператор) на обработку своих персональных данных.

1. Цель обработки персональных данных:

_____

_____

2. Перечень персональных данных, передаваемых на обработку:

_____

_____

_____

3. Перечень действий с персональными данными, осуществляемых Оператором:

_____
(указывается общее описание используемых Оператором способов обработки персональных данных)

4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных
5. Мне разъяснены мои права и обязанности, в части обработки персональных данных, в том числе, моя обязанность проинформировать оператора в случае изменения персональных данных.

«____» _____ 20___ г. _____
(подпись)

Приложение №1.1
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области
(Согласие на передачу 3-м лицам)*

Согласие на передачу персональных данных*

Я, _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

зарегистрированный (ая) по адресу: _____

_____

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие Министерству образования Пензенской области (далее – Оператор), зарегистрированному по адресу: 440034, г. Пенза, ул. Маркина, стр. 2, на передачу своих персональных данных в

_____
(указывается наименование организации третьего лица, реквизиты организации третьего лица)

1. Цель передачи персональных данных:

_____

2. Перечень передаваемых персональных данных:

_____
(указывается перечень передаваемых персональных данных)

_____

3. Перечень действий с персональными данными, осуществляемых Оператором _____

_____
(указывается общее описание используемых Оператором способов обработки персональных данных):

4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных [указываются конкретный срок либо условия, определяемые действующим законодательством Российской Федерации].
5. Ответственность за обеспечение сохранности и конфиденциальности передаваемых персональных данных и за нарушения _____
(наименование организации третьего лица)
при обработке переданных персональных данных несет Оператор.

«____» _____ 20___ г. _____
(подпись)

*(Используется при необходимости)

Приложение №1.2
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Согласие законного представителя на обработку персональных данных несовершеннолетнего

Я, _____
(фамилия, имя, отчество)
документ, удостоверяющий личность _____ серия _____
(вид документа)
№ _____, выдан _____

_____
(кем и когда)
зарегистрированный (ая) по адресу:

_____

_____
являюсь законным представителем субъекта персональных данных: _____ (ФИО), проживающего по адресу

_____

_____,
Свидетельство о рождении серия _____ № _____ выдано (кем и когда): _____
на основании статьи 64 Семейного кодекса Российской Федерации (или указывается иное правовое основание) в соответствии со в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных) даю свое согласие Министерству образования Пензенской области, зарегистрированному по адресу: 440034, г. Пенза, ул. Маркина, стр. 2 (далее - Оператор) на обработку персональных данных несовершеннолетнего

1. Цель обработки персональных данных:

_____

2. Перечень персональных данных, на обработку которых дается согласие:

_____
(указывается перечень персональных данных)

3. Перечень действий с персональными данными, на совершение которых дается согласие:

_____
(указывается общее описание используемых Оператором способов обработки персональных данных)

4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с законодательством Российской Федерации сроков хранения персональных данных.
5. Согласие может быть досрочно отозвано путем подачи письменного заявления в адрес Оператора.
6. Я предупрежден(а), что в случае отзыва согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6 и ч. 2 ст. 10 Федерального закона «О персональных данных».

«____» _____ 20___ г. _____
(подпись)

Приложение №2
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Разъяснение
субъекту персональных данных юридических последствий отказа предоставить персональные данные

Мне, _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

зарегистрированный (ая) по адресу: _____

_____

в соответствии с частью 2 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» разъяснены юридические последствия отказа предоставить мои персональные данные Министерству образования Пензенской области, зарегистрированному по адресу: 440034, г. Пенза, ул. Маркина, стр. 2, в целях:

_____

_____
(цели обработки персональных данных)

В случае отказа субъекта предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим юридическим последствиям:

_____

_____

_____
(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

«____» _____ 20___ г. _____
(подпись)

Приложение №3
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Обязательство
о неразглашении персональных данных

Я, _____

паспорт серии _____ номер _____, выданный «_____» _____ _____ года в период трудовых (служебных) отношений с Министерством образования Пензенской области и в течение _____ лет после их прекращения в соответствии с Политикой в отношении обработки персональных данных и требованиями к защите информации в Министерстве образования Пензенской области обязуюсь:

1. не разглашать и не передавать третьим лицам сведения, содержащие персональные данные, которые мне будут доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения ответственного за организацию обработки персональных данных в организации;
2. выполнять требования приказов, положений и инструкций по обработке персональных данных в части меня касающейся;
3. в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, а также в случае утери носителей информации, содержащих такие сведения, немедленно сообщить об этом лицу, ответственному за организацию обработки персональных данных;
4. не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в Министерстве образования Пензенской области.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных при автоматизированной обработке информации и осуществляемой без средств автоматизации.

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную действующим законодательством Российской Федерации.

«_____» _____ 20___ г. _____
(подпись)

Приложение №4
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Согласие
на обработку персональных данных,
разрешенных субъектом персональных данных
для распространения

Настоящим я, _____,
(фамилия, имя, отчество)

_____
контактная информация (номер телефона, адрес электронной почты или почтовый адрес)

руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю свое согласие Министерству образования Пензенской области, зарегистрированному по адресу: 440034, г. Пенза, ул. Маркина, стр. 2, ИНН: 5836011445, ОГРН: 1025801354149 (далее - Оператор) на обработку моих персональных данных на следующих информационных ресурсах оператора[1] :

_____
(указываются сведения об информационных ресурсах оператора)

с целью _____
(указываются цель обработки персональных данных))

в следующем порядке:

Категория персональных данных	Перечень персональных данных	Разрешение к распространению (да/нет)[2]	Установленные условия и запреты[3] по обработке персональных данных	Условия по передаче персональных данных с использованием сетей передачи данных либо без передачи[4]
1	2	3	4	5
Иные	фамилия, имя, отчество (при наличии)			
	год, месяц, дата рождения			
	место рождения			

[1] Указывается адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных
[2] Субъектом персональных данных собственноручно осуществляется отметка в графе 3 о наличии либо отсутствии разрешения к распространению персональных данных.
[3] Графа 4 заполняется по желанию субъекта персональных данных, где указываются категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов.
4 Графа 5 заполняется по желанию субъекта персональных данных, в которой указываются условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных

	адрес			
	семейное положение			
	образование			
	профессия			
	социальное положение			

Настоящее согласие дано мной добровольно на срок _____ (определенный период времени или дата окончания срока действия).

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования оператор обязан немедленно прекратить распространять мои персональные данные.

«___» _____ 20___г. _____ _____
(подпись) (фамилия, имя, отчество)

Приложение №5
к Правилам обработки персональных данных
в РИС ГИА в Министерстве образования Пензенской области

Информирование о факте обработки персональных данных без использования средств автоматизации

Я, _____,
(фамилия, имя, отчество)
паспорт серии _____ № _____
выдан _____
_____

дата выдачи «____»_____ ____г.

работающий(ая) в должности
_____
_____
_____
(должность, наименование структурного подразделения)

проинформирован(а):
– о факте обработки мною персональных данных, обработка которых осуществляется Министерством образования Пензенской области без использования средств автоматизации*;
– о категориях обрабатываемых персональных данных;
– о правилах осуществления такой обработки, установленных нормативными правовыми актами Российской Федерации, а также локальными правовыми актами Министерства образования Пензенской области.

* обработка персональных данных, содержащихся 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» либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Я предупрежден(а) о том, что в случае нарушения, установленного законодательством Российской Федерации порядка сбора, хранения, использования или распространения персональных данных я несу ответственность в соответствии с законодательством Российской Федерации.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение №2
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-0

Правила

рассмотрения запросов субъектов персональных данных или их представителей в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) в Министерстве образования Пензенской области определяют порядок рассмотрения запросов субъектов персональных или их представителей в указанном региональном органе исполнительной власти.

1.2. В настоящих Правилах используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящем Правилах, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
Роскомнадзор	Уполномоченный орган по защите прав субъектов персональных данных
Федеральный закон № 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95

1.3. Перечень нормативных правовых актов, на основании которых разработаны Правила:

- Гражданский кодекс Российской Федерации;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,
- Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

1.4. Сотрудники Министерства образования Пензенской области, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящими Правилами до начала обработки под подпись. Обязанность по организации ознакомления сотрудников с настоящими Правилами возлагается на ответственного за организацию обработки ПДн.

2. Правила рассмотрения запросов субъектов персональных данных

2.1. Организация приема и обработки обращений и запросов субъектов ПДн или их представителей, а также контроль за их приемом и обработкой возлагается на ответственного за организацию обработки ПДн.

2.2. Субъект ПДн имеет право на получение информации в Министерстве образования Пензенской области касающейся обработки его ПДн (часть 7 статьи 14 Федерального закона № 152-ФЗ), в том числе содержащей:

- подтверждение факта обработки ПДн Министерством образования Пензенской области;
- правовые основания и цели обработки ПДн;
- цели и применяемые способы обработки ПДн в Министерстве образования Пензенской области;
- наименование и место нахождения Министерства образования Пензенской области, сведения о лицах (за исключением сотрудников Министерства образования Пензенской области), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Министерства образования Пензенской области, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами Российской Федерации.

2.3. Сведения, указанные в пункте 2.2., должны предоставляться субъекту ПДн или его представителю Министерством образования Пензенской области при обращении либо при получении запроса субъекта ПДн или его представителя.

2.4. Запрос субъекта ПДн должен содержать:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта ПДн в отношениях с Министерством образования Пензенской области (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

- подпись субъекта ПДн или его представителя.

2.5. В Министерстве образования Пензенской области разработаны и используются соответствующие бланки с формами обращений субъектов ПДн (Приложения №1, №2, №3 и №4).

2.6. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

2.7. Сведения, указанные в пункте 2.2., предоставляются субъекту ПДн Министерством образования Пензенской области в доступной форме, и в них не содержатся ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

2.8. Субъект ПДн вправе требовать от Министерства образования Пензенской области уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2.9. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона № 152-ФЗ.

2.10. Запросы, поступающие в Министерство образования Пензенской области, обрабатываются в соответствии с требованиями Федерального закона № 152-ФЗ и рассматриваются в соответствии с требованиями Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» и локальными актами Министерства образования Пензенской области.

2.11. Все поступившие в Министерство образования Пензенской области запросы регистрируются в день их поступления в Журнале учета обращений субъектов персональных данных или представителей субъектов ПДн (Приложение №5). На запросе указывается входящий номер и дата регистрации.

2.12. Обязанность ведения Журнала учета обращений субъектов персональных данных или представителей субъектов персональных данных в Министерства образования Пензенской области возлагается на сотрудника соответствующим приказом оператора.

2.13. Рассмотрение запросов и подготовка ответов осуществляется по поручению министра образования Пензенской области.

2.14. Сотрудник Министерства образования Пензенской области, осуществляющий обработку ПДн, в соответствии с должностной инструкцией, подготавливает проект ответа субъекту ПДн и визирует его у ответственного за организацию обработки ПДн в Министерстве образования Пензенской области.

2.15. Ответ субъекту ПДн направляется за подписью министра образования Пензенской области.

2.16. Ответы субъекту ПДн направляются в виде уведомлений. В Министерства образования Пензенской области разработаны и используются соответствующие формы бланков уведомлений (Приложения №6, №7, №8, №9, №10, №11).

2.17 После отправки ответа на запрос осуществляется отметка в Журнале учета обращений субъектов персональных данных или представителей субъектов ПДн с указанием даты отправки.

2.18. Хранение запросов субъектов ПДн или их представителей и подготовленных ответов осуществляется не менее трех лет. Условия хранения указанных запросов и ответов должны препятствовать несанкционированному доступу до момента их уничтожения.

3. Ответственность

3.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в соответствии с законодательством Российской Федерации.

Приложение № 1
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Оператору персональных данных -
Министерство образования Пензенской области Адрес:
440034, г. Пенза, ул. Маркина, стр. 2

Запрос

на предоставление информации об обработке персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

Адрес: _____

Сведения, подтверждающие факт обработки персональных данных в Министерстве образования Пензенской области:

_____

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» прошу предоставить мне следующую информацию, касающуюся обработки моих персональных данных:

- ☐ подтвердить факт обработки моих персональных данных;
- ☐ правовые основания и цели обработки моих персональных данных;
- ☐ цели и применяемые способы обработки персональных данных;
- ☐ наименование и местонахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к моим персональным данным или которым могут быть раскрыты мои персональные данные на основании договора или на основании федерального закона;
- ☐ относящиеся ко мне обрабатываемые персональные данные, источник их получения;
- ☐ сроки обработки моих персональных данных, в том числе сроки их хранения;
- ☐ порядок осуществления мной прав, предусмотренных Федеральным законом «О персональных данных»;
- ☐ информацию об осуществленной или предполагаемой трансграничной передаче моих персональных данных;
- ☐ наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку моих персональных данных если обработка поручена или будет поручена такому лицу
- ☐ _____.
(иные сведения)

Данный запрос является первичным / повторным, на основании того, что:

_____
(ОБЯЗАТЕЛЬНО: указать причину направления повторного запроса)

Указанные сведения прошу предоставить по адресу: _____

_____ _____
(дата) (подпись)

Приложение № 2
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Оператору персональных данных -
Министерство образования Пензенской области Адрес:
440034, г. Пенза, ул. Маркина, стр. 2

Заявление

об отзыве согласия на обработку персональных данных

От, _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

Адрес: _____

_____

Сведения, подтверждающие факт обработки персональных данных в Министерстве образования Пензенской области:

_____

Прошу прекратить обработку моих персональных данных, осуществляемую в целях:

_____
(цели обработки персональных данных, в отношении которых отзывается согласие)

по причине:

_____

_____ _____
(дата) (подпись)

Приложение № 3
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования пензенской области

Оператору персональных данных -
Министерство образования Пензенской области Адрес:
440034, г. Пенза, ул. Маркина, стр. 2

Запрос
на уточнение персональных данных

От, _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

Адрес: _____

_____

Сведения, подтверждающие факт обработки персональных данных в Министерстве образования Пензенской области:

_____

в соответствии с положениями статьями 14, 21 Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных» прошу уточнить/ уничтожить мои персональные данные в связи с тем, что:

_____
(указать причину: персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются

_____
необходимыми для заявленной цели обработки; с персональными данными, совершаются неправомерные действия – указать какие)

_____ _____
(дата) (подпись)

Приложение № 4
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Возражение
против принятия решений на основании исключительно
автоматизированной обработки персональных данных

От _____
(фамилия, имя, отчество)

документ, удостоверяющий личность _____ серия _____
(вид документа)

№ _____, выдан _____

_____
(кем и когда)

Адрес: _____

_____

Сведения, подтверждающие факт обработки персональных данных в Министерстве образования Пензенской области:

_____

Прошу исключить принятие в отношении меня юридически значимых решений на основании исключительно автоматизированной обработки моих персональных данных.

_____ _____
(дата) (подпись)

Приложение № 5
к Правилам рассмотрения запросов
субъектов персональных данных в Министерстве образования Пензенской области

Журнал

обращений субъектов персональных данных или представителей субъектов персональных данных в Министерство образования Пензенской области

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№	Сведения о запрашивающем лице (Ф.И.О., адрес)	Сведения о запросе			Сведения о принятом решении		Подпись ответственного лица	Примечание
		Дата поступления запроса	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации		
1	2	3	4	5	6	7	8	9
1	*Иванов И.И., РФ г. Иванов, ул Иванова, д. 1, кв. 1*	*01.11.2021*	*перечень измененных персональных данных*	*уточнение персональных данных*	*отправлено почтовое уведомление №233 об уточнении ПДн*	*10.11.2021*	*[Ф.И.О. Фамилия ответственного за организацию обработки ПДн]*	*Пример заполнения*

Лист _____

Правила

по формированию и ведению

журнала обращений субъектов персональных данных или представителей субъектов персональных данных в Министерство образования Пензенской области

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – Ф.И.О. и адрес субъекта ПДн, обратившегося в организацию по вопросу обработки его персональных данных;
- Графа 3 – дата поступления запроса;
- Графа 4 – кратко содержание обращения;
- Графа 5 – кратко о цели обращения субъекта ПДн;
- Графа 6 – запись о действии в ответ на обращение;
- Графа 7 – дата отправки уведомления субъекту ПДн;
- Графа 8 – подпись сотрудника, отправившего уведомление субъекту ПДн.
- Графа 9 – любая информация, относящаяся к обращению субъекта ПДн.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 6
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Уведомление

Оператор персональных данных – Министерство образования Пензенской области Адрес: 440034, г. Пенза, ул. Маркина, стр. 2, не осуществляет обработку Ваших персональных данных, начиная с:

_____
(Дата, с которой прекращена обработка ПДН)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 7
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Отказ
в предоставлении сведений

Оператор персональных данных – Министерство образования Пензенской области Адрес: 440034, г. Пенза, ул. Маркина, стр. 2.

Вам отказано в предоставлении сведений по запросу от:

_____
(дата запроса)

на основании _____
(ссылка на нормы ФЗ РФ «О персональных данных» или иных федеральных законов)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 8
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Уведомление

Оператор персональных данных - Министерство образования Пензенской области Адрес: 440034, г. Пенза, ул. Маркина, стр. 2 по Вашему запросу от

_____
(дата запроса)

уведомляет Вас о невозможности отзыва согласия на обработку персональных данных в следующих целях:

_____

Дата начала обработки персональных данных:

_____

Срок или условие прекращения обработки персональных данных:

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 9
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Уведомление

Оператор персональных данных – Министерство образования Пензенской области Адрес: 440034, г. Пенза, ул. Маркина, стр. 2.

По Вашему запросу от: _____,
(дата запроса)

было произведено уточнение Ваших персональных данных.

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 10
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Ответ

на возражение против принятия решений на основании исключительно автоматизированной обработки персональных данных

Оператор персональных данных: Министерство образования Пензенской области Адрес: 440034, г. Пенза, ул. Маркина, стр. 2,

рассмотрел Ваши возражения от: _____
(дата запроса)

И принял следующее решение:

_____

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 11
к Правилам рассмотрения запросов
субъектов персональных данных
в Министерстве образования Пензенской области

Субъекту персональных данных:

_____

_____

_____
(Ф.И.О.)

Адрес: _____

_____

Уведомление
о блокировании персональных данных

Оператор персональных данных – Министерство образования Пензенской области, находящийся по адресу: 440034, г. Пенза, ул. Маркина, стр. 2, осуществил блокирование Ваших персональных данных, включая:

_____
(перечисление блокированных персональных данных: Ф.И.О., адрес, телефон)

которые обрабатывались в целях:

_____
(цель обработки указанных персональных данных)

Указанные персональные данные были заблокированы _____
(дата блокирования)

в связи с: _____
(причина блокирования персональных данных)

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

« » _____ 20 г.

Приложение № 3
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-04

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяют в Министерстве образования Пензенской области (основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Министерства образования Пензенской области в отношении обработки персональных данных, локальным актам Министерства образования Пензенской области.

1.2. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.3. Перечень нормативных правовых актов, на основании которых разработаны Правила:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

- постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687);

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства РФ № 1119);

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее – приказ ФСТЭК России № 17);

- приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – приказ ФСТЭК России № 21).

- приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведении работ по аттестации объектов информатизации на соответствие требованиям о защите

информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России № 77).

1.4. Лица, допущенные к обработке персональных данных в Министерстве образования Пензенской области в связи с необходимостью выполнения ими трудовых (служебных) обязанностей, должны быть ознакомлены с настоящими Правилами под подпись до начала обработки персональных данных. Обязанность по организации ознакомления указанных сотрудников с настоящими Правилами возлагается на ответственного за организацию обработки персональных данных в Министерстве образования Пензенской области.

2. Основания проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Основаниями для проведения внутреннего контроля являются требования пункта 4 части 1 статьи 18.1., пункта 1 части 4, статьи 22.1. Федерального закона № 152-ФЗ, пункта 17 требований к защите персональных данных при их обработке в информационных системах персональных данных (далее - требования), утвержденных постановлением Правительства РФ № 1119, ежегодный план внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, утверждаемый министром образования Пензенской области.

2.2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) осуществляется в Министерстве образования Пензенской области путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов Министерства образования Пензенской области по обработке и защите персональных данных.

2.3. Организация разработки проекта ежегодного плана внутренних проверок обеспечивается ответственным за организацию обработки в Министерстве образования Пензенской области (ответственным за защиту информации в РИС ГИА).

2.4. Обеспечивается проведение периодического контроля уровня защиты информации, результаты которого оформляются протоколами и отражаются в Технических паспортах информационных систем. Протоколы контроля защиты информации в РИС ГИА не реже 1 раза в 2 года предоставляются в территориальный орган ФСТЭК России.

Непредставление протоколов контроля защиты информации в территориальный орган ФСТЭК России является основанием для приостановления действия аттестата соответствия РИС ГИА требованиям по защите информации.

3. Порядок осуществления внутреннего контроля

3.1. Внутренний контроль проводится самостоятельно Министерством образования Пензенской области и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Для проведения внутреннего контроля в Министерстве образования Пензенской области создается комиссия по осуществлению внутреннего контроля

соответствия обработки персональных данных требованиям к защите персональных данных (далее - Комиссия).

3.3. Состав Комиссии, состоящий, как правило, из не менее трех сотрудников Министерства образования Пензенской области, утверждается приказом Министерства образования Пензенской области.

3.4. Председателем Комиссии, как правило, назначается ответственный за организацию обработки персональных данных в Министерстве образования Пензенской области.

3.5. В состав Комиссии также входят администратор безопасности информационной системы (систем) персональных данных, администратор безопасности государственной информационной системы, содержащей персональные данные (далее – государственные информационные системы) и руководитель кадрового аппарата Министерства образования Пензенской области.

3.6. Все члены комиссии при принятии решения обладают равными правами.

3.7. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

3.8. Комиссия при проведении проверки обязана:

3.8.1. Провести анализ реализации мер, направленных на обеспечение выполнения Министерством образования Пензенской области, предусмотренных статьями 18.1, 19 Федерального закона № 152-ФЗ и принятыми в соответствии с ним локальными актами в отношении обработки персональных данных, и проверить:

- наличие актуального приказа о назначении лица, ответственного за организацию обработки персональных данных в Министерстве образования Пензенской области, утвержденной инструкции ответственного за организацию обработки персональных данных в Министерстве образования Пензенской области, а также внесение соответствующих дополнений в должностную инструкцию (регламент) сотрудника, назначенного ответственным за организацию обработки персональных данных в Министерстве образования Пензенской области.

- актуальность сведений, содержащихся в реестре операторов, осуществляющих обработку персональных данных, которые размещены на официальном сайте уполномоченного органа по защите прав субъектов персональных данных;

- актуальность Политики в отношении обработки персональных данных в Министерстве образования Пензенской области (далее - Политика) и обеспечение неограниченного доступа к Политике и сведениям о реализуемых требованиях к защите персональных данных, в том числе размещение их на официальном сайте Министерства образования Пензенской области в информационно-телекоммуникационной сети;

- наличие и актуальность Перечня персональных данных по каждой категории персональных данных, обрабатываемых в Министерства образования Пензенской области, и Перечня информационных систем персональных данных Министерства образования Пензенской области;

- наличие правовых оснований для обработки персональных данных по каждой категории субъектов персональных данных, независимо от способа обработки персональных данных;

- соответствие целей обработки персональных данных содержанию и объему обрабатываемых персональных данных, независимо от способа их обработки;

- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения Министерством образования Пензенской области обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

- ознакомление сотрудников (документально подтвержденное), непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Министерства образования Пензенской области в отношении обработки персональных данных, локальными актами по вопросам обработки и обеспечения безопасности персональных данных;

- соответствие установленных прав доступа к персональным данным в информационной системе (системах) персональных данных трудовым (служебным) обязанностям сотрудников Министерства образования Пензенской области;

- наличие и полноту заполнения сотрудниками Министерства образования Пензенской области обязательств о соблюдении конфиденциальности персональных данных, документа об информировании о факте обработки персональных данных без использования средств автоматизации, разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

- наличие согласий субъектов персональных данных на обработку персональных данных и разъяснений субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в случаях, когда этого требует законодательство Российской Федерации;

- наличие и ведение Журнала обращений субъектов персональных данных и представителей субъектов персональных данных, соблюдения процедур и сроков подготовки ответов на обращения субъектов персональных данных, а также учета предоставления персональных данных субъектов персональных данных по письменным запросам третьих лиц в порядке, установленном действующим законодательством Российской Федерации;

- наличие (в случае заключения соответствующего договора) в поручении на обработку персональных данных: перечня действия (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона № 152-ФЗ;

- актуальность Перечня мест хранения материальных носителей персональных данных и обеспечение контроля хранения материальных носителей персональных данных в условиях, исключающих несанкционированный доступ к ним, а также обеспечение раздельного хранения персональных данных в случаях их обработки без использования средств автоматизации при несовместимости целей обработки персональных данных;

- соблюдение сроков хранения и порядка уничтожения материальных носителей персональных данных, а также персональных данных на носителях информации;

- актуальность организационно-распорядительных документов по вопросам обработки персональных данных.

3.8.2. Проанализировать выполнение в Министерстве образования Пензенской области требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства РФ № 1119, и проверить:

- соответствие указанных в утвержденном в Министерства образования Пензенской области Перечне обрабатываемых персональных данных в информационной системе персональных данных категорий персональных данных, категорий субъектов персональных данных и количества субъектов персональных данных фактически обрабатываемым в информационной системе персональных данных, государственной информационной системе Пензенской области;

- соответствие фактического типа актуальных угроз безопасности персональных данных в информационной системе персональных данных с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, типу актуальных угроз безопасности персональных данных, указанному в утвержденном министром образования Пензенской области Акте классификации информационной системы персональных данных (в случае, если проводились работы по аттестации информационной системы персональных данных) либо в акте определения уровня защищенности персональных данных в информационной системе персональных данных (в случае, если работы по аттестации информационной системы персональных данных не проводились);

- назначение сотрудника, ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных (за управление (администрирование) системой защиты информации государственной информационной системы);

- соответствие Перечня помещений, в которых размещена информационная система персональных данных, утвержденного в Министерстве образования Пензенской области фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации;

- соответствие перечня лиц, имеющих доступ к персональным данным в связи с исполнением своих трудовых (служебных) обязанностей перечню лиц, имеющих доступ в помещения, в которых размещена информационная система персональных

данных, утвержденного в Министерстве образования Пензенской области, фактически находящимся в указанных помещениях на момент проверки;

- фактическое выполнение организационных и технических мер по обеспечению безопасности помещений, в которых размещена информационная система персональных данных, препятствующих возможности неконтролируемого проникновения или пребывания в указанных помещениях лиц, не имеющих права доступа в них (при наличии - фактическое опечатывание входных дверей указанных помещений, применение систем контроля и управления доступом, средств охранной сигнализации, систем видеонаблюдения, оборудование оконных проемов первых и последних этажей здания, где размещено оборудование информационной системы персональных данных, запирающимися ставнями и т.д.);

- наличие сертификатов соответствия требованиям безопасности информации на все используемые средства защиты информации в Министерстве образования Пензенской области;

- обеспечение сохранности машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные в информационной системе персональных данных, государственной информационной системе Пензенской области путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей информации.

3.8.3. Проанализировать состояние работы в Министерстве образования Пензенской области по реализации Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России № 21, а также Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭ №17, и проверить:

- фактическую реализацию установленного в Министерстве образования Пензенской области порядка идентификации и аутентификации пользователей информационной системы персональных данных, государственной информационной системы;

- реализацию процесса управления доступом к ресурсам информационной системы персональных данных;

- регистрацию событий информационной безопасности в информационной системе персональных данных, государственной информационной системе Пензенской области в соответствии с Инструкцией по управлению событиями информационной безопасности;

- реализацию выявления инцидентов информационной безопасности и реагирования на них;

- организацию антивирусной защиты в информационной системе персональных данных и регулярность обновления базы данных признаков вредоносных программ (вирусов);

- реализацию выявления, анализа и устранения уязвимостей в информационной системе персональных данных, государственной информационной системе Пензенской области;

- установку обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации;

- наличие проверок настройки правильности функционирования программного обеспечения и средств защиты информации в информационной системе персональных данных, государственной информационной системе Пензенской области;

- организацию физического доступа к техническим средствам, средствам защиты информации информационной системы персональных данных, государственной информационной системы (в том числе опечатывание корпуса средств вычислительной техники);

- организацию размещения технических средств отображения информации информационных систем персональных данных, исключая ее несанкционированный просмотр;

- состав технических средств, программного обеспечения и средств защиты информации, входящих в состав информационной системы на соответствие Техническому паспорту информационной системы, государственной информационной системы;

- реализацию процесса управления конфигурацией информационной системы персональных данных, государственной информационной системы и их системы защиты информации.

4. Права комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

4.1. Комиссия при проведении проверки вправе:

- запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

- получать в соответствии с Инструкцией пользователей информационной системы персональных данных временный доступ к ресурсам информационной системы персональных данных, в части касающейся ее полномочий;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;

- вносить министру образования Пензенской области предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных нормативными правовыми актами Российской Федерации.

4.2. При проведении проверки члены Комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;

- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

4.3. По результатам проверки составляется Акт проверки, который подписывается всем составом комиссии и представляется министру образования Пензенской области для принятия соответствующего решения. В Министерстве образования Пензенской области разработана и используется специальная форма соответствующего Акта (**Приложение**).

4.4. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты информации (в том числе персональных данных), об их характере и о лицах, допустивших указанные нарушения.

4.5. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и Политике Министерства образования Пензенской области в отношении обработки персональных данных, установленным Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. Заключение о соответствии должно быть сформулировано для информационной системы персональных данных.

5. Ответственность

5.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами в соответствии с законодательством Российской Федерации.

Приложение
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных
в Министерстве образования Пензенской области

Акт № _____

проведения внутренней проверки условий

обработки персональных данных в Министерстве образования Пензенской области

Дата составления: «____» _____ 20____ г.

Место проведение проверки: _____

Комиссия, назначенная приказом Министерства образования Пензенской области от «___» _____ 20___ № ____ в составе:

Председатель:

_____(Ф.И.О.)

Члены комиссии:

_____(Ф.И.О.)

_____(Ф.И.О.)

руководствуясь Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, Политике в Министерстве образования Пензенской области в отношении обработки персональных данных провела проверку условий обработки персональных данных в Министерстве образования Пензенской области.

В ходе проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными актами Министерства образования Пензенской области, определяющих его политику в отношении обработки персональных данных;
- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- проведен анализ реализации Министерством образования Пензенской области организационных и технических мер по обеспечению безопасности персональных данных по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- проведен анализ реализации в Министерстве образования Пензенской области организационных и технических мер по обеспечению уровня защищенности информации в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- проведен анализ состава оборудования, программных средств, включая средства защиты. входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения: _____

_____

_____

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует (не соответствует)[1] требованиям к защите персональных данных и политике организации в отношении обработки персональных данных, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Председатель комиссии _____ (подпись)

Члены комиссии: _____ (подпись)

_____ (подпись)

[1] Нужное подчеркнуть

Приложение № 4
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-07

План внутреннего контроля обработки и защиты персональных данных в Министерстве образования Пензенской области на 202_ год

№ п/п	Содержание планируемого мероприятия	Периодичность	Дата проведения мероприятия	Ответственный
1.	Осуществление аудита (в том числе проведение инвентаризации информационных ресурсов с целью выявления в них ПДн) по установлению соответствия обработки персональных данных (далее- ПДн) Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) и принятым в соответствии с ним нормативным правовым актам (наличие правовых оснований для обработки ПДн по каждой категории ПДн, независимо от способа обработки ПДн, а также соответствие целей обработки ПДн содержанию и объему обрабатываемых ПДн). (п.4. ч.1 ст.18.1. Федерального закона)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС
2.	Проверка ознакомления лиц, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, локальными актами по вопросам обработки и обеспечения безопасности ПДн. (п.6. ч.1 ст.18.1. Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн;

3.	Осуществление проверки получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство Российской Федерации. (ст.9 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн
4.	Проверка подписания лицами, осуществляющими обработку ПДн, форм документов, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн, в том числе:			
4.1.	- документа об информировании о факте обработки ПДн без использования средств автоматизации; (п. 6 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687);	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, где осуществлятся обработка ПДн с использованием бумажных носителей информации
4.2.	- обязательства о соблюдении конфиденциальности ПДн; (ст.7 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС; - руководитель подразделения кадрового аппарата

4.3.	- листов ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами Министерства образования Пензенской области по вопросам обработки ПДн; (п.2 ч.4 ст.22.1 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководитель подразделения кадрового аппарата
4.4.	- разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн. (ч.2 ст.18 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководитель подразделения кадрового аппарата
5.	Проверка в поручении (в случае заключения соответствующего договора) на обработку персональных данных: перечня действия (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона. (ч.3 ст.6 Федерального закона)	не менее одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, ответственных за подготовку договора

6.	Осуществление проверки фактического уничтожения ПДн в информационных системах персональных данных, на материальных носителях ПДн (бумажных и машинных), а также ПДн на носителях информации с составлением соответствующих актов уничтожения в порядке, установленном в Министерстве образования Пензенской области. (п.7 ст.5 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн
7.	Проверка ведения Журнала обращений субъектов ПДн или их представителей, а также обеспечение учета предоставления ПДн субъектов ПДн по письменным запросам третьих лиц, в порядке установленном Федеральным законом и действующим законодательством Российской Федерации. (ст.14 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн
8.	Осуществление проверки на предмет выявления изменений в правилах обработки и защиты ПДн, установленных в Министерстве образования Пензенской области в соответствии с действующим законодательством Российской Федерации. (ч.2. ст.24 Федерального закона, п.3 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС

9.	Проверка наличия и актуальности Перечня персональных данных по каждой цели обработки персональных данных, обрабатываемых в Министерстве образования Пензенской области, и Перечня информационных систем персональных данных в Министерстве образования Пензенской области.	Не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн;
10.	Проверка соответствия установленных прав доступа к персональным данным в информационной системе (системах) персональных данных, государственной информационной системе Пензенской области (системах) трудовым (служебным) обязанностям сотрудников Министерства образования Пензенской области. (п.6. ч.2 ст.19 Федерального закона)	Не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС
11.	Реализация мероприятий по проверке актуализации Перечня мест хранения материальных носителей ПДн, соблюдения условий хранения материальных носителей ПДн, исключающих несанкционированный доступ к ним, а также раздельного хранения ПДн в случаях их обработки без использования средств автоматизации при несовместимости целей обработки ПДн.	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн

	(п. 5 ч.2 ст.19 Федерального закона, п.14 и п.15 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)			
12.	Проверка актуальности сведений, содержащихся в реестре операторов, осуществляющих обработку ПДн, которые размещены на официальном сайте уполномоченного органа по защите прав субъектов ПДн. (ст.22 Федерального закона).	не реже одного раза в полгода		- ответственный за организацию обработки ПДн
13.	Осуществление проверки по организации мероприятий по поддержанию в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Министерства образования Пензенской области в отношении обработки ПДн. Обеспечение неограниченного доступа к Политике Министерства образования Пензенской области в отношении обработки ПДн и сведениям о реализуемых требованиях к защите ПДн, в том числе размещение их на официальном сайте Министерства образования Пензенской области в информационно-телекоммуникационной сети. (п.2 ч.1 ст.18.1 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн, - администратор безопасности ИСПДН, ГИС

14.	Проверка организации анализа и пересмотра имеющихся актуальных угроз безопасности ПДн. (п.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
15.	Осуществление оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона с учетом соотношения указанного вреда и принимаемых Министерством образования Пензенской области, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом. (п.5 ч.1 ст.18.1 Федерального закона)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
16.	Осуществление сверки Перечня помещений, в которых размещена информационная система персональных данных (государственная информационная система Пензенской области), утвержденного в Министерстве образования Пензенской области, фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации. (пп. «а» п. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС

17.	Осуществление проверки актуальности утвержденного в Министерстве образования Пензенской области перечня лиц, доступ которых к ПДн, обрабатываемым в Министерства образования Пензенской области, необходим для выполнения ими трудовых (служебных) обязанностей. (пп. «в» п. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, п.13 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС
18.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия. (п.3 ч.2 ст.19 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС

19.	Проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн (далее - ИСПДн). (п.4 ч.2 ст.19 Федерального закона, п. 32 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	до издания приказа о вводе в эксплуатацию информационной системы ПДн, далее - 1 раз в 3 года. В случае проведения такого мероприятия в форме аттестации – не реже одного раза в 2 года с направлением протокола контроля защиты информации в ФСТЭК России		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
20.	Проведение проверки по обеспечению контроля за учетом машинных носителей персональных данных, на которых хранятся и (или) обрабатываются ПДн в ИСПДн, государственной информационной системе Пензенской области (далее - ГИС) путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей ПДн. (п.5 ч.2 ст.19 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
21.	Проверка наличия приказа Министерства образования Пензенской области о назначении администратора безопасности в ИСПДн, ГИС (далее - администратор безопасности).	не реже одного раза в полгода		ответственный за организацию обработки ПДн

	(п. 14 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119)			
22.	Обеспечение контроля за принимаемыми мерами в связи с изменениями в структурно-функциональные характеристики ИС, ГИС.	не реже одного раза в квартал		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
23.	Проверка реализации установленного в Министерстве образования Пензенской области порядка идентификации и аутентификации пользователей ИС, ГИС в соответствии с Инструкцией по идентификации и аутентификации.	не реже одного раза в квартал		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
24.	Проверка регистрации событий информационной безопасности в ИСПДн, ГИС в соответствии с Инструкцией по управлению событиями информационной безопасности, утвержденной в Министерства образования Пензенской области.	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
25.	Осуществление проверки реализации в Министерстве образования Пензенской области выявления инцидентов информационной безопасности и реагирования на них при наличии запланированных работ по аттестации ИС.	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС

	(п.6 ч.2 ст.19 Федерального закона, пп. «ж» п. 11 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)			
26.	Проверка организации антивирусной защиты в ИСПДн, ГИС и регулярности обновления базы данных признаков вредоносных программ (вирусов).	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
27.	Осуществление проверки по реализации мероприятий по выявлению, анализу и устранению уязвимостей в ИСПДн, ГИС. (пп. «з» п. 11 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
28.	Организация проведения проверки по реализации мероприятий по установке обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации.	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС

29.	Проверка организации размещения технических средств отображения информации ИСПДн, ГИС исключая ее несанкционированный просмотр, в соответствии с Инструкцией по защите технических средств ИСПДн, ГИС, утвержденной в Министерстве образования Пензенской области.	не менее одного раза в квартал		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС
30.	Проверка состояния работы по реализации процесса управления конфигурацией ИСПДн, ГИС и системы защиты информации. (пп. «ж» п. 11 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не менее одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности ИСПДн, ГИС
31.	Проверка состава технических средств, программного обеспечения и средств защиты информации, входящих в состав ИСПДн, ГИС на соответствие Техническому паспорту ИСПДн, ГИС. (п. 33 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, сотрудниками которых осуществляется обработка ПДн; - администратор безопасности ИСПДн, ГИС

Приложение № 5
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-07

План мероприятий по защите информации 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» на 202__ год
(далее - РИС ГИА)

№ п/п	Содержание планируемого мероприятия	Периодичность	Дата проведения мероприятия	Ответственный
1.	Назначение лица, ответственного за организацию обработки персональных данных в Министерстве образования Пензенской области	Разовое (по мере необходимости)		Министр образования Пензенской области
2.	Направление в уполномоченный орган (Роскомнадзор) уведомления о намерении осуществлять обработку персональных данных	Разовое (по мере необходимости)		Ответственный за организацию обработки персональных данных
3.	Утверждение Политики в отношении обработки персональных данных (далее - Политика) и обеспечение неограниченного доступа к Политике и сведениям о реализуемых требованиях к защите персональных данных, в том числе размещение их на официальном сайте – Министерства образования Пензенской области в информационно-телекоммуникационной сети)	Разовое (по мере необходимости)		Ответственный за организацию обработки персональных данных

4.	Назначение лица, ответственного за защиту информации в РИС ГИА, а также за планирование и контроль мероприятий по защите информации в РИС ГИА	Разовое (по мере необходимости)		Министр образования Пензенской области
5.	Назначение ответственного за управление (администрирование) системой защиты информации (далее - администратор безопасности) государственной информационной системы «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (далее - РИС ГИА;	Разовое (по мере необходимости)		Ответственный за защиту информации в РИС ГИА
6.	Утверждение перечня лиц, которым разрешены действия по внесению изменений в конфигурацию РИС ГИА; и ее системы защиты информации	Разовое (по мере необходимости)		Ответственный за защиту информации в РИС ГИА
7.	Утверждение перечня лиц, ответственных за выявление инцидентов в РИС ГИА и реагирование на них	Разовое (по мере необходимости)		Ответственный за защиту информации в РИС ГИА
8.	Назначение ответственного пользователя средств криптографической защиты информации	Разовое (по мере необходимости)		Ответственный за защиту информации в РИС ГИА
9.	Утверждение перечня персональных данных, обрабатываемых в РИС ГИА	По мере необходимости		Ответственный за организацию обработки персональных данных

10.	Определение степени оценки вреда, который может быть причинен субъектам персональных данных, чьи персональные данные обрабатываются в РИС ГИА, в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом	По мере необходимости		Ответственный за организацию обработки персональных данных в Министерстве образования Пензенской области
11.	Определение типа актуальных угроз безопасности персональных данных в РИС ГИА с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», типу актуальных угроз безопасности персональных данных, указанному в утвержденном министром образования Пензенской области Акте классификации РИС ГИА. Классификация РИС ГИА.	По мере необходимости		-Ответственный за организацию обработки персональных данных, - ответственный за защиту информации в РИС ГИА, - комиссия по установлению класса защищенности РИС ГИА
12.	Определение лиц, доступ которых к персональным данным, обрабатываемым РИС ГИА, необходим для выполнения ими трудовых (служебных) обязанностей	По мере необходимости		Ответственный за организацию обработки персональных данных
13.	Доведение до сведения положений законодательства Российской Федерации о персональных данных, разработанных внутренних локальных актов по вопросам обработки персоналных данных и требований к защите персональных данных	По мере необходимости		Ответственный за организацию обработки персональных данных
14.	Информирование персонала РИС ГИА о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации РИС ГИА	не реже 1 раза в два года		Ответственный за защиту информации

15.	Доведение до персонала РИС ГИА требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений	по мере необходимости		Ответственный за защиту информации
16.	Обучение персонала РИС ГИА правилам эксплуатации отдельных средств защиты информации	Не реже 1 раза в год		Администратор безопасности
17.	Проведение практических занятий и тренировок с персоналом РИС ГИА по блокированию угроз безопасности информации и реагированию на инциденты	Не реже 1 раза в год		Администратор безопасности
18.	Контроль осведомленности персонала РИС ГИА об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.	Не реже1 раза в год		Ответственный за защиту информации
19.	Организация приёма и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приёмом и обработкой таких обращений и запросов	По мере необходимости		Ответственный за организацию обработки персональных данных
20.	Получение согласий субъектов персональных данных на обработку персональных данных и разъяснений субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в случаях, когда этого требует законодательство Российской Федерации	По мере необходимости		-Ответственный за организацию обработки персональных данных, -руководители структурных подразделений, сотрудниками которых осуществляется обработка персональных данных
21.	Получение от сотрудников обязательств о соблюдении конфиденциальности персональных данных, документа об информировании о факте обработки персональных данных без использования средств автоматизации, разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	По мере необходимости		-Ответственный за организацию обработки персональных данных, -руководители структурных подразделений, сотрудниками которых осуществляется обработка персональных данных

22.	Утверждение границ контролируемой зоны РИС ГИА и перечня помещений, в которых размещена РИС ГИА	По мере необходимости		Ответственный за защиту информации
23.	Определение перечня лиц, имеющих право доступа в помещения, в которых размещена РИС ГИА	По мере необходимости		Ответственный за защиту информации
24.	Определение мест хранения материальных носителей персональных данных и обеспечение контроля хранения материальных носителей персональных данных в условиях, исключающих несанкционированный доступ к ним, а также обеспечение раздельного хранения персональных данных в случаях их обработки без использования средств автоматизации при несовместимости целей обработки персональных данных;	По мере необходимости		Ответственный за организацию обработки персональных данных
25.	Организация режима обеспечения безопасности помещений, в которых размещена РИС ГИА, препятствующих возможности неконтролируемого проникновения или пребывания в указанных помещениях лиц, не имеющих права доступа в них	По мере необходимости		Ответственный за организацию обработки персональных данных, Ответственный за защиту информации
26.	Утверждение перечня помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств	По мере необходимости		Ответственный пользователь криптосредств
27.	Утверждение перечня лиц, допущенных к работе со средствами криптографичсской защиты информации	По мере необходимости		Ответственный пользователь криптосредств
28.	Учет и обеспечение эксплуатации средств криптографической защиты	Постоянно		Ответственный пользователь криптосредств

29.	Разработка и актуализация организационно-распорядительной документации по обработке и защите информации (в том числе персональных данных) в РИС ГИА	По мере необходимости		- Ответственный за организацию обработки персональных данных. - Ответственный ха защиту информации - администратор безопасности
30.	Наличие сертификатов соответствия требованиям безопасности информации на все используемые средства защиты информации	По мере необходимости		- Ответственный за организацию обработки персональных данных, - Ответственный за защиту информации, - администратор безопасности
31.	Реализация управления доступом к РИС ГИА	постоянно		администратор безопасности
32.	Учет машинных носителей информации (в том числе персональных данных) и контроль их использования	постоянно		администратор безопасности
33.	Регистрация событий информационной безопасности в РИС ГИА	постоянно		администратор безопасности
34.	Организация и реализация антивирусной защиты	постоянно		-Ответственный за защиту информации, - Ответственный за защиту информации, - администратор безопасности
35.	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	не позднее 1 рабочего дня с момента возникновения инцидента		- Ответственный за защиту информации, - Ответственный за организацию обработки персональных данных - администратор безопасности
36.	Планирование и принятие мер по устранению инцидентов, в том числе по восстановлению РИС ГИА и ее сегментов в случае отказа в обслуживании или после сбоев,	в случае необходимости		Администратор безопасности

	устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов			
37.	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	в случае необходимости		Ответственный за защиту информации
38.	Настройка правильности функционирования программного обеспечения и средств защиты информации в РИС ГИА	постоянно		-администратор безопасности, -администратор
39.	Организация физического доступа к техническим средствам, средствам защиты информации РИС ГИА, (в том числе опечатывание корпуса средств вычислительной техники)	По мере необходимости		-Ответственный за защиту информации, - администратор безопасности
40.	Обновление программного обеспечения, в том числе обновление программного обеспечения средств защиты информации	По мере необходимости		-администратор безопасности, -администратор
41.	Управление конфигурацией РИС ГИА и системы защиты	По мере необходимости		-Ответственный за защиту информации, - администратор безопасности, -лица, которым разрешены действия по внесению изменений в конфигурацию РИС ГИА и системы защиты
42.	Осуществление внутреннего контроля обработки и защиты персональных данных по отдельному плану	согласно плану		-Ответственный за организацию обработки персональных данных, - администратор безопасности, -руководители структурных

					подразделений, сотрудниками которых осуществляется обработка персональных данных

Приложение № 6
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-07

Инструкция
о порядке взаимодействия с уполномоченным органом
по защите прав субъектов персональных данных
в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1 Инструкция о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Министерстве образования Пензенской области (далее - Инструкция) определяет порядок действий в Министерстве образования Пензенской области по выполнению положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при взаимодействии с уполномоченным органом защите прав субъекгов персональных данных (далее – территориальный орган Роскомнадзора).

1.2 В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно. Иные термины, применяемые в настоящей Инструкции, используются в значениях, определенных законодательством Российской Федерации в области обработки и защиты персональных данных.

Таблица 1 – Перечнь сокращений

Сокращение	Расшифровка сокращений
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
Федеральный закон № 152-ФЗ	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Обработка персональных данных	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными	Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»

1.3 Лица, осуществляющие обработку персональных данных, должны быть ознакомлены с настоящей Инструкцией до начала обработки под подпись. Обязанность по организации ознакомления сотрудников с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн в Министерстве образования Пензенской области (далее – ответственный за организацию обработки ПДн).

1.4 Обязанность по организации выполнения требований данной Инструкции возлагается на ответственного за организацию обработки ПДн.

2. Порядок действий ответственного за организацию обработки ПДн

2.1 Перед началом обработки персональных данных ответственный за организацию ПДн обеспечивает уведомление территориального органа Роскомнадзора по месту нахождения Министерства образования Пензенской области о намерении Министерства образования Пензенской области осуществлять обработку ПДн.

2.2 В случае изменения сведений, указанных в уведомлении о намерении осуществлять обработку ПДн, Ответственный за организацию обработки ПДн **не позднее 15-го числа** месяца, следующего за месяцем, в котором возникли такие изменения, организует направление в территориальный орган Роскомнадзора уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку ПДн. В случае прекращения обработки ПДн ответственный за организацию обработки ПДн организует направление в территориальный орган Роскомнадзора уведомления о прекращении обработки ПДн, в срок, не превышающий **10 рабочих дней** с даты прекращения обработки ПДн.

2.3 Если из территориального органа Роскомнадзора поступил запрос о предоставлении информации, то ответственный за организацию обработки ПДн в **течение 10 рабочих дней** с момента получения запроса из территориального органа Роскомнадзора формирует и организует направление ответа на запрос. Указанный срок может быть продлен, но не более чем **на 5 рабочих дней в** случае направления ответственным за организацию обработки ПДн в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

2.4 Полученные запросы уполномоченного органа по защите прав субъектов ПДн регистрируются ответственным за организацию обработки ПДн в Журнале учета запросов уполномоченного органа по защите прав субъектов ПДн **(Приложение)**.

2.5 При получении правомерного запроса из территориального органа Роскомнадзора на исправление выявленных нарушений ответственный за организацию обработки ПДн организует силами администраторов безопасности ИСПДн, администраторов ИСПДн, в которых обрабатываются указанные ПДн, разработку перечня действий по устранению выявленных нарушений и обеспечивает его согласование с заинтересованными подразделениями Министерства образования Пензенской области. Устранение выявленных нарушений осуществляется в срок, **не превышающий 3 рабочих дней** со дня выявления нарушений. По факту устранения нарушений уведомляется территориальный орган Роскомнадзора через регистрируемое почтовое отправление с заказным уведомлением о вручении. Контроль за своевременным уведомлением территориального органа Роскомнадзора возлагается на ответственного за организацию обработки ПДн.

2.6 Уведомление об устранении нарушений в порядке обработки ПДн, ответственный за организацию обработки ПДн регистрирует в Журнале учета запросов уполномоченного органа по защите прав субъектов ПДн.

2.7 В случае, если обеспечить правомерность обработки ПДн невозможно, то ответственный за организацию обработки ПДн оформляет служебную записку на имя руководителя Министерства образования Пензенской области о необходимости уничтожения ПДн. Уничтожение ПДн осуществляется Комиссией Министерства образования Пензенской области в соответствии с Положением о комиссии Министерства образования Пензенской области по уничтожению персональных данных, утвержденным приказом Министерства образования Пензенской области, в

срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн. По факту уничтожения ПДн составляется Акт об уничтожении персональных данных, а также обеспечивается выгрузка из журнала регистрации событий в соответствующей информационной системе персональных данных (при наличии). Об уничтожении указанных ПДн уведомляется территориальный орган Роскомнадзора в порядке, установленном пунктом 2.6 настоящей Инструкции.

2.8 В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, ответственный за организацию обработки ПДн с момента выявления такого инцидента Министерства образования Пензенской области, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомляет территориальный орган Роскомнадзора:

- **в течение 24 часов** о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном Министерством образования Пензенской области на взаимодействие с территориальным органом Роскомнадзора, по вопросам, связанным с выявленным инцидентом;

- **в течение 72 часов** о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Для передачи указанной информации в территориальный орган Роскомнадзора необходимо перейти по ссылке: https://pd.rkn.gov.ru/incidents/

2.9 В случае, если территориальным органом Роскомнадзора осуществлялась выездная проверка, то по её окончании должностное лицо территориального органа Роскомнадзора производит запись о проведенной проверке в журнале учета проверок. Форма журнала регламентирована приказом министерства экономического развития Российской Федерации от 30.04.2009 № 141 «О реализации положений Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». Ведение указанного журнала обеспечивает ответственный за организацию обработки ПДн.

3. Взаимодействие с территориальным органом с использованием информационно-телекоммуникационной сети Интернет

3.1 Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является дополнительным средством для обеспечения возможности обращений граждан объединений граждан и юридических лиц в Роскомнадзор. Для подготовки и отправки уведомления о намерении осуществлять обработку персональных данных либо уведомления об изменении сведений, содержащихся в уведомлении о намерении

осуществлять обработку персональных данных (далее – информационное письмо) необходимо перейти на официальный сайт Роскомнадзора в информационно-телекоммуникационной сети Интернет по адресу **http://pd.rkn.gov.ru/operators-registry/notification/form/**

3.2 Для отправки уведомления либо информационного письма требуется выбрать один из трех способов заполнения и направления уведомления либо информационного письма в территориальный орган Роскомнадзора:

- сформировать уведомление либо информационное письмо и направить его в бумажном виде;

- сформировать уведомление и направить в электронном виде с использованием усиленной квалифицированной электронной подписи;

- сформировать уведомление и направить в электронном виде с использованием средств аутентификации Единой системы идентификации и аутентификации.

3.3 В случае выбора способа направления уведомления (информационного) письма в Роскомнадзор в бумажном виде и после открытия соответствующей формы, следует её заполнить и отправить в информационную систему Роскомнадзора, а затем распечатать заполненную форму на бланке письма Министерства образования Пензенской области, подписать её у министра образования Пензенской области, поставить печать Министерства образования Пензенской области и направить в соответствующий территориальный орган Роскомнадзора по месту нахождения Министерства образования Пензенской области нарочным под подпись о получении сотрудником территориального органа Роскомнадзора.

3.4 В случаях, если форма подписывается усиленной квалифицированной электронной подписью либо направляется в электронном виде с использованием средств аутентификации Единой системы идентификации и аутентификации, то её дальнейшее направление на бумажном носителе в территориальный орган Роскомнадзора не требуется.

3.5 При выборе способа направления формы с использованием усиленной квалифицированной электронной подписи необходим плагин КриптоПро ЭЦП Browser plug-in и настроена работа с ним.

3.6 В случае выбора способа направления формы в электронном виде с использованием средств аутентификации Единой системы идентификации и аутентификации требуется пройти аутентификацию на портале Государственных услуг, заполнить форму и направить ее в электронном виде. При этом уже должна иметься подтвержденная учетная запись, привязанная к Министерству образования Пензенской области на портале Государственных услуг.

4. Ответственность

4.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией в соответствии с действующим законодательством Российской Федерации.

Приложение

к Инструкции о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Министерстве образования Пензенской области

Журнал

запросов уполномоченного органа по защите прав субъектов персональных данных

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№	Краткое содержание запроса	Цель запроса	Отметка об ответе на запрос	Дата передачи ответа на запрос.	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7
1	*перечень выявленных при проверке нарушений*	*устранение выявленных нарушений*	*отправлены сроки исправления нарушений*	*01.01.2021*	*ИНН, Фамилия ответственного за организацию обработки ПДн*	*Пример заполнения*

Лист _____

Правила

по формированию и ведению журнала запросов уполномоченного органа по защите прав субъектов персональных данных

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается), подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

2.1 Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

2.2 Графы журнала заполняются следующим образом:

- Графа 1 – номер записи по порядку.
- Графа 2 – краткое содержание запроса (например – перечень выявленных при проверке нарушениях).
- Графа 3 – цель запроса (например – устранение выявленных нарушений).
- Графа 4 – запись об отправленном ответе (например – отправлены сроки исправления нарушений).
- Графа 5 – дата отправки ответа.
- Графа 6 – подпись сотрудника, отправившего ответ.
- Графа 7 – любая информация, касающаяся данного запроса.

2.3 Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 7
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция
пользователя государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»
(РИС ГИА)

Оглавление

1. Общие положения

1.1 Инструкция пользователя РИС ГИА (далее – Инструкция) определяет в Министерстве образования Пензенской области, права и ответственность пользователей РИС ГИА.

1.2 Пользователями РИС ГИА являются сотрудники Министерства образования Пензенской области, допущенные к информационным ресурсам 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 - РИС ГИА) в соответствии с утвержденным Министерством образования Пензенской области приказом «О предоставлении пользователям доступа к информационным ресурсам государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования».

1.3. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	**Расшифровка сокращения**
АРМ	Автоматизированное рабочее место
ИС	Информационная система
ПДн	Персональные данные
СВТ	Средства вычислительной техники

Таблица 2 – Перечень терминов и определений

Термин	**Определение**	**Источник**
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден

Термин	Определение	Источник
		ФСТЭК России 11.02.2014
Государственные информационные системы	Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов	Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде.	
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.4. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

приказ ФСБ России от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности»,

приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственной тайны».

1.5. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы с РИС ГИА. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Обязанности пользователя РИС ГИА

2.1. Пользователи РИС ГИА обязаны знать и выполнять требования законодательства Российской Федерации и локальных актов Министерства образования Пензенской области устанавливающих правила обработки и защиты информации в РИС ГИА.

2.2. 11ри эксплуатации РИС ГИА с целью защиты информации в РИС ГИА пользователь обязан:

- руководствоваться требованиями организационно – распорядительной документации по организации обработки и защиты информации, в том числе персональных данных;
- соблюдать установленную технологию обработки и защиты информации в РИС ГИА;
- знать свои идентификаторы и пароли, осуществлять ввод паролей в условиях, исключающих их просмотр;
- не записывать значения паролей на бумагу, электронные носители, иные предметы и не разглашать (не сообщать или любым другим способом не доводить до кого-либо, включая сотрудников Министерства образования Пензенской области, в т.ч.

руководителей, администратора безопасности и администратора РИС ГИА) значения действующих паролей;

- осуществлять смену пароля не реже, чем через 90 дней;
- надежно хранить индивидуальный аппаратный аутентификатор, не передавать индивидуальный аппаратный аутентификатор другим лицам;
- ежедневно вести антивирусный контроль на непосредственных средствах вычислительной техники (далее – СВТ);
- проверять вложения электронной почты, съемные машинные носители информации перед началом работы на предмет наличия вредоносного программного обеспечения (далее – ПО);
- использовать для записи ПДн только съемные машинные носители информации, учтенные в установленном порядке;
- хранить съемные машинные носители персональных данных в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним;
- использовать для вывода на печать документов, содержащих информацию, находящуюся в РИС ГИА, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники РИС ГИА посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ.

В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ РИС ГИА, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ.

Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Докладывать администратору безопасности и своему непосредственному руководителю:

- о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ РИС ГИА, помещениям, в которых располагаются СВТ РИС ГИА, и хранилищам;
- об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка ПДн и хранилищ;
- об обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), при иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.), а также при нетипичном

поведении РИС ГИА (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбои в работе);

- о попытках получения информации лицами, не имеющими к ней допуска;
- о попытках неконтролируемого проникновения посторонних лиц в помещения контролируемой зоны РИС ГИА;
- об иных нештатных ситуациях, связанных с угрозой безопасности РИС ГИА.

2.5. Пользователю запрещается:

- подключать к СВТ РИС ГИА нештатные устройства;
- применять в РИС ГИА незарегистрированные машинные носители информации либо использовать учтенные машинные носители информации в неслужебных целях;
- выносить машинные носители информации, мобильные технические средства данных за пределы контролируемой зоны без письменного разрешения министра образования Пензенской области;
- несанкционированно вносить незарегистрированные машинные носители информации, мобильные технические средства;
- блокировать, изменять настройки и выгружать антивирусное ПО на своих СВТ;
- самостоятельно осуществлять подключение (отключение) СВТ к локальной вычислительной сети;
- продолжать работы на СВТ при обнаружении вредоносного ПО в процессе обработки информации;
- самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ РИС ГИА;
- самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в РИС ГИА;
- самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) РИС ГИА;
- сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к РИС ГИА;
- разрешать работу с СВТ РИС ГИА лицам, не допущенным к обработке ПДн в установленном порядке;
- находиться в нерабочее время в помещениях, где размещено оборудование РИС ГИА и СЗИ без служебной записки (или иного вида разрешающего документа), подписанного министром образования Пензенской области.

3. Права пользователя РИС ГИА

3.1. Пользователь РИС ГИА имеет право:

- обращаться к администратору безопасности, администратору РИС ГИА и ответственному за организацию обработки ПДн, ответственному за защиту

информации в РИС ГИА по любым вопросам, касающихся обработки и защиты информации в РИС ГИА (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации в РИС ГИА);

- обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в РИС ГИА информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);
- обращаться к администратору и администратору безопасности РИС ГИА с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств РИС ГИА.

4. Ответственность

4.1. На пользователя РИС ГИА возлагается персональная ответственность:

- за соблюдение установленной технологии обработки защищаемой информации, в том числе ПДн;
- за соблюдение режима конфиденциальности информации;
- за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в РИС ГИА;
- за соблюдение требований локальных актов по вопросам обработки и защиты информации, в том числе ПДн, в РИС ГИА.

4.2. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 8
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Положение

о порядке организации и проведении работ по защите информации, обрабатываемой 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»
(РИС ГИА)

Оглавление

1. Общие положения

1.1 Настоящее Положение о порядке организации и проведении работ по защите информации, обрабатываемой в РИС ГИА в Министерстве образования Пензенской области (далее – Положение), разработано в соответствии со следующими нормативными правовыми актами Российской Федерации в области обработки и обеспечения безопасности информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация):

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
- приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственной тайны».

1.2 Сокращения, термины и определения

В настоящем Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Антивирусное ПО	Программное обеспечение средств антивирусной защиты
Вредоносное ПО	Вредоносная компьютерная программа (вирус)
АРМ	Автоматизированное рабочее место
ГИС	Государственная информационная система
ПДн	Персональные данные

Сокращение	Расшифровка сокращения
ПО	Программное обеспечение
СВТ	Средства вычислительной техники

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России от 11.02.2014
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России от 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»,

Термин	Определение	Источник
	(нарушению конфиденциальности, целостности, доступности)	утвержден ФСТЭК России от 11.02.2014
Компьютерный вирус	Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы	ГОСТ Р 51275-2006
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных (далее – ПДн)) в электронном виде.	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Событие информационной безопасности	Идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России от 11.02.2014

1.3 Администратор безопасности, администратор и пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись.

Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

1.4. Для координации и контроля выполнения мероприятий по организации обработки и защиты персональных данных в Министерстве образования Пензенской области назначается должностное лицо, ответственное за организацию обработки персональных данных.

При выполнении своих обязанностей ответственный за организацию обработки персональных данных руководствуется требованиями Инструкции ответственного за организацию обработки персональных данных в Министерстве образования Пензенской области.

1.5 В Министерства образования Пензенской области утверждены Правила обработки персональных данных в РИС ГИА в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке персональных данных в РИС ГИА;

- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о персональных данных, иных правовых актов Российской Федерации, внутренних документов Министерства образования Пензенской области по вопросам обработки и защиты персональных данных;

- определения целей обработки персональных данных в Министерстве образования Пензенской области в установленной сфере деятельности, включая содержание обрабатываемых персональных данных, категории субъектов персональных данных, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых персональных данных, а также порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований;

- установления ответственности сотрудников Министерства образования Пензенской области, имеющих доступ к персональным данным субъектов персональных данных в РИС ГИА, за невыполнение требований норм, регулирующих обработку персональных данных, установленных законодательством Российской Федерации, настоящими Правилами и иными локальными актами Министерства образования Пензенской области.

1.6 Для непосредственного выполнения работ по обеспечению безопасности защищаемой информации, не содержащей информацию, составляющей государственную тайну, в том числе персональных данных с использованием программно-аппаратных средств защиты информации (далее – СЗИ) назначается администратор безопасности.

При выполнении своих обязанностей администратор безопасности действует в соответствии с требованиями Инструкции администратора безопасности РИС ГИА и требованиями эксплуатационной документации на средства защиты информации, используемые в составе системы защиты информации.

1.7 Для обеспечения защиты информации, содержащейся в РИС ГИА, назначается лицо, ответственное за защиту информации в РИС ГИА, а также за планирование и контроль мероприятий по защите информации в РИС ГИА.

При выполнении своих обязанностей ответственный за защиту информации в РИС ГИА действует в соответствии с требованиями Инструкции ответственного за защиту информации в РИС ГИА, а также за планирование и контроль мероприятий по защите информации в РИС ГИА.

1.8 Все пользователи РИС ГИА участвуют в защите информации, содержащейся в РИС ГИА, и обязаны знать и выполнять требования:

– нормативных правовых документов Российской Федерации по защите информации, в том числе по защите персональных данных;

- настоящего Положения и перечисленных в нём инструкций, в части их касающейся;
- Инструкции пользователя РИС ГИА.

1.9 В ходе эксплуатации РИС ГИА обеспечение безопасности защищаемой информации обеспечивается выполнением процедур:

- управления (администрирования) системой защиты информации в РИС ГИА;
- выявления инцидентов и реагирования на них;
- управления конфигурацией РИС ГИА и её системы защиты информации;
- контроля обеспечения уровня защищённости персональных данных в РИС ГИА.

2. Управление системой защиты информации РИС ГИА

2.1 Процедуры управления системой защиты информации обеспечивают:

- функционирование системы защиты информации РИС ГИА в штатном режиме с характеристиками, установленными в проектной документации;
- документированный поток информации о событиях безопасности в РИС ГИА и её системе защиты, на основании которой возможна реализация процедур управления инцидентами, управления конфигурацией РИС ГИА и её системы защиты, процедуры контроля уровня защищённости информации, обрабатываемой в РИС ГИА.

2.2 Порядок действий пользователей РИС ГИА при прохождении процедур идентификации (узнавании) и аутентификации (подтверждении подлинности узнанного пользователя) при входе в РИС ГИА отражается в Инструкции по идентификации и аутентификации пользователей РИС ГИА.

2.3. Порядок управления доступом пользователей к информационным ресурсам РИС ГИА устанавливается в Инструкции по управлению доступом к РИС ГИА.

2.4. Порядок действий пользователей РИС ГИА при работе с машинными носителями информации (в том числе персональных данных), правила учёта, хранения и доступа к машинным носителям информации устанавливается в Инструкции по защите машинных носителей информации РИС ГИА.

2.5 Порядок действий администратора безопасности и администраторов РИС ГИА при появлении событий безопасности отражается в Инструкции по управлению событиями информационной безопасности РИС ГИА.

2.6 Порядок действий пользователей при обнаружении вредоносного ПО, описаны в Инструкции по антивирусной защите РИС ГИА.

2.7. Порядок выявления, идентификации, регистрации инцидентов информационной безопасности, их анализ и принятие мер по устранению последствий инцидентов информационной безопасности и предотвращению повторного возникновения инцидентов информационной безопасности в РИС ГИА определен в Порядке по выявлению инцидентов в РИС ГИА и реагированию на них».

2.8 Порядок действий администраторов и администратора безопасности РИС ГИА с целью:

- выявления ошибок и недостатков программного обеспечения и аппаратных средств, и средств защиты персональных данных РИС ГИА;

- контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;
- контроля состава технических и программных средств РИС ГИА, в том числе средств защиты информации описан в Инструкции по контролю (анализу) защищенности информации в РИС ГИА.

2.9. Порядок доступа пользователей к техническим средствам РИС ГИА и ее системы защиты информации описан в Инструкции по защите технических средств РИС ГИА.

2.10. Организация и последовательность действий в случае необходимости принятия решения о внесении изменений в конфигурацию РИС ГИА и системы защиты персональных данных определены в Порядке по управлению изменениями в конфигурации РИС ГИА.

2.11. Организация резервного копирования и восстановления защищаемой информации в РИС ГИА обеспечивается ответственным за защиту информации в РИС ГИА с заданной им периодичностью в соответствии с Матрицей доступа пользователей к РИС ГИА.

2.12. Организация режима безопасности помещений, в которых размещена РИС ГИА, правила доступа в помещения в рабочее, нерабочее время и в нештатных ситуациях определены в Порядке доступа в помещения, в которых размещена информационная система РИС ГИА.

2.13. Обеспечение безопасности защищаемой информации в РИС ГИА с использованием средств криптографической защиты информации осуществляется в соответствии с Положением по использованию средств криптографической защиты информации в Министерстве образования Пензенской области, Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Министерстве образования Пензенской области, Инструкцией пользователя средств криптографической защиты информации в Министерстве образования Пензенской области, Инструкцией ответственного пользователя средств криптографической защиты информации в Министерстве образования Пензенской области.

3. Контроль обеспечения уровня защищённости информации РИС ГИА

3.1 Периодичность контроля обеспечения уровня защищённости информации, обрабатываемой в РИС ГИА, составляет не реже одного раза в год.

3.2 Для контроля обеспечения уровня защищённости используются следующие документы:

- отчёты о событиях информационной безопасности;
- акты расследования инцидентов;
- журнал регистрации инцидентов;
- результаты контроля защищённости;
- информация из специальных источников по новым угрозам безопасности для используемых в РИС ГИА программных и программно – технических средств.

3.3 Порядок осуществления контроля за обеспечением уровня защищённости информации в РИС ГИА (далее – внутренний контроль) определен в Правилах осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Министерстве образования Пензенской области.

3.4 На основании выводов по результатам внутреннего контроля ответственный за защиту информации в РИС ГИА при необходимости доработки системы защиты информации докладывает об этом министру образования Пензенской области. Решение о доработке и последующей аттестации принимает министр образования Пензенской области.

3.5 Контроль за обеспечением уровня защищенности персональных данных может проводиться Министерством образования Пензенской области самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

4. Протоколы контроля и защиты информации в РИС ГИА

4.1. Министерство образования Пензенской области обеспечивает поддержку безопасности РИС ГИА в соответствии с аттестатом соответствия путем реализации требований по защите информации в ходе эксплуатации аттестованной РИС ГИА и проведения периодического контроля уровня защиты информации аттестованной РИС ГИА, результаты которого оформляются протоколами и отражаются в Техническом паспорте РИС ГИА.

4.2. Протоколы контроля защиты информации аттестованной РИС ГИА не реже 1раза в два года представляются владельцем объекта информатизации в ФСТЭК России (территориальный орган ФСТЭК России). Непредставление протоколов контроля защиты информации в ФСТЭК России (территориальный орган ФСТЭК России) является основанием для приостановления действия аттестата соответствия.

5. Ответственность

5.1. Пользователи РИС ГИА должны быть предупреждены об ответственности за действия с защищаемой информацией, содержащейся в РИС ГИА, и действия с техническими средствами РИС ГИА и системы защиты информации, нарушающие требования настоящего Положения и других организационно-распорядительных документов, определяющих меры по обеспечение безопасности защищаемой информации в РИС ГИА.

Приложение № 9
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция
по идентификации и аутентификации пользователей государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по идентификации и аутентификации пользователей РИС ГИА (далее - Инструкция) определяет в Министерства образования Пензенской области порядок идентификации и аутентификации пользователей РИС ГИА, являющихся сотрудниками Министерства образования Пензенской области, порядок управления аппаратными средствами аутентификации, порядок идентификации и аутентификации устройств, а также обязанности пользователей РИС ГИА и администратора безопасности РИС ГИА.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ИС	Информационная система персональных данных
ПДн	Персональные данные

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Аутентификационная информация	Информация, используемая для установления подлинности	Методический документ ФСТЭК России «Меры

Термин	Определение	Источник
	(верификации) субъекта доступа в информационной системе	защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Идентификатор	Представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Многофакторная аутентификация	Аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»,

Термин	Определение	Источник
		утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в ГИС под подпись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Порядок идентификации и аутентификации внутренних пользователей

2.1. К работе в РИС ГИА допускается только определенный круг пользователей.

К внутренним пользователям РИС ГИА относятся сотрудники Министерства образования Пензенской области, допуск которых осуществляется в минимальном объеме, необходимом для выполнения трудовых (служебных) обязанностей, в соответствии с утвержденным приказом Министерства образования Пензенской области перечнем лиц, имеющих доступ к защищаемой информации (в том числе

персональным данным) в РИС ГИА, содержащей сведения, не составляющие государственную тайну, который необходим для выполнения ими трудовых (служебных) обязанностей.

Пользователю РИС ГИА присваивается уникальная символьная последовательность в виде персонального идентификатора (логин, имя пользователя), которая однозначно его идентифицирует. Идентификаторы определяют доступ к техническим средствам и информационным ресурсам РИС ГИА и ее системе защиты информации.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в РИС ГИА и пароль, обеспечивающий аутентификацию в РИС ГИА.

Права пользователя по доступу к информационным ресурсам РИС ГИА, определяются в соответствии со служебной запиской начальника структурного подразделения на имя министра образования Пензенской области.

2.3. Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более *90* дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены из РИС ГИА при увольнении сотрудника немедленно по окончании последнего сеанса работы пользователя, а уволенный сотрудник должен быть исключен из числа пользователей РИС ГИА.

2.4. При приеме (увольнении) на работу лица или изменении полномочий (временное или бессрочное) действующего сотрудника Министерства образования Пензенской области, изменения в его доступе к информационным ресурсам РИС ГИА и генерацию (уничтожение) идентификаторов и паролей, производит администратор безопасности.

Исключается повторное использование идентификатора в течение времени - не менее 1 года.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и выдаются пользователю под подпись в журнале учета выдачи первичных паролей РИС ГИА (Приложение №1 к настоящей Инструкции).

Ведение и надежное хранение журнала учета выдачи первичных паролей РИС ГИА (далее - Журнал) осуществляет администратор безопасности.

Срок хранения завершенного Журнала определяется утвержденной номенклатурой Министерства образования Пензенской области.

Уничтожение Журнала по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерстве образования Пензенской области.

2.6. Идентификация и аутентификация пользователя РИС ГИА осуществляется при доступе в ИС. Авторизация пользователей РИС ГИА производится на основании положительных результатов аутентификации.

При первом доступе к РИС ГИА пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции (пункт 2.8).

2.7. В случаях, предусмотренных нормативными документами по обеспечению защиты информации, в том числе персональных, не содержащей сведения, составляющие государственную тайну, обрабатываемой в РИС ГИА, либо по решению министра образования Пензенской области помимо паролей могут использоваться дополнительные атрибуты доступа – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надежную многофакторную аутентификацию.

2.8. Требования к сложности пароля:

– длина пароля должна быть не менее 6 символов;

– алфавит пароля не менее 70 символов;

– в числе символов пароля обязательно должны присутствовать латинские строчные и прописные буквы, цифры и специальные символы;

– пароль не должен включать в себя легко вычисляемые значения символов (имена, фамилии, имена детей или домашних животных, наименования информационных систем, типичных для организации профессиональных терминов, номера телефонов, номера или марки автомобилей, адреса и т. д., а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.) и другие данные, которые могут быть подобраны путем анализа информации о пользователе);

– в качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 символах;

– новое значение пароля не должно совпадать с 5 предыдущими значениями пароля.

2.9. Пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.10. Администратор безопасности осуществляет настройку в РИС ГИА:

– политики паролей в соответствии с п.2.8, п.2.9;

– параметров количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки до 5 попыток;

– блокирование программно-технического средства или учетной записи пользователя РИС ГИА в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут;

– блокирование сеанса доступа в РИС ГИА после установленного времени бездействия (неактивности) пользователя 30 минут или по запросу пользователя.

2.11. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

2.12. Администратор безопасности контролирует настройку защиты обратной связи при вводе аутентификационной информации (исключение отображения для пользователя действительного значения пароля, когда вводимые символы отображаются условными знаками «*»).

3. Управление аппаратными средствами аутентификации

3.1. В случае использования аппаратных средств аутентификации пользователей (смарт-карты, электронные ключи) выдачу, инициализацию, блокирование и утилизацию аппаратных средств аутентификации организует администратор безопасности.

3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор безопасности в журнале учета аппаратных средств аутентификации Министерства образования Пензенской области (Приложение №2 к настоящей Инструкции).

Ведение и надежное хранение журнала учета аппаратных средств аутентификации Министерства образования Пензенской области осуществляет администратор безопасности.

Срок хранения завершенного журнала учета аппаратных средств аутентификации Министерства образования Пензенской области определяется утвержденной номенклатурой Министерства образования Пензенской области.

Уничтожение журнала учета аппаратных средств аутентификации Министерства образования Пензенской области по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерстве образования Пензенской области.

4. Идентификация и аутентификация внешних пользователей (при наличии)

4.1. Присвоение идентификатора и выдача атрибутов аутентификации внешним пользователям РИС ГИА, осуществляется администратором безопасности. Учет внешних пользователей, допущенных к обработке защищаемой информации (в том числе персональных данных) в РИС ГИА, содержащей сведения, не составляющие государственную тайну (далее – защищаемая информация) осуществляет администратор безопасности.

4.2. Выдачу и смену паролей, учет паролей, учет аппаратных средств аутентификации внешних пользователей, допущенных к обработке защищаемой информации, организует администратор безопасности по правилам пунктов 2, 3 настоящей Инструкции.

5. Обязанности пользователя

5.1. Пользователь РИС ГИА является частью системы обеспечения безопасности защищаемой информации и обязан соблюдать следующие правила информационной безопасности:

- знать, помнить свой идентификатор и пароль для доступа к РИС ГИА;
- не разглашать, не сообщать или любым другим способом не доводить до кого-либо, включая сотрудников Министерства образования Пензенской области, в т.ч. руководителей, администратора безопасности и администратора, значения действующих паролей;
- не записывать значения паролей на бумагу, электронные носители, иные предметы;
- осуществлять ввод паролей в условиях, исключающих просмотр;
- осуществлять смену пароля не реже, чем через 90 дней;
- надежно хранить индивидуальный аппаратный идентификатор,
- не передавать индивидуальный аппаратный идентификатор другим лицам;
- немедленно сообщать администратору безопасности о фактах компрометации паролей, об утере либо повреждении индивидуального аппаратного идентификатора. В этих случаях не использовать РИС ГИА до специального разрешения администратора безопасности.

6. Обязанности администратора безопасности

6.1. Администратор безопасности осуществляет 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.

6.2. Администратор безопасности обязан:

- создавать, присваивать, уничтожать, вести учет и осуществлять выдачу пользователям персональных идентификаторов и паролей 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 и надежно хранить Журнал учета выдачи первичных паролей РИС ГИА;
- надежно хранить и вести учет аппаратных средств аутентификации по Журналу учета аппаратных средств Министерства образования Пензенской области;

– обеспечивать смену паролей пользователей с периодичностью не реже 1 раза в 90 дней с момента очередной смены;

– изменять свой собственный пароль не реже 1 раза в месяц;

– принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов;

– сообщать ответственному за защиту информации в РИС ГИА об инцидентах, связанных с компрометацией или утерей паролей, аппаратных идентификаторов;

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

6.3. Действия администратора безопасности при компрометации паролей и утрате аппаратных идентификаторов:

– заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора к РИС ГИА;

– выявить действия, произведенные в РИС ГИА с использованием скомпрометированных персональных идентификаторов и паролей доступа;

– доложить ответственному за защиту информации в РИС ГИА об инциденте в соответствии с Порядком по выявлению инцидентов в РИС ГИА и реагированию на них»;

– создать и выдать пользователю новый персональный идентификатор и пароль (при необходимости аппаратный идентификатор) доступа к РИС ГИА.

6.4. Администратор безопасности в рамках проведения мероприятий по контролю (анализу) защищённости информации РИС ГИА осуществляет ежеквартально контроль создания, использования, изменения и прекращения действия учетных записей РИС ГИА. Ответственный за защиту информации в РИС ГИА координирует деятельность администратора безопасности.

7. Ответственность

7.1. Пользователи РИС ГИА должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

7.2. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции по идентификации и
аутентификации пользователей
РИС ГИА

ЖУРНАЛ

учета выдачи первичных паролей РИС ГИА

Учетный № _____

Журнал начат _____
Журнал окончен _____
Листов (_____)

Лист ___

№ п/п	Ф.И.О. сотрудника	Должность	Подразделение	Тип доступа	Первичный пароль	Дата выдачи/блокирования	Подпись	Примечание
1	2	3	4	5	6	7	8	9
1	[И.О. Фамилия пользователя]	[наименование должности пользователя]		Пользователь				
2	[И.О. Фамилия администратора безопасности]	[Должность администратора безопасности]		Администратор				
3								
4								
5								
6								
7								

Правила
по формированию и ведению
журнала учета выдачи первичных паролей
РИС ГИА

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается), подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне титульного листа указывается номер журнала по номенклатуре дел Министерства образования Пензенской области и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – Ф.И.О. сотрудника;
- Графа 3 – занимаемая должность в Министерстве образования Пензенской области;
- Графа 4 – подразделение Министерства образования Пензенской области;
- Графа 5 – тип доступа (пользователь или администратор);
- Графа 6 – пароль, назначаемый администратором безопасности;
- Графа 7 – дата выдачи или блокирования пароля;
- Графа 8 – подпись сотрудника (при выдаче) или администратора безопасности (при блокировании);
- Графа 9 – Примечание (любая информация, относящаяся к пользователю).

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 2
к Инструкции по идентификации и
аутентификации пользователей
РИС ГИА

Журнал
учета аппаратных средств аутентификации
Министерства образования Пензенской области

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№ п/п	Наименование устройства	Инвентарный номер	ИС	Дата периодического осмотра и подпись администратора безопасности	Отметка о выдаче			Отметка о возврате		Примечание
					Дата получения	ФИО, должность пользователя	Подпись пользователя за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10	11
1	*ESMART Token USB 64K Metal*	*инв. № 000011*	*«Наименование ИС»*	*01.01.2021 АБ [И.О. Фамилия администратора безопасности]*	*12.06.2021*	*И.О. Фамилия, должность ответственного за организацию обработки ПДн*		*30.12.2021*	*[И.О. Фамилия ответственного за организацию обработки ПДн]*	*Пример заполнения*
2										
3										
4										
5										
6										
7										
8										
9										
10										

Правила
по формированию и ведению
журнала учета аппаратных средств аутентификации
Министерства образования Пензенской области

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – наименование устройства;
- Графа 3 – инвентарный (серийный) номер устройства;
- Графа 4 – название ИС;
- Графа 5 – дата последнего осмотра и подпись администратора безопасности;
- Графа 6 – дата передачи пользователю;
- Графа 7 – Ф.И.О. сотрудника, занимаемая должность в Министерстве образования Пензенской области;
- Графа 8 – подпись сотрудника за получение устройства;
- Графа 9 – дата возврата сотрудником устройства администратору безопасности;
- Графа 10 – Ф.И.О. сотрудника, подпись за возврат устройства;
- Графа 10 – Примечание. Любая информация, относящаяся к записанному устройству.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 10
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция

по управлению доступом к государственной информационной системе Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по управлению доступом к РИС ГИА (далее – Инструкция) определяет в Министерстве образования Пензенской области порядок действий администратора безопасности РИС ГИА при разграничении доступа к ее ресурсам и информации.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные
СЗИ	Средства защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь. уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»,

Термин	Определение	Источник
		утвержден ФСТЭК России от 11.02.2014
Аутентификационная информация	Информация, используемая при аутентификации субъекта доступа или объекта доступа	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Идентификация	Присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Термин	Определение	Источник
Средство защиты информации	Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации	ГОСТ Р 50922-2006

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»;

- постановление Правительства РФ от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы с указанной государственной информационной системой. Обязанность по организации ознакомления с настоящей Инструкцией пользователей РИС ГИА возлагается на ответственного за защиту информации РИС ГИА.

2. Порядок предоставления допуска к обработке информации в РИС ГИА

2.1. Допуск сотрудников Министерства образования Пензенской области к обработке информации в РИС ГИА осуществляется в минимальном объеме, необходимом для выполнения их трудовых (служебных) обязанностей.

2.2. Министерства образования Пензенской области допускаются к обработке информации в РИС ГИА в соответствии с утвержденным перечнем перечень лиц, имеющих доступ к защищаемой информации (в том числе персональным данным) в РИС ГИА, содержащей сведения, не составляющие государственную тайну, который необходим для выполнения ими трудовых (служебных) обязанностей, Матрицей доступа к РИС ГИА и на основании служебной записки начальника структурного подразделения на имя министра образования Пензенской области.

2.3. Допуск сотрудников Министерства образования Пензенской области непосредственно к обработке информации в РИС ГИА предоставляется исключительно после прохождения инструктажа по вопросам обработки и защиты информации (в том числе персональных данных), содержащей сведения, не составляющие государственную тайну, при их обработке в государственной информационной системе Пензенской области.

3. Матрица доступа

3.1. Разграничение доступа к ресурсам и информации РИС ГИА осуществляет и контролирует администратор безопасности путем настройки программно–технических средств и средств защиты информации РИС ГИА на основании журналов учета выдачи первичных паролей и Матрицы доступа.

3.2. Предоставление доступа к информационным ресурсам РИС ГИА осуществляется в соответствии с приказом Министерства образования Пензенской области «О предоставлении пользователям доступа к информационным ресурсам РИС ГИА.

3.3. В Министерстве образования Пензенской области разработана и утверждена Матрица доступа к ресурсам РИС ГИА.

3.4. Сохранность, конфиденциальность и актуальность Матрицы доступа обеспечивает администратор безопасности.

4. Общий порядок предоставления доступа к РИС ГИА

4.1. Каждому лицу, имеющему доступ к РИС ГИА, присваивается учетная запись. Все действия, совершаемые с использованием учетной записи пользователя РИС ГИА, рассматриваются как совершаемые лично им.

Учетные записи пользователей РИС ГИА персонифицированы, то есть однозначно определяют своего владельца.

4.2. Заведение, активацию, блокирование и уничтожение учетных записей в РИС ГИА осуществляет администратор безопасности.

4.3. Управление учетными записями, реализация необходимых методов, типов и правил разграничения доступа осуществляется в соответствии с Матрицей доступа.

4.4. Гостевые учетные записи в РИС ГИА не используются.

4.5. Заведение учетных записей администраторов осуществляется в соответствии с утвержденными приказами Министерства образования Пензенской области и Матрицей доступа. Контроль использования учетных записей администраторов РИС ГИА осуществляется ответственным за защиту информации в РИС ГИА.

4.6. Администратор безопасности осуществляет настройку в РИС ГИА:

– блокирования учетной записи при превышении времени неиспользования более 90 дней;

– блокирования сеанса доступа в РИС ГИА после установленного времени бездействия (неактивности) пользователя 30 минут или по его запросу;

– в РИС ГИА на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы);

– блокирования учетной записи в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут (максимальное количество неуспешных попыток аутентификации до блокировки - 5).

4.7. Вход в РИС ГИА и действия с ресурсами РИС ГИА до процедур идентификации и аутентификации разрешен администратору безопасности для восстановления РИС ГИА после сбоев и аварий технических средств РИС ГИА. Срок действия разрешения заканчивается в момент запуска РИС ГИА после восстановления.

Доступ к ресурсам РИС ГИА до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4.8. При предоставлении прав доступа к РИС ГИА используются встроенные функции контроля доступа системного и прикладного программного обеспечения, требующие перед получением доступа обязательного прохождения аутентификации с минимально возможными требованиями использования механизмов аутентификации на основе учетной записи и пароля.

4.9. В случае утраты и (или) компрометации средств аутентификации пользователи РИС ГИА немедленно обязаны уведомить администратора безопасности, который незамедлительно предпринимает действия по блокированию учетной записи.

4.10. Управление информационными потоками обеспечивается разрешенным маршрутом прохождения информации между пользователями, устройствами в рамках РИС ГИА, а также между информационными системами или при взаимодействии с сетью Интернет. Управление информационными потоками блокирует передачу защищаемой информации через информационно-телекоммуникационную сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из РИС ГИА и (или) входящие в РИС ГИА.

4.11. Процедура предоставления удаленного доступа пользователей РИС ГИА (при наличии) осуществляется с порядком предоставления доступа, определенного в разделе 5 настоящей Инструкции.

4.12. Процедура использования мобильных технических средств (в случае использования) осуществляется в соответствии с порядком использования, определенного в разделе 6 настоящей Инструкции.

4.13. В РИС ГИА до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) осуществляется идентификация и аутентификация следующих типов устройств (технических средств), используемых в РИС ГИА:

– криптографические шлюзы (криптомаршрутизаторы);

– АРМ пользователей.

Идентификация устройств (технических средств) осуществляется по

физическим адресам (MAC-адресам) устройства и логическим именам (имя устройства).

5. Порядок предоставления удаленного доступа (при наличии)

Указанные в пункте 5 требования следует соблюдать только в случае, если Министерство образования Пензенской области использует или планирует использовать удаленный доступ (через сеть Интернет) к ресурсам РИС ГИА.

5.1. Удаленный доступ пользователей к информационным ресурсам РИС ГИА возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью Министерства образования Пензенской области и внесенных в Журнал разрешенных устройств удаленного доступа в Министерстве образования Пензенской области (Приложение №1 к настоящей Инструкции).

Ведение и надежное хранение Журнала разрешенных устройств удаленного доступа в Министерстве образования Пензенской области осуществляет администратор безопасности.

Срок хранения завершенного Журнала учета разрешенных устройств удаленного доступа в Министерстве образования Пензенской области определяется утвержденной номенклатурой Министерства образования Пензенской области.

Уничтожение Журнала учета разрешенных устройств удаленного доступа в Министерстве образования Пензенской области по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерства образования Пензенской области.

5.2. Выдачу, учет, хранение, настройку программного обеспечения, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор безопасности. Все данные по конфигурации и настройкам должны быть записаны в Журнал разрешенных устройств удаленного доступа в Министерстве образования Пензенской области.

5.3. При настройке средств удаленного доступа к ресурсам РИС ГИА администратор безопасности осуществляет возможность удаленного доступа к ресурсам РИС ГИА с автоматической аутентификацией средств удаленного доступа.

5.4. Контроль использования технических средств удаленного доступа к РИС ГИА возлагается на администратора безопасности.

5.5. При организации удаленного доступа к объектам доступа РИС ГИА администратором безопасности обеспечивается использование ограниченного (минимально необходимого) количества точек подключения к РИС ГИА.

5.6. Удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования РИС ГИА и ее системы защиты информации запрещается.

6. Порядок использования мобильных технических средств (в случае использования)

Указанные в пункте 6 требования следует соблюдать только в случае, если Министерство образования Пензенской области использует или планирует использовать мобильные технические средства для доступа к ресурсам РИС ГИА.

6.1. К мобильным техническим средствам Министерства образования Пензенской области отнесены все переносные технические устройства, на которые может быть записана и с помощью которых может быть осуществлена обработка информации, содержащейся в РИС ГИА.

6.2. В РИС ГИА администратором безопасности обеспечивается регламентация и контроль использования мобильных технических средств.

Регламентация и контроль использования мобильных технических средств включают:

- использование проводного вида доступа с использованием мобильных технических средств, входящих в состав РИС ГИА;
- использование в составе РИС ГИА мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с установленными требованиями ФСТЭК России;
- ограничение на использование мобильных технических средств в соответствии с функциями РИС ГИА, для решения использования таких средств, где это необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с общим порядком предоставления доступа;
- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам РИС ГИА;
- запрет возможности запуска без команды пользователя в РИС ГИА ПО, используемого для взаимодействия с мобильным техническим средством.

6.3. Все мобильные технические средства Министерства образования Пензенской области должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в Журнале учета разрешенных мобильных технических средств в Министерстве образования Пензенской области (Приложение №2 к настоящей Инструкции).

6.4. Ведение и надежное хранение журнала разрешенных устройств мобильных технических средств в Министерстве образования Пензенской области осуществляет администратор безопасности.

6.5. Срок хранения завершенного Журнала учета разрешенных мобильных технических средств в Министерстве образования Пензенской области определяется утвержденной номенклатурой Министерства образования Пензенской области.

6.6. Уничтожение Журнала учета разрешенных мобильных технических средств в Министерстве образования Пензенской области по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерства образования Пензенской области.

6.7. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор безопасности полностью очищает их от персональных

данных и информации, имеющей отношение к РИС ГИА, в соответствии с Инструкцией по защите машинных носителей информации в Министерстве образования Пензенской области.

6.8. Контроль использования мобильных технических средств для доступа к РИС ГИА возлагается на администратора безопасности.

7. Взаимодействие с внешними информационными системами

7.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам РИС ГИА устанавливают в Матрице доступа.

7.2. Администратор безопасности осуществляет процедуру доступа внешних пользователей к ресурсам РИС ГИА в соответствии с пунктом 4 настоящей Инструкции.

7.3. Управление взаимодействием с внешними информационными системами предусматривает:

- предоставление доступа к РИС ГИА только авторизованным (уполномоченным) пользователям;
- определение типов прикладного программного обеспечения информационной системы, к которым разрешён доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учётных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к РИС ГИА авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

7.4. Ответственным за защиту информации в РИС ГИА осуществляется контроль управления взаимодействия с внешними информационными системами.

8. Ответственность

8.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции по управлению доступом к РИС ГИА

Журнал
учета разрешенных средств удаленного доступа
к РИС ГИА

Учетный №_____

Журнал начат _____
Журнал окончен_____
Листов (_____)

№ п/п	Наименование	Инвентарный номер	Состояние	Отметка о выдаче			Отметка о возврате		Примечание
				Дата получения	ФИО, должность пользователя	Подпись пользователя за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*12.06.2021*	*И.О. Фамилия, должность ответственного за организацию обработки ПДн*	_____/	*30.10.2021*	_____ *(И.О. Фамилия ответственного за организацию обработки ПДн)*	*Пример заполнения*
2									
3									
4									
5									
6									
7									
8									
9									
10									

Лист _____

Правила

по формированию и ведению
журнала учета разрешенных средств удаленного доступа
в Министерстве образования Пензенской области

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне титульного лица указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – наименование оборудования или программного средства;
- Графа 3 – инвентарный или серийный номер;
- Графа 4 – указывается техническое состояние устройства.
- Графа 5 – дата передачи пользователю;
- Графа 6 – Ф.И.О. сотрудника, занимаемая должность в Министерстве образования Пензенской области;
- Графа 7 – подпись сотрудника за получение устройства (средства);
- Графа 8 – дата возврата сотрудником устройства администратору безопасности;
- Графа 9 – Ф.И.О. сотрудника, подпись за возврат устройства;
- Графа 10 – любая информация, относящаяся к записанному устройству или программному средству.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2
к Инструкции по управлению доступом к РИС ГИА

Журнал

учета разрешенных мобильных технических средств
в Министерстве образования Пензенской области

Учетный № _____ _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№ п/п	Наименование оборудования	Инвентарный номер	Состояние	Отметка о выдаче			Отметка о возврате		Примечание
				Дата получения	ФИО, должность пользователя	Подпись пользователя за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*12.06.2021*	*И.О. Фамилия, должность ответственного за организацию обработки ПДн*	_____	*30.10.2021*	_____ *И.О. Фамилия ответственного за организацию обработки ПДн*	*Пример заполнения*
2									
3									
4									
5									
6									
7									
8									
9									
10									

Лист _____

Правила
по формированию и ведению
журнала учета разрешенных мобильных технических средств
в Министерстве образования Пензенской области

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Все листы журнала, вместе с обложкой сшиваются.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне титульного листа указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

– Графа 1 – учетный порядковый номер записи;

– Графа 2 – наименование оборудования;

– Графа 3 – инвентарный или серийный номер;

– Графа 4 – указывается техническое состояние оборудования.

– Графа 5 – дата передачи пользователю;

– Графа 6 – Ф.И.О. сотрудника, занимаемая должность в Министерстве образования Пензенской области;

– Графа 7 – подпись сотрудника за получение устройства (средства);

– Графа 8 – дата возврата сотрудником оборудования администратору безопасности;

– Графа 9 – Ф.И.О. сотрудника, подпись за возврат устройства;

– Графа 10 – любая информация, относящаяся к записанному устройству или программному средству.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 11
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция
по защите машинных носителей информации
в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по защите машинных носителей информации в Министерстве образования Пензенской области (далее - Инструкция) определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей с защищаемой информацией (в том числе персональными данными), не содержащей сведения, составляющие государственную тайну (далее – машинные носители информации), используемых в Министерстве образования Пензенской области.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ФСБ	Федеральная служба безопасности
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
АРМ	Автоматизированное рабочее место
ГИС	Государственная информационная система
ИС	Информационная система
ПДн	Персональные данные
СВТ	Средства вычислительной техники
СКЗИ	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и	Методический документ ФСТЭК России «Меры защиты информации

Термин	Определение	Источник
	технических средств	в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Машинный носитель данных	Сменный носитель данных, предназначенный для записи и считывания данных, представленных в стандартных кодах	ГОСТ 25868-91
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде.	
Машинный носитель персональных данных	Машинный носитель информации, на которых хранятся и (или) обрабатываются персональные данные	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера. К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической

Термин	Определение	Источник
	- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	защиты информации»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСБ России от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных

информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»,

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

- приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

1.4. Сотрудники, допущенные к обработке информации, ограниченного доступа, не составляющей государственную тайну, в том числе персональных данных (далее – защищаемая информация), в связи с необходимостью выполнения ими трудовых (служебных) обязанностей в Министерстве образования Пензенской области (далее – сотрудники), должны быть ознакомлены с настоящей Инструкцией до начала обработки защищаемой информации под подпись. Обязанность по организации ознакомления сотрудников с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн, ответственного за защиту информации в ГИС.

2. Организация учета машинных носителей информации

2.1. Все используемые в Министерстве образования Пензенской области машинные носители информации подлежат регистрации и учету, а именно:

– несъёмные машинные носители (жесткие диски, находящиеся в системных блоках серверов, в том числе во внешних RAID-массивах серверов, и системных блоках АРМ ИС),

– съёмные машинные носители (флеш-память, SSd-диски, оптические носители информации и пр. технические средства, предназначенные для запоминания информации, и оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) либо считывания с них информации в память АРМ (или сервера)).

2.2. Применение в Министерстве образования Пензенской области незарегистрированных машинных носителей информации запрещается.

2.3. Приобретенные машинные носители информации перед использованием передаются администратору безопасности для регистрации.

2.4. Ответственным за регистрацию, хранение, выдачу машинных носителей информации, ведение учетной документации и контроль уничтожения машинных носителей информации в установленном порядке является администратор безопасности.

2.5. Обязанность организации процедуры уничтожения машинных носителей информации возлагается на ответственного за организацию обработки ПДн.

2.6. При смене администратора безопасности составляется акт приема-сдачи учетной документации и машинных носителей информации.

3. Порядок учета машинных носителей информации

3.1. Основной учет машинных носителей информации производится по Журналу учета машинных носителей информации в Министерстве образования Пензенской области (Приложение №1 к настоящей Инструкции).

Ведение и надежное хранение Журнала машинных носителей информации в Министерстве образования Пензенской области осуществляет администратор безопасности.

Срок хранения завершенного Журнала учета машинных носителей информации в Министерстве образования Пензенской области определяется утвержденной номенклатурой Министерства образования Пензенской области.

Уничтожение Журнала учета машинных носителей информации в Министерстве образования Пензенской области по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерстве образования Пензенской области.

3.2. Учет осуществляется с использованием регистрационных (заводских)/инвентарных номеров.

3.3. Учетный номер каждого зарегистрированного носителя – уникальный.

3.4. Учетный номер наносится на машинный носитель персональных данных способом, обеспечивающим сохранность маркировки в процессе эксплуатации носителя и не приводящим его в негодность:

– учетный номер оптического носителя информации наносится несмываемыми чернилами на его нерабочую поверхность и заверяется подписью администратора безопасности (на нерабочей стороне может указываться дополнительная информация, используемая в процессе применения);

– учетный номер жесткого диска наносится непосредственно на корпус носителя (при эксплуатации жесткого диска в составе СВТ, на корпус таких СВТ может наклеиваться этикетка с указанием количества и учетных номеров установленных в нем носителей информации);

– учетный номер флеш-памяти, ssd-дисков может наноситься посредством специальной наклейки, номер заверяется подписью администратора безопасности.

4. Выдача машинных носителей информации

4.1. Сотрудники получают учтенный машинный носитель информации от администратора безопасности для выполнения работ на конкретный срок.

4.2. Выдача машинных носителей информации сотрудниками производится по Журналу учета машинных носителей информации в Министерстве образования Пензенской области под подпись.

4.3. Выдача сотрудникам съёмных машинных носителей информации разрешается исключительно для реализации технологических процессов в ИС, ГИС необходимых для выполнения трудовых (служебных) обязанностей, и осуществляется с оформлением заявления на право использования съёмного машинного носителя информации по форме согласно Приложению №2 к настоящей Инструкции.

4.4. По завершении работ или установленного срока использования сотрудник сдает машинный носитель персональных данных администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации в Министерстве образования Пензенской области.

5. Использование и передача машинных носителей информации

5.1. На машинные носители информации записываются исключительно защищаемая информация и программные средства обработки информации. содержащиеся в ИС, ГИС.

5.2. Машинные носители персональных данных, допускающие повторную запись информации, при передаче между пользователями, в сторонние организации для ремонта или утилизации· проходят процедуру уничтожения (стирания) персональных данных с оформлением Акта об уничтожении персональных данных в соответствии с приказом Министерства образования Пензенской области «О комиссии по уничтожению персоналных данных в Министерстве образования Пензенской области» с целью уничтожения остаточной информации. Процедуру организует и контролирует администратор безопасности. Акт об уничтожении персональных данных хранится у ответственного за организацию обработки ПДн.

5.3. Ремонт машинных носителей информации, содержащих защищаемую информацию, сторонней организацией запрещен.

5.4. Защищаемая информация, используемая в различных целях, записывается на разные машинные носители информации.

5.5. Вынос машинных носителей информации за пределы установленных мест обработки допустим только с письменного разрешения министра образования Пензенской области.

5.6. Передача носителей, содержащих защищаемую информацию, которая обрабатывается в ИС, ГИС сторонним организациям или третьим лицам производится по приказу министра образования Пензенской области через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации в Министерстве образования Пензенской области.

6. Хранение машинных носителей информации

6.1. Хранение машинных носителей информации осуществляется в условиях, препятствующих несанкционированному ознакомлению, копированию, изменению или уничтожению защищаемой информации, содержащейся на машинных носителях.

6.2. Машинные носители информации хранятся в служебных помещениях, съёмные машинные носители информации - в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками.

В случае если на съёмном машинном носителе информации хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

6.3. Хранение машинных носителей информации осуществляется в условиях, исключающих утрату их функциональности и хранимой информации (оптические носители хранятся в конвертах или специальных коробках, обеспечивающих сохранность рабочей поверхности носителя от загрязнения и механических повреждений).

6.4. Порядок хранения машинных носителей информации, предназначенных к списанию (уничтожению), в том числе нечитаемых вследствие выхода из строя из-за неисправности (износа), не изменяется.

6.5. Ответственным за сохранность машинного носителя информации является пользователь ИС, ГИС, получивший машинный носитель информации в соответствии с разделом 4 настоящей Инструкции.

7. Действия при выходе из строя, порче или утрате машинных носителей информации

7.1. В случае выхода из строя, утраты или порчи пользователем машинного носителя информации немедленно ставится в известность администратор безопасности. Администратор безопасности докладывает об инциденте ответственному за организацию обработки ПДн ответственному за защиту информации в ГИС.

7.2. Факт выхода из строя машинного носителя информации устанавливается утвержденной приказом в Министерстве образования Пензенской области комиссией (в состав комиссии включается администратор безопасности, администратор ИС, ГИС и ответственный за организацию обработки персональных данных) с оформлением «Акта технической экспертизы состояния машинного носителя информации» (Приложение №3 к настоящей Инструкции), утверждаемого министром образования Пензенской области.

Неисправный носитель заменяется исправным, после чего администратором безопасности делаются соответствующие отметки в документах учета.

7.3. По факту утраты или порчи машинного носителя информации, несанкционированного и (или) нецелевого использования учтенных машинных носителей информации проводится служебная проверка в установленном порядке по решению министра образования Пензенской области.

Администратором безопасности делаются соответствующие отметки в документах учета.

7.4. Машинные носители информации, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

8. Уничтожение машинных носителей информации

8.1. Уничтожение машинных носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей в Министерстве образования Пензенской области.

8.2. Уничтожение машинных носителей информации производится в присутствии членов комиссии, утвержденной приказом Министерства образования Пензенской области «О комиссии по уничтожению персональных данных в Министерстве образования Пензенской области».

8.3. В случае уничтожение машинного носителя сторонней организацией факт уничтожения машинного носителя информации оформляется Актом, который находится на хранении у администратора безопасности.

8.4. Утилизация лома уничтоженных носителей производится в соответствии с правилами уничтожения СВТ.

9. Контроль применения машинных носителей информации

9.1. Контроль наличия машинных носителей информации, правил и условий их хранения осуществляется посредством периодических проверок утвержденной приказом Министерства образования Пензенской области комиссией (в состав комиссии включаются ответственный за организацию обработки персональных данных и администратор безопасности). Результаты проверки наличия машинных носителей информации оформляются актом проверки наличия и состояния машинных носителей информации» по форме, установленной Приложение №4 к настоящей Инструкцией).

9.2. Проверке подлежат: соответствие количества учтенных носителей фактическому, наличие и состояние учетной документации, соответствие серийных (заводских) и учетных номеров, условия хранения и использования носителей.

9.3. Акт проверки хранится у администратора безопасности.

10. Ответственность

10.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией в соответствии с законодательством Российской Федерации.

Приложение № 1
к Инструкции по защите машинных носителей информации
в Министерстве образования Пензенской области

Журнал
учета машинных носителей информации
в Министерстве образования Пензенской области

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№ п/п	Учетный (инвентарный) номер	Дата постановки на учет	Наименование, модель, емкость носителя	Заводской (серийный) номер	Тип носителя (съемный /несъемный)	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения носителя и подпись	Дата возврата носителя и подпись администратора	Отметка об уничтожении носителя	Примечание
1	2	3	4	5	6	7	8	9	10	11	12
1	*инв. № 1000613*	*11.01.2021*	*USB flash drive Transcend JF 130 2Gb*	*SIGB77NBH B3F AC1X0*	*Съемный*	*нет*	*[И.О. Фамилия ответственного за организацию обработки ПДн]*	*01.01.2021 [И.О. Фамилия ответственного за организацию обработки ПДн]*	*12.06.2021 [И.О. Фамилия администратора безопасности]*	*уничтожен 20.06.2021*	

Лист ______

Правила
по формированию и ведению
журнала учета машинных носителей информации
в Министерстве образования Пензенской области

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением листов титульного), нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – учетный (инвентарный) номер носителя;
- Графа 3 – дата постановки на учет;
- Графа 4 – наименование, модель, емкость носителя;
- Графа 5 – заводской (серийный) номер носителя;
- Графа 6 – указывается тип носителя (съемный, несъёмный);
- Графа 7 – для несъемных носителей указывается АРМ пользователя.
- Графа 8 – Ф.И.О. сотрудника
- Графа 9 – дата получения носителя и подпись пользователя;
- Графа 10 – дата возврата носителя и подпись администратора безопасности;
- Графа 11 – отметку делает администратор безопасности после уничтожения носителя;
- Графа 12 – любая информация, относящаяся к носителю.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2
к Инструкции по защите машинных носителей информации
в Министерстве образования Пензенской области

Разрешаю
Министр образования Пензенской области
_____/_____/
«___» _____ 20__ г.

Заявление
на право использования съёмного машинного носителя информации

Прошу разрешить для выполнения трудовых (служебных) обязанностей использование и подключение к АРМ (инв. № _____) съёмного машинного носителя информации:

Должность	
ФИО полностью	
Цель использования в соответствии с должностными обязанностями	
Технологический процесс, для реализации которого необходимо использование машинного носителя информации	

Я предупрежден(а), что записывать, хранить на съёмных машинных носителях информации информацию ограниченного доступа допускается исключительно для реализации технологических процессов (регламентов, порядков работы и т.п.), необходимых для выполнения трудовых (служебных) обязанностей.

Подпись _____/_____/

Дата _____

Согласовано:

Руководитель структурного подразделения _____/_____/

Выдан съёмный машинный носитель информации:

Учетный (регистрационный) № _____

Администратор безопасности _____/_____/

Приложение № 3
к Инструкции по защите машинных носителей информации
в Министерстве образования Пензенской области

Утверждаю
Министр образования Пензенской области
_____/_____/
«___» _____ 20__ г.

Акт № _____

технической экспертизы

состояния машинного носителя информации

г. _____ «____» _____ ____г.

Комиссия в составе:

Председатель комиссии: _____
(должность, ФИО)

Члены комиссии: _____
(должность, ФИО)

_____
(должность, ФИО)

на основании _____
(приказ о назначении комиссии)

произвела наружный осмотр и контроль, сверила с данными регистрационного учета следующие носители информации:

№ п/п	Учетный (инвентарный) номер носителя	Наименование, модель, емкость носителя	Серийный (заводской) номер носителя	Место установки	Неисправность

в количестве _____.
(количество цифрами и прописью)

В результате осмотра и контроля комиссия установила:

_____
(проявление неисправности, метод определения неработоспособности носителя информации)

_____
(возможность дальнейшего использования носителя информации, подлежит/не подлежит ремонту)

Характер записанной информации конфиденциальный, поэтому передача его в ремонт сторонней организации невозможна.

Заключение комиссии:

_____

(носитель информации подлежит /не подлежит утилизации)

Председатель комиссии:

_____	_____	_____
(должность)	(подпись)	(ФИО)

Члены комиссии:

_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)

Приложение № 4
к Инструкции по защите машинных носителей информации
в Министерстве образования Пензенской области

Утверждаю
Министр образования Пензенской области
_____/_____/
«___» _____ 20__ г.

Акт № _____
проверки наличия и состояния
машинных носителей информации

г. _____ «____» _____ ____г.

Комиссия в составе:
Председатель комиссии: _____
(должность, ФИО)
Члены комиссии: _____
(должность, ФИО)
_____
(должность, ФИО)

на основании _____
(приказ о назначении комиссии)
провела проверку наличия и состояния машинных носителей информации в Министерстве образования Пензенской области.

Для проверки представлена следующая документация:
- Журнал учета носителей информации в Министерстве образования Пензенской области.

В соответствии с учетной документацией в Министерстве образования Пензенской области числится:

1. Оптические диски в количестве ____ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

2. Флеш – накопители в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

3. Накопители на жестких дисках в количестве ___ штук:

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

№ п/п	Тип носителя	Учетный (инвентарный) номер	Примечание

В ходе проверки выявлено:

_____

(соответствие/ не соответствие учетных носителей информации фактически представленному)

Заключение комиссии:

_____

(носители информации находятся в исправном/ неисправном состоянии, условия хранения и использования машинных носителей информации соответствуют/ не соответствуют требованиям Инструкции по защите машинных носителей информации в Министерстве образования Пензенской области

Председатель комиссии:

_____ _____ _____

(должность) (подпись) (ФИО)

Члены комиссии:

_____ _____ _____

(должность) (подпись) (ФИО)

_____ _____ _____

(должность) (подпись) (ФИО)

Приложение № 12
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция

по управлению событиями информационной безопасности государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»
(РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по управлению событиями информационной безопасности РИС ГИА (далее – Инструкция) определяет в Министерстве образования Пензенской области перечень событий информационной безопасности, подлежащих регистрации и сроки их хранения, состав и содержание информации о событиях безопасности, подлежащих регистрации, порядок сбора, записи и хранения информации о событиях информационной безопасности в течение определенного времени хранения, а также порядок защиты информации о событиях информационной безопасности РИС ГИА.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система
ПДн	Персональные данные
Событие ИБ	Событие информационной безопасности

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и	Методический документ ФСТЭК

Термин	Определение	Источник
	обеспечивающих ее обработку информационных технологий и технических средств	России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Событие информационной безопасности	Идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Администратор безопасности РИС ГИА и администратор РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления вышеуказанных сотрудников с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Перечень событий информационной безопасности, подлежащих регистрации, и сроки их хранения

2.1. К регистрируемым событиям ИБ относятся события:

– события ИБ, имеющие отношение к возможности реализации угроз безопасности информации (в том числе ПДн), обрабатываемой в РИС ГИА, описанных в Модели угроз безопасности информации РИС ГИА;

– события ИБ, регистрируемые в журналах операционных систем технических средств РИС ГИА и средств защиты информации;

– организационно-технические события информационной безопасности в инфраструктуре РИС ГИА.

2.2. Автоматически определяемые события ИБ регистрируются автоматически в электронных журналах сообщений программных средств РИС ГИА и средств защиты информации и хранятся в течение времени не менее 1 месяца со дня регистрации события ИБ.

2.3. События ИБ, не определяемые автоматически, регистрируются в журнале событий информационной безопасности РИС ГИА по форме, установленной Приложением №1 к настоящей Инструкции.

Ведение и надежное хранение журнала событий информационной безопасности РИС ГИА осуществляет администратор безопасности.

Срок хранения завершенного журнала событий информационной безопасности в РИС ГИА определяется утвержденной номенклатурой Министерства образования Пензенской области.

Уничтожение журнала событий информационной безопасности РИС ГИА по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Министерстве образования Пензенской области.

2.4. Перечень событий безопасности, не определяемых автоматически и которые необходимо регистрировать при их возникновении, приведен в Перечне регистрируемых событий информационной безопасности РИС ГИА (Приложение №2 к настоящей Инструкции).

3. Состав и содержание информации о событиях информационной безопасности, подлежащих регистрации

3.1. Состав и содержание информации по каждому событию ИБ должны идентифицировать тип события, источник события ИБ, дату, время и результат события, а также пользователя РИС ГИА, связанного с данным событием.

4. Порядок сбора, записи и хранения событий информационной безопасности

4.1. Настройку электронных журналов регистрации событий ИБ в программном обеспечении РИС ГИА и средств защиты информации осуществляет администратор РИС ГИА и администратор безопасности каждый в своей части. Настройка осуществляется в соответствии с эксплуатационной документацией на программно–технические средства РИС ГИА.

4.2. Администраторы РИС ГИА и администратор безопасности должны с периодичностью не реже 1 раза в неделю просматривать журналы регистрации событий безопасности РИС ГИА.

4.3. Настройки электронных журналов регистрации событий ИБ должны обеспечивать запись в память технических средств РИС ГИА и средств защиты информации сведения о поступающих событиях безопасности без переполнения памяти в течение 1 месяца с момента регистрации события ИБ.

4.4. Информация о событиях безопасности в РИС ГИА, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового характера) должна фиксироваться администратором безопасности при ее обнаружении в журнале событий информационной безопасности РИС ГИА.

4.5. В РИС ГИА осуществляется реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

4.6. Реагирование на сбои при регистрации событий безопасности предусматривает:

- предупреждение (сигнализация, индикация) администратора безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения администратором безопасности параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов РИС ГИА, запись поверх устаревших хранимых записей событий безопасности.

4.7. В случае обнаружения установления факта и/или компьютерного инцидента неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, администратор безопасности обязан немедленно сообщить о таком факте

ответственному за организацию обработки персональных данных в Министерстве образования Пензенской области, который принимает меры в соответствии с Инструкцией о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в Министерстве образования Пензенской области.

5. Защита информации о событиях информационной безопасности

5.1. Права доступа к файлам отчетов электронных журналов безопасности и настройкам журналов установлены администратору безопасности и администратором РИС ГИА в части касающейся в соответствии с Матрицей доступа.

5.2. Доступ к электронным журналам безопасности РИС ГИА пользователям РИС ГИА запрещен.

5.3. Ответственность за сохранность журнала событий информационной безопасности, заполняемого по форме Приложения №1 к настоящей Инструкции, и за конфиденциальность заносимой в него информации несет администратор безопасности.

6. Ответственность

6.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции по управлению событиями
информационной безопасности РИС ГИА

Журнал
событий информационной безопасности
РИС ГИА

Учетный № _____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№	Код события (в соответствии с перечнем регистрируемых событий ИБ)	Место события ИБ	Участники события ИБ, источник события ИБ	Дата и время события ИБ	ФИО пользователя	Результат события ИБ	Подпись администратора безопасности
1	2	3	4	5	6	7	8
1	*006*	*АРМ №1*	*[И.О. Фамилия ответственного за занесну информации в ГИС «РИС ГИА»] [И.О. Фамилия администратора безопасности] И.И. Иванов*	*обнаружено 01.01.2021, 11:45*	*Петров Сергей Геннадьевич*	*Пользователь заблокирован*	*[И.О. Фамилия администратора безопасности]*

Правила

по формированию и ведению

журнала событий информационной безопасности

РИС ГИА

1. Формирование журнала

Журнал ведется на бумажных носителях (формируется из листов формата А4, ориентация листа - альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны министром образования Пензенской области с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – код события из перечня регистрируемых событий;
- Графа 3 – указывается название рабочего места пользователя;
- Графа 4 – указываются участники события и источник события ИБ;
- Графа 5 – дата и время события ИБ;
- Графа 6 – Ф.И.О. пользователя;
- Графа 7 – результат события ИБ;
- Графа 8 – подпись администратора безопасности.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется несколько строк.

Приложение № 2
к Инструкции по управлению событиями
информационной безопасности РИС ГИА

Перечень
регистрируемых событий информационной безопасности РИС ГИА

№ группы	Группа	Код события	Событие
1	Идентификация и аутентификация пользователей и устройств	001	Устаревший пароль (не соблюдены требования к срокам обновления пароля)
		002	Скомпрометированный пароль (пароль пользователя известен другому лицу)
		003	Утеря пароля (блокировка входа после неверного пятикратного входа)
		004	Пользователь не внесен в журнал выдачи первичных паролей
		005	Нет отметки в журнале выдачи первичных паролей отметки о блокировании доступа уволенному сотруднику.
		006	Пароль пользователя не соответствует требованиям
		007	Бездействие пользователя более установленного времени (блокировка доступа по истечению установленного интервала)
		008	Утеря аппаратного средства аутентификации.
		009	Порча аппаратного средства аутентификации
		010	
2	Машинные носители информации	011	Отсутствует учетный номер на МНИ и запись в журнале учета
		012	Превышение срока пользования учтенным МНИ
		013	Запись на учтенный МНИ иной информации вместе с ПДн
		014	Несанкционированный вынос МНИ из зоны обработки защищаемой информации
		015	Несанкционированная передача МНИ другому пользователю
		016	Хранение МНИ на рабочем столе пользователя
		017	МНИ, оставленный без присмотра
		018	

		019	
		020	
3	Вирусы	021	Вирусная атака (заражение)
		022	Истек срок лицензии на антивирусное ПО и ПО не обновлено
		023	Сбои (нарушения в работе) антивирусного ПО
		024	
		025	
4	Контролируемая зона	026	Вынос учтенного оборудования ИС за границы контролируемой зоны
		027	Внутри контролируемой зоны неучтенные МНИ или неучтенные технические средства чтения и записи информации.
		028	Экран монитора виден со стороны двери или окон в контролируемом помещении
		029	В помещении контролируемой зоны отсутствуют сотрудники, помещение не заперто.
		030	В помещении контролируемой зоны без сопровождения присутствует сотрудник, не имеющий допуска к обработке защищаемой информации.
		031	
		032	
		033	
		034	
		035	
5	СКЗИ	036	Компрометация СКЗИ (ключевая информация известна другому пользователю)
		037	Утеря СКЗИ или ключевой информации.
		038	Информация в журнале учета СКЗИ неактуальна (не обновлена)
		039	Нахождение инсталлирующих носителей, ЭД и ТД на СКЗИ в неположенном месте
		040	Действующие и резервные ключевые документы хранятся нераздельно
		041	Отсутствие или нарушение опломбирования оборудования с СКЗИ
		042	
		043	
		044	
		045	

Приложение № 13
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-07

Инструкция
по антивирусной защите государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по антивирусной защите РИС ГИА(далее - Инструкция) определяет в Министерстве образования Пензенской областипорядок организации антивирусной защиты, порядок действий администратора безопасности и пользователей РИС ГИАпри обнаружении вредоносных компьютерных программ (вирусов).

1.2. Сокращения, термины и определения

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Антивирусное ПО	Программное обеспечение средств антивирусной защиты
Вредоносное ПО	Вредоносная компьютерная программа (вирус)
АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
ПО	Программное обеспечение
СВТ	Средства вычислительной техники

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы	ГОСТ Р 51275-2006

Термин	Определение	Источник
	информационной системы	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Машинный носитель информации	Материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных (далее – ПДн)) в электронном виде.	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Пользователи РИС ГИАдолжны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИАпод подпись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Общий порядок организации антивирусной защиты

2.1. Антивирусное ПО устанавливается на все СВТ, входящие в состав РИС ГИАдля предотвращения заражения вредоносными компьютерными программами (вирусами) (далее – вредоносным ПО) через съемные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сервисы) и информационного обмена (Интернет).

2.2. К использованию в РИС ГИАдопускаются только лицензионные средства антивирусной защиты, прошедшие в установленном порядке процедуру сертификации средств защиты информации по требованиям безопасности информации.

2.3. На все применяемые в РИС ГИАсредства антивирусной защиты должны быть документы, подтверждающие права Министерства образования Пензенской области на их использование и действующие сертификаты ФСТЭК России.

2.4. Ответственный за защиту информации в РИС ГИАобеспечивает организацию антивирусной защиты РИС ГИА.

2.5. Администратор безопасности осуществляет установку, конфигурирование и управление средствами антивирусной защиты РИС ГИАв соответствии с эксплуатационной документацией на антивирусное ПО, а также надежное хранение эталонных копий антивирусного ПО.

2.6. Пользователи РИС ГИАявляются ответственными за ежедневный контроль на своих АРМ и своевременное информирование администратора безопасности в случае обнаружения вредоносного ПО или при появлении иных предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.).

2.7. Контроль над работой пользователя РИС ГИАпо применению на непосредственных АРМ средств антивирусной защиты осуществляет администратор безопасности.

3. Реализация антивирусной защиты

3.1.Антивирусное ПО должно запускаться автоматически при старте операционной системы СВТ РИС ГИАи функционировать до завершения работы операционной системы.

3.2. Пользователям РИС ГИАзапрещается блокировать, изменять настройки и выгружать антивирусное ПО на своих АРМ.

3.3 Антивирусная проверка должна осуществляться для следующих объектов:

- файлов загрузки – при загрузке операционной системы;

– системного и прикладного программного обеспечения, исполняемых файлов – в автоматическом режиме в период сеанса работы;

– поступающей информации по каналам передачи данных – в автоматическим режиме до открытия информации (запуска исполняемых файлов);

– информации, поступающей на съемных носителях – при подключении съемного носителя к техническому средству;

– исходящей информации – непосредственно перед ее отправкой (записью на съемный носитель);

– устанавливаемого (изменяемого) программного обеспечения – непосредственно перед установкой;

– машинных носителях информации, установленных в корпус СВТ (накопители на жестких дисках) – не реже одного раза в неделю.

3.4. Любое устанавливаемое (обновляемое) программное обеспечение в РИС ГИАпроверяется на отсутствие вредоносного ПО до момента установки. После установки или обновления программного обеспечения проводится повторная антивирусная проверка.

3.5. Администратор безопасности при управлении средствами антивирусной защиты РИС ГИАобеспечивает:

– установку, настройку, управление конфигурацией и логической структурой всего антивирусного ПО;

– установку и обновление лицензионных ключей средств антивирусной защиты;

– установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);

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

– настройку рассылки сообщений об обнаружении вредоносного ПО, о сбоях в работе средств антивирусной защиты, о необходимости обновления базы данных признаков вредоносных компьютерных программ (вирусов) и т.п.;

– внеплановую проверку АРМ, съемных машинных носителей информации в случае подозрения на наличие вредоносного ПО;

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

– решение проблем, возникающих в процессе использования средств антивирусной защиты.

3.6. Администратор безопасности осуществляет настройку регистрации событий информационной безопасности средств антивирусной защиты РИС ГИА, включая:

– отказ работоспособности средств антивирусной защиты и их компонентов;

– обнаружение вредоносного ПО;

– изменение любых текущих настроек средств антивирусной защиты;

– установку и распространение обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

Журналы регистрации событий средства антивирусной защиты РИС ГИАдолжны быть доступны для оперативного анализа в течение 1 месяца с момента регистрации события.

4. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

4.1. Базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты РИС ГИАавтоматически обновляются на ежедневной основе из доверенных источников.

4.2. Администратор безопасности не реже 1 раза в день проводит контроль обновления баз данных признаков вредоносных компьютерных программ (вирусов).

5. Порядок действий при обнаружении вредоносного программного обеспечения

5.1. При обнаружении вредоносного ПО на съемных носителях, в электронных отправлениях или при посещении ресурсов сети Интернет пользовательРИС ГИАобязан:

– приостановить работу с источником угрозы (съемным носителем, электронным отправлением, Интернет-ресурсом), иные работы на автоматизированном рабочем месте не запрещаются;

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, рекомендованные администратором безопасности.

5.2. При обнаружении вредоносного ПО в процессе обработки информации, за исключением пункта 3.1, пользователь обязан:

– приостановить все работы на АРМ;

– сообщить администратору безопасности об обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, рекомендованные администратором безопасности.

5.3. Администратор безопасности по факту событий, предусмотренных пунктами 5.1, 5.2 должен зарегистрировать вирусную атаку в журнале событий безопасности в соответствии с Инструкцией по управлению событиями информационной безопасности РИС ГИА.

5.4. При обнаружении вредоносного ПО на серверном или телекоммуникационном оборудовании администратор безопасности обязан:

– немедленно сообщить ответственному за защиту информации в РИС ГИАоб обнаружении вредоносного программного обеспечения;

– принять меры по локализации и удалению вредоносного ПО, а также по выявлению источника и способа проникновения вредоносного ПО.

5.5. В случае невозможности удаления вредоносного ПО, администратору безопасности следует обратиться в организацию, осуществляющую техническую поддержку средств антивирусной защиты. При передаче образцов зараженных файлов, а также при предоставлении информации о вирусной атаке в организацию, осуществляющую техническую поддержку средств антивирусной защиты информации, должны быть соблюдены требования конфиденциальности обрабатываемой информации в РИС ГИА.

6. Обязанности пользователей РИС ГИА

6.1. При работе в РИС ГИАпользователи обязаны:

– вести ежедневный контроль над работой средств антивирусной защиты;

– проверять вложения электронной почты, съёмные машинные носители информации перед началом работы на предмет наличия вредоносного ПО;

– немедленно уведомлять администратора безопасности при подозрении на заражение АРМ вредоносным ПО (медленная работа при открытии приложений, частое зависание ПО, самопроизвольный перезапуск, сбои в работе), при обнаружении вредоносного ПО (сообщение на экране монитора о наличии вируса), а также при появлении любых предупреждающих сообщений средств антивирусной защиты (истечения срока лицензии, о неактуальности базы данных признаков вредоносных программ (вирусов) и т.п.);

6.2. Пользователям РИС ГИАзапрещается:

– отключать, изменять настройки и выгружать антивирусное ПО на своих АРМ.

– самостоятельно осуществлять подключение (отключение) АРМ к локальной вычислительной сети, устанавливать (удалять) ПО, оборудование;

– использовать незарегистрированные в Министерстве образования Пензенской области машинные носители информации;

– продолжать обработку защищаемой информации (в том числе персональных данных) и иные работы при обнаружении вредоносного ПО в процессе обработки информации.

7. Ответственность

7.1. Пользователи РИС ГИА должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции.

7.2. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 14
Утверждено
приказом Министерства образования
Пензенской области

от 26.01.2026 № 99/01-

Инструкция

по контролю (анализу) защищенности 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»
(РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по контролю (анализу) защищенности информации РИС ГИА (далее - Инструкция) определяет в Министерстве образования Пензенской области порядок выявления (поиска), анализа и устранения уязвимостей информационной системы, недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков, а также порядок действий администратора безопасности и администраторов РИС ГИА при контроле защищенности информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), обрабатываемой в РИС ГИА.

1.2. Сокращения, термины, определения

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система Пензенской области
ПДн	Персональные данные
ПО	Программное обеспечение
СЗИ	Средства защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия	Методический документ ФСТЭК

Термин	Определение	Источник
	(имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Уязвимость	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.3. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Выявление анализ и устранение уязвимостей РИС ГИА

2.1. С целью предотвращения реализации угроз безопасности осуществляется выявление (поиск), анализ и устранение уязвимостей РИС ГИА.

2.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей РИС ГИА составляет не реже одного раза в год.

Внеплановые процедуры выявления, анализа и устранения уязвимостей РИС ГИА проводятся по распоряжению ответственного за защиту информации в РИС ГИА в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет ответственный защиту информации в РИС ГИА на основе анализа журналов событий безопасности.

2.3. В РИС ГИА должно осуществляться выявление и устранение следующих типов уязвимостей:

– недостатки и (или) ошибки кода в ПО (общесистемном, прикладном. специальном) РИС ГИА и ПО ее системы защиты информации;

– недостатки аппаратных средств РИС ГИА, в том числе аппаратных средств защиты информации;

– организационно-технические недостатки.

2.4. Мероприятия по выявлению, анализу и устранению уязвимостей организует ответственный за защиту информации в РИС ГИА.

План устранения выявленных уязвимостей разрабатывает администратор безопасности.

2.5. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального ПО, технических средств, а также другие базы данных уязвимостей (опубликованные в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средств и ПО).

2.6. В РИС ГИА администратором безопасности обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования РИС ГИА на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

2.7. Функции выявления (поиска) уязвимостей с использованием сканера безопасности в РИС ГИА осуществляется только администратором безопасности).

3. Недостатки программного обеспечения

3.1. Мероприятия по выявлению и анализу недостатков программного обеспечения РИС ГИА включают в себя выполнение следующих проверок:

– проверка конфигурации и настроек программно – технических средств РИС ГИА и системы защиты информации на соответствие требованиям эксплуатационной документации и требований к защите ПДн;

– проверка наличия и сроков действия лицензий на установленное программное обеспечение РИС ГИА;

– проверка наличия последних обновлений используемого программного обеспечения РИС ГИА и системы защиты информации:

– проверка соответствия обновлений версиям программного обеспечения, установленного в РИС ГИА и системе защиты информации;

– проверка обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты;

– проверка обновлений баз сигнатур уязвимостей средств контроля (анализа) защищенности.

3.2. Проверочные мероприятия, указанные в пункте 3.1, и устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор безопасности и администраторы РИС ГИА.

3.3. Все устанавливаемые обновления ПО РИС ГИА и ПО системы защиты информации должны быть предварительно проверены на работоспособность, а также на отсутствие вредоносного кода в соответствии с Инструкцией по антивирусной защите РИС ГИА.

3.4. После установки обновления программного обеспечения администратор РИС ГИА и администратор безопасности каждый в своей части выполняют необходимые настройки, проводят тестирование работоспособности и вносят соответствующие изменения в эксплуатационную документацию (формуляр или паспорт) и Технический паспорт на РИС ГИА.

3.5. Мониторинг наличия обновлений, выпускаемыми разработчиками для всего используемого в РИС ГИА программного обеспечения осуществляют не реже 1 раза в неделю администратор безопасности и администратор РИС ГИА.

4. Недостатки аппаратных средств

4.1. К недостаткам аппаратных средств, используемых в РИС ГИА, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

4.2. При выявлении недостатков аппаратных средств проверяют:

- техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств РИС ГИА за период контроля защищенности РИС ГИА;
- наличие сертификатов соответствия на примененные в РИС ГИА и ее системе защиты информации аппаратные средства;
- наличие у поставщиков обновленных версий аппаратных средств, примененных в РИС ГИА и системе защиты информации;
- перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;
- конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

4.3. Проверочные мероприятия, указанные в пункте 4.2. настоящей Инструкции, осуществляет администратор безопасности с привлечением администратора РИС ГИА.

4.4. Проверка конфигурации РИС ГИА и ее системы защиты информации осуществляется в соответствии с Порядком по управлению изменениями в конфигурации РИС ГИА, утвержденным приказом Министерства образования Пензенской области.

4.5. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор безопасности принимает меры по ремонту или замене этих аппаратных средств.

5. Контроль установки обновлений программного обеспечения

5.1. Контроль установки обновлений ежеквартально проводит администратор безопасности.

5.2. Получение обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода осуществляется из доверенных источников.

5.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного обеспечения, включая программное обеспечение средств защиты информации, установленное в РИС ГИА и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке обновлений и в Техническом паспорте РИС ГИА в соответствии с Порядком по управлению изменениями в конфигурации РИС ГИА.

5.4. При обновлении программного обеспечения средств защиты информации аттестованной информационной системы – отправляется уведомление в орган по аттестации.

5.5. При контроле обновлений системы защиты информации осуществляется проверка версий:

– баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты;

– баз сигнатур уязвимостей средства контроля (анализа) защищенности.

5.6. При получении информации о прекращении поддержки разработчиком используемого ПО в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки администратор безопасности и администратор РИС ГИА незамедлительно сообщают ответственному за защиту информации в соответствии с Порядком по управлению изменениями в конфигурации РИС ГИА.

6. Организационно – технические недостатки

6.1. Мероприятия по выявлению, анализу и устранению организационно-технических недостатков включают в себя выполнение следующих проверок:

– проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по обеспечению безопасности защищаемой информации;

– проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД);

– проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям;

– проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям;

– проверка соответствия выполнения правил разграничения доступа к защищаемой информации и ресурсам РИС ГИА принятым требованиям;

– проверка соответствия полномочий пользователей принятым требованиям;

– проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;

– проверка состояния физической защиты РИС ГИА (средства охраны и физического доступа в контролируемых зонах РИС ГИА);

– проверка знания и соблюдения пользователями РИС ГИА основных нормативно-правовых актов в области обеспечения безопасности защищаемой информации и требований ОРД;

6.2. Проверки организует ответственный защиту информации в РИС ГИА с участием администратор безопасности.

7. Контроль создания, использования, изменения и прекращения действия учетных записей РИС ГИА

7.1. Администратор безопасности осуществляет ежеквартально контроль создания, использования, изменения и прекращения действия учетных записей РИС ГИА.

7.2. Ответственный за защиту информации координирует деятельность администратора безопасности.

7.3. Ежеквартальный контроль оформляется в виде Отчета о несоответствиях в выдаче прав доступа к РИС ГИА (далее - Отчет) (Приложение), подписывается администратором безопасности и утверждается ответственным за защиту информации.

7.4. Отчет передаётся ответственному за защиту информации.

8. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

8.1. Администраторам безопасности и администратором в части касающейся осуществляется периодический контроль конфигурации и настроек программно – технических средств РИС ГИА и средств защиты информации на соответствие требованиям эксплуатационной документации и требований к обеспечению безопасности защищаемой информации, в том числе:

– работоспособности (неотключения) ПО и средств защиты информации в РИС ГИА (ежедневно);

– правильности функционирования ПО и средств защиты информации в РИС ГИА (ежедневно);

– соответствия настроек ПО и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на РИС ГИА (ежеквартально).

8.2. В случае выявления сбоев, отказов или несоответствия настройкам проводится восстановление ПО и СЗИ.

Восстановление производится с использованием резервных копий и (или) дистрибутивов.

8.3. Запрещается осуществлять обработку защищаемой информации в случае обнаружения неисправностей в системе защиты информации РИС ГИА.

9. Контроль состава технических средств, программного обеспечения и средств защиты информации

9.1. Контроль состава технических средств, ПО и средств защиты информации в РИС ГИА осуществляется с целью поддержания актуальной конфигурации программно-технических средств РИС ГИА.

9.2. Администратором безопасности не реже 1 раза в полгода проводится контроль на соответствие Техническому паспорту РИС ГИА, составленному по итогам аттестации РИС ГИА, состава технических средств, ПО и средств защиты информации.

9.3. Администратором безопасности не реже 1 раза в полгода проводится контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков.

9.4. Проверка действующей конфигурации программного обеспечения и состава технических средств РИС ГИА эксплуатационной документации проводится в соответствии с Порядком по управлению изменениями в конфигурации РИС ГИА.

9.5. К установке в РИС ГИА допускается следующее программное обеспечение.

- прикладное программное обеспечение;
- общесистемное программное обеспечение,
- иное ПО, содержащееся в Техническом паспорте РИС ГИА[1].

9.6. Перечень разрешенного к установке ПО СЗИ определяется Техническим паспортом РИС ГИА.

9.7. К установке в РИС ГИА запрещено следующее ПО:

- вредоносное программное обеспечение;
- программное обеспечение для майнинга криптовалюты;
- программное обеспечение для несанкционированного создания VPN;
- ПО для работы с торрент-сетями.

9.8. Администратором безопасности обеспечивается не реже 1 раза в полгода осуществляется контроль установленного (инсталлированного) программного обеспечения в РИС ГИА на предмет соответствия его перечню программного обеспечения. разрешенному к установке, а также на предмет отсутствия программного обеспечения, запрещенного в Министерстве образования Пензенской области.

10. Ответственность

10.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

---

[1] Кроме вышеуказанного программного обеспечения, разрешенного к установке в ГИС «РИС ГИА», также относится системное программное обеспечение, прикладное и специальное программное обеспечение, идущее в составе с системным программным обеспечением, драйверы используемых устройств и компоненты, вспомогательные компоненты, необходимые для нормального функционирования используемого программного обеспечения и средств защиты информации РИС ГИА

Приложение
к Инструкции по контролю (анализу) защищенности
информации РИС ГИА

Отчет
о несоответствиях в выдаче прав доступа к РИС ГИА

№ п/п	Имя учетной записи	Выявленное несоответствие	Принятые меры (блокировка, изменение прав и т.д.)	Примечание

Администратор безопасности _____ *(Ф.И.О.)* _____ *(подпись)*

Приложение № 15
Утверждено
приказом Министерства образования
Пензенской области
от 26.04.2016 № 99/01-04

Инструкция

по защите технических средств государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по защите технических средств РИС ГИА (далее – Инструкция) определяет в Министерстве образования Пензенской области порядок действий администратора безопасности и пользователей РИС ГИА, в том числе технических средств ее системы защиты.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»,

Термин	Определение	Источник
		утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления пользователей РИС ГИА с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Определение границ контролируемой зоны

2.1. Границами контролируемой зоны РИС ГИА являются ограждающие конструкции здания, в котором установлены технические средства РИС ГИА, в том числе средства защиты информации (внешние границы стен помещений, включая окна и двери).

2.2. Границы контролируемой зоны РИС ГИА определены приказом Министерства образования Пензенской области.

2.3. Помещения, предназначенные для размещения технических средств РИС ГИА и ее средств защиты информации, определены в эксплуатационной документации

на систему защиты информации РИС ГИА и утверждены приказом Министерства образования Пензенской области.

2.4. Перемещение стационарного оборудования РИС ГИА и средств защиты информации за границу контролируемой зоны не допускается.

2.5. Несанкционированный вынос за границу контролируемой зоны учтенных машинных носителей, мобильных технических средств запрещен.

2.6. Вынос для ремонта за границу контролируемой зоны оборудования РИС ГИА и средств защиты информации допустим только с письменного разрешения министра образования Пензенской области с учетом выполнения требований Инструкции по защите машинных носителей информации в Министерстве образования Пензенской области.

2.7. Несанкционированный внос пользователями РИС ГИА неучтенных машинных носителей, мобильных технических средств запрещен.

3. Доступ в контролируемую зону

3.1. На период обработки информации, содержащей сведения (в том числе ПДн), не составляющих государственную тайну (далее – защищаемая информация), в Помещениях, где размещено оборудование РИС ГИА и ее средства защиты информации, могут находиться только лица, допущенные к обработке защищаемой информации в соответствии с утвержденным приказом Министерства образования Пензенской области «Об утверждении перечней лиц, имеющих право доступа в помещения, в которых размещена РИС ГИА.

3.2. Доступ в контролируемую зону осуществляется в соответствии с Порядком доступа в помещения, в которых размещена РИС ГИА.

3.3. Организацию физического доступа в помещения контролируемой зоны РИС ГИА осуществляет ответственный за защиту информации в РИС ГИА.

4. Правила размещения технических средств и устройств вывода информации.

4.1. При размещении в Помещениях технических средств РИС ГИА. в том числе средств защиты информации, должны быть реализованы меры, направленные на предотвращение случаев несанкционированного вскрытия средств вычислительной техники.

4.2. Корпуса средств вычислительной техники РИС ГИА опечатываются.

4.3. При размещении в помещениях контролируемых зон средств отображения информации (мониторы и другие средства визуального отображения информации) должен быть исключен несанкционированный просмотр выводимой на них информации.

4.4. Размещение средств отображения информации указано в эксплуатационной документации на РИС ГИА и эксплуатационной документации на систему защиты информации.

4.5. При обнаружении нарушения целостности пломб ставится в известность администратор безопасности.

4.6. Выполнение требований к размещению устройств вывода информации и контроль целостности пломб в контролируемых зонах обеспечивает администратор безопасности.

5. Защита каналов связи

5.1. Технические средства (кабельные разъемы, маршрутизаторы, сетевой экран и т.п.) для подключения РИС ГИА к каналам связи, выходящими за пределы контролируемой зоны, должны быть размещены в пределах контролируемой зоны.

5.2. Расположение указанных технических средств и физический доступ к ним контролирует администратор безопасности.

6. Ответственность

6.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 16
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-04

Порядок

по управлению изменениями в конфигурации государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»
(РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящий Порядок по управлению изменениями в конфигурации РИС ГИА (далее – Порядок) определяет в Министерстве образования Пензенской области организацию и последовательность действий сотрудников Министерства образования Пензенской области в случае необходимости принятия решения о внесении изменений в конфигурацию РИС ГИА.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
СЗИ	Система защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработан Порядок:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации. информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведении работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России от 29.04.2021 №77).

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящим Порядком до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления пользователей РИС ГИА с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Общий порядок управления изменениями в конфигурации РИС ГИА и ее СЗИ

2.1. Организацию и управление изменениями в конфигурации РИС ГИА и ее СЗИ осуществляет администратор безопасности.

2.2. Изменение конфигурации РИС ГИА и ее СЗИ инициируется на основании служебных записок начальников структурных подразделений на имя министра образования Пензенской области с обоснованием необходимости внесения изменений в конфигурацию РИС ГИА и ее СЗИ и указанием перечня предлагаемых изменений.

2.3. Изменением конфигурации РИС ГИА и ее СЗИ является:

– изменение места расположения в Министерстве образования Пензенской области технических средств, входящих в РИС ГИА и ее СЗИ;

– передача технических средств, входящего в РИС ГИА и ее СЗИ, между структурными подразделениями и пользователями РИС ГИА;

– изменение параметров настроек программных, программно-технических средств и средств защиты информации;

– обновление программных, программно-технических средств и средств защиты информации или замена их на аналогичные средства;

– исключение из компонентов РИС ГИА и ее СЗИ программных средств, программно-технических и средств защиты информации или добавление аналогичных средств;

– изменение видов и типов программных, программно-технических средств и средств защиты информации;

– замена, установка и ввод в эксплуатацию нового оборудования, входящего в состав РИС ГИА, ее СЗИ;

– изъятие, списание и утилизация оборудования, входящего в состав РИС ГИА, ее СЗИ.

2.4. Изменение конфигурации РИС ГИА и ее СЗИ допустимо только после согласования служебной записки с администратором безопасности.

2.5. Непосредственная реализация мероприятий по изменению конфигурации РИС ГИА и ее СЗИ осуществляется лицами, включенными в утвержденный приказом Министерства образования Пензенской области перечень лиц, которым разрешены действия по внесению изменений в конфигурацию РИС ГИА (далее – уполномоченный сотрудник).

2.6. Запрещается осуществление изменения конфигурации РИС ГИА и ее СЗИ лицами, не включенными в перечень лиц в соответствии с пунктом 2.5. настоящего Порядка.

2.7. Запрещается вносить несанкционированные изменения в конфигурацию программных, программно-технических средств, средств защиты информации.

2.8. Запрещается осуществлять несанкционированную замену программных, программно-технических средств, средств защиты информации на аналогичные средства.

2.9. Запрещается вносить изменения в архитектуру системы защиты информации, изменять состав, структуру системы защиты информации.

2.10. Изменение в составе технических и программных средств отражается в Техническом паспорте информационной (автоматизированной) системы РИС ГИА и соответствующей эксплуатационной документации.

3. Последовательность действий по внесению изменений в конфигурацию РИС ГИА и ее СЗИ

3.1. Изменение конфигурации осуществляется на основании служебной записки начальника структурного подразделения на имя министра образования Пензенской области, согласованной с администратором безопасности.

3.2. При принятии решения о необходимости внесения изменения в конфигурацию РИС ГИА и ее СЗИ администратор безопасности проводит анализ потенциального воздействия планируемых изменений в конфигурацию РИС ГИА и ее СЗИ:

– возникновение дополнительных угроз безопасности;

– влияние изменений на работоспособность РИС ГИА и ее СЗИ;

– влияние изменений на существующие аттестованные механизмы обеспечения безопасности в РИС ГИА и ее СЗИ.

3.3. В случае развития (модернизации) РИС ГИА, в ходе которого предусматривается:

– изменение конфигурации (параметров настройки) программных, программно-технических и средств защиты информации;

– исключение программных, программно-технических и средств защиты информации;

– замена программных, программно-технических и средств защиты информации на аналогичные средства;

– **проведение дополнительных аттестационных испытаний** в соответствии с пунктом 33 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 №77. Сведения об изменениях аттестованного объекта информатизации и проведенных при этом аттестационных испытаниях включаются в технический паспорт. Действие аттестата соответствия не прекращается.

3.4. Проводится повторная аттестация в случае развития (модернизации) РИС ГИА приводящего к повышению класса защищенности (уровня защищенности персональных данных) РИС ГИА и (или):

– изменения архитектуры системы защиты информации РИС ГИА в части изменения видов и типов программных, программно-технических средств и средств защиты информации;

– изменения структуры системы защиты информации РИС ГИА;

– состава и мест расположения РИС ГИА и ее компонентов.

3.5. При отсутствии возможности по реализации мероприятий по внесению изменений в конфигурацию РИС ГИА и ее СЗИ, изложенных в служебной записке, или если предлагаемые изменения в конфигурацию РИС ГИА и ее СЗИ влияют на механизмы обеспечения безопасности информации и влекут за собой прохождение повторной аттестации, администратор безопасности отклоняет ее с указанием причин отказа.

3.6. В случае наличия технической возможности реализации предлагаемых мероприятий по изменению конфигурации РИС ГИА и ее СЗИ и, если предлагаемые изменения в конфигурацию РИС ГИА и ее СЗИ не влияют на механизмы обеспечения безопасности информации и не влекут за собой прохождение повторной аттестации, администратор безопасности передает указанную служебную записку для исполнения уполномоченному сотруднику.

3.7. Уполномоченный сотрудник осуществляет изменение конфигурации РИС ГИА и ее СЗИ и оповещает администратора безопасности о ходе и результатах исполнения мероприятий, предлагаемых в служебной записке.

3.8. Администратор безопасности осуществляет проверку корректности изменения конфигурации и при необходимости совместно с ответственным за защиту информации в РИС ГИА организует актуализацию документации по вопросам обеспечения безопасности информации в РИС ГИА, при этом также осуществляется контроль за обеспечением безопасности ПДн в РИС ГИА со стороны ответственного за организацию обработки ПДн в Министерстве образования Пензенской области и ответственного за защиту информации в РИС ГИА.

3.9. Решение о проведении повторной аттестации принимает министр образования Пензенской области по представлению ответственного за защиту информации в РИС ГИА и ответственного за организацию обработки ПДн в Министерстве образования Пензенской области.

4. Контроль действий по внесению изменений в конфигурацию РИС ГИА и ее СЗИ

4.1. Ответственный за защиту информации РИС ГИА не реже 1 раза в год организует проверку текущей конфигурации РИС ГИА и ее СЗИ на соответствие базовой конфигурации.

4.2. Результаты проверки оформляются Актом контроля текущей конфигурации, который также подписывает ответственный за организацию обработки ПДн в Министерстве образования Пензенской области, ответственным за защиту информации в РИС ГИА.

5. Ответственность

5.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 17
Утверждено
приказом Министерства образования
Пензенской области
от 26.04.2016 № 99/01-04

Порядок

по выявлению инцидентов 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» и реагированию на них
(РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящий Порядок по выявлению инцидентов в РИС ГИА и реагированию на них (далее – Порядок) определяет в Министерстве образования Пензенской области порядок выявления, идентификации, регистрации инцидентов информационной безопасности, их анализ и принятие мер по устранению последствий инцидентов информационной безопасности и предотвращению повторного возникновения инцидентов информационной безопасности в РИС ГИА.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система Пензенской области
ИБ	Информационная безопасность
ПДн	Персональные данные

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут	Методический документ ФСТЭК России «Меры

Термин	Определение	Источник
	привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).	защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Событие информационной безопасности	Идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Перечень нормативных правовых актов, на основании которых разработан Порядок:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведении работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России от 29.04.2021 №77);

- приказ ФСБ России от 13.02.2023 N 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных» (далее - приказ ФСБ России от 13.02.2023 N 77).

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящим Порядком до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления пользователей с настоящим Порядком возлагается на ответственного за защиту информации в РИС ГИА.

2. Порядок выявления, идентификации и регистрации инцидентов ИБ

2.1. К инцидентам ИБ относятся нарушение конфиденциальности, целостности или доступности информации (в том персональных данных), не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), обрабатываемых в РИС ГИА, а также попытки и факты получения несанкционированного доступа к РИС ГИА и средствам защиты информации, в том числе:

- отказ технических средств РИС ГИА и средств защиты информации;
- системные сбои или перезагрузки технических средств РИС ГИА и средств защиты информации;
- сбои программного обеспечения и средств защиты информации;
- несанкционированное внесение изменений в конфигурации РИС ГИА и ее систему защиты информации;
- внедрение вредоносных компьютерных программ (вирусов);
- нарушение физических мер защиты защищаемой информации, обрабатываемой РИС ГИА;
- нарушение правил разграничения доступа к защищаемой информации, обрабатываемой в РИС ГИА;
- совершение попыток несанкционированного доступа к защищаемой информации в РИС ГИА;
- ошибки пользователей РИС ГИА;

– несоблюдение пользователями РИС ГИА требований организационно-распорядительных документов и действующих нормативных правовых актов по защите информации;

2.2. Непосредственная реализация мероприятий по выявлению инцидентов и реагированию на них осуществляется лицами, включенными в утвержденный приказом Министерства образования Пензенской области перечень лиц, ответственных за выявление инцидентов в РИС ГИА и реагирование на них.

2.3. Порядок сбора информации о событиях информационной безопасности и регистрация событий информационной безопасности РИС ГИА приведены в Инструкции по управлению событиями информационной РИС ГИА.

2.4. После получения информации о событии ИБ администратор безопасности осуществляет:

– анализ полученной информации, при необходимости получает дополнительные сведения из других источников;

– подтверждает, что событие является инцидентом ИБ;

– проверяет взаимосвязь с событиями/инцидентами ИБ, произошедшими ранее.

2.5. В случае, если по результатам анализа подтверждается, что данное событие является инцидентом ИБ, администратор безопасности оформляет отчет об инциденте ИБ и предоставляет его ответственному за защиту информации в РИС ГИА.

2.6. Не допускается осуществлять обработку защищаемой информации в случае обнаружения инцидента безопасности.

3. Информирование о возникновении инцидентов ИБ в РИС ГИА

3.1. Пользователь РИС ГИА, обнаруживший информацию о событии ИБ в РИС ГИА, должен незамедлительно любым доступным способом сообщить ее сотрудникам, включенным в утвержденный приказом Министерства образования Пензенской области Перечень лиц, ответственных за выявление инцидентов в РИС ГИА, и реагирование на них, и начальнику структурного подразделения Министерства образования Пензенской области.

3.2. Администратор безопасности оповещает об инциденте ИБ ответственного за защиту информации в РИС ГИА и, в случае необходимости, информирует пользователей РИС ГИА о возникновении инцидента ИБ и дает указания по дальнейшим действиям.

Форму и порядок оповещения устанавливает администратор безопасности.

3.3. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Министерство образования Пензенской области обязано с момента выявления такого инцидента Министерством образования Пензенской области, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:

– **в течение 24 часов** о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Министерством образования Пензенской области на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

– **в течение 72 часов** о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.4. Министерство образования Пензенской области обязано в порядке, утвержденном приказом ФСБ России от 13.02.2023 №77, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

4. Анализ инцидентов ИБ в РИС ГИА

4.1. В целях локализации, устранения последствий инцидента ИБ, определения причин и источников возникновения инцидента ИБ, а также оценки последствий и формирования перечня мероприятий по недопущению повторного возникновения инцидента ИБ проводят анализ инцидента ИБ в РИС ГИА.

4.2. Анализ выявленного инцидента ИБ осуществляет постоянно действующая комиссия, состав и полномочия которой определяются приказом Министерства образования Пензенской области в соответствии с требованиями действующего законодательства Российской Федерации (далее - Комиссия).

4.3.В ходе анализа инцидента ИБ осуществляется сбор информации:

– описание произошедшего инцидента ИБ (время, место, обстоятельства возникновения инцидента ИБ), причин, повлекшие за собой его возникновение;

– определение задействованных в инциденте ИБ ресурсов РИС ГИА;

– описание всех выявленных уязвимостей (источников возникновения инцидента ИБ), в результате эксплуатации которых произошел инцидент ИБ.

4.4. По выявленному инциденту ИБ проводят служебное расследование.

4.5. Служебное расследование по выявленному инциденту ИБ – это деятельность Комиссии, направленная на сбор, анализ, оценку информации и документов в целях установления причин и условий, способствовавших возникновению инцидента информационной безопасности, а также установлению лиц, причастных к его возникновению.

4.6. Непосредственный порядок проведения служебного расследования и сроки его проведения определяются локальным актом Министерства образования Пензенской области.

4.7. Результаты служебного расследования оформляются заключением в соответствии с формой, установленной Приложением к настоящему Порядку.

5. Порядок устранения последствий инцидента ИБ

5.1. Ответственным лицом за принятие мер по устранению последствий инцидента ИБ в РИС ГИА является администратор безопасности.

При устранении последствий инцидента ИБ администратор безопасности вправе привлекать к работам администратора, сотрудников других структурных подразделений Министерства образования Пензенской области.

5.2. При нарушении конфиденциальности защищаемой информации, обрабатываемой в РИС ГИА, или подозрении в ее нарушении администратор безопасности:

- проводит процедуру смены паролей пользователям;
- пересматривает и обновляет, с учетом содержания инцидента, матрицу доступа к ресурсам РИС ГИА.

5.3. При нарушении целостности и доступности защищаемой информации, обрабатываемой в РИС ГИА, администратор безопасности:

- организует переустановку программного обеспечения РИС ГИА и системы защиты информации с дистрибутивных носителей используемого программного обеспечения;
- осуществляет удаление вредоносного программного обеспечения;
- организует восстановление данных из резервных копий;
- организует устранение уязвимостей;
- проверяет состав конфигурации РИС ГИА и ее системы защиты информации (при необходимости восстанавливает конфигурацию в соответствии с эксплуатационной документацией).

6. Порядок устранения причин инцидента ИБ и принятие мер по недопущению повторного возникновения инцидента ИБ

6.1. В Министерстве образования Пензенской области осуществляется планирование и принятие мер по устранению инцидентов, в том числе по восстановлению РИС ГИА в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов.

6.2. Причины инцидентов ИБ в РИС ГИА разделяют на типы:

- аппаратно–программные причины;
- организационные причины.

6.3. К аппаратно–программным причинам относятся все причины, связанные с недостатками аппаратной и программной частей РИС ГИА и ее системы защиты информации (вирусное заражение, несанкционированный доступ или его попытка,

несанкционированное изменение состава конфигурации, ошибки кода, ошибки настроек, неисправности оборудования, электромагнитная совместимость и т.п.).

6.4. К организационным причинам относятся недостатки организационно-распорядительной документации, ошибки пользователей, недостатки физической защиты доступа, дисциплинарные, умысел на причинение ущерба и т.п.

6.5. Устранение аппаратно–программных причин инцидентов осуществляет администратор безопасности совместно с администраторами в части касающейся. Сроки и состав действий определяются индивидуально по каждому инциденту.

6.6. Устранение организационных причин организовывает ответственный за защиту информации в РИС ГИА совместно с ответственным за организацию обработки ПДн в Министерстве образования Пензенской области по письменным предложениям администратора безопасности. Сроки и состав действий по устранению организационных причин устанавливаются индивидуально по каждому инциденту.

6.7. Перечень мероприятий, направленных на предупреждение повторного возникновения инцидента ИБ в дальнейшем, формируется администратором безопасности после согласования с ответственным защиту информации в РИС ГИА.

7. Ответственность

7.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.

Приложение
к Порядку по выявлению инцидентов
в РИС ГИА
и реагированию на них

Утверждаю
Министр образования Пензенской
области
_____/_____/
«___» _____ 20__ г.

ЗАКЛЮЧЕНИЕ № ___
служебного расследования инцидента информационной безопасности

Дата составления: «____» _____ 20 г.

Место проведения служебного расследования:

_____

Комиссия в составе:

Председатель комиссии: _____
(должность, ФИО)

Члены комиссии: _____
(должность, ФИО)

_____
(должность, ФИО)

на основании приказа Министерства образования Пензенской области от «___» _____ 202_ г. №___ провела служебное расследование по инциденту информационной безопасности:

_____

_____

_____

_____

В ходе служебной выявлен следующий ущерб:

_____

_____

_____

_____

и причины инцидента:

_____

Заключение и выводы комиссии:

Предлагаемые мероприятия для реализации:

Председатель комиссии:

(должность)	(подпись)	(ФИО)

Члены комиссии:

(должность)	(подпись)	(ФИО)
(должность)	(подпись)	(ФИО)

Приложение № 18
Утверждено
приказом Министерства образования
Пензенской области
от 16.02.2026 № 99/01-04

Порядок

доступа в помещения, в которых размещена государственная информационная система Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»
(РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящий Порядок доступа в помещения, в которых размещена РИС ГИА (далее - Порядок) определяет в Министерстве образования Пензенской области порядок организации режима безопасности помещений, в которых размещена РИС ГИА в рабочее, нерабочее время и в нештатных ситуациях.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
Помещения	Помещения, в которых размещена РИС ГИА (технические средства РИС ГИА, включая средства защиты информации)

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Контролируемая зона	Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а	Методический документ ФСТЭК России «Меры защиты информации в государственных

Термин	Определение	Источник
	также транспортных, технических или иных средств	информационных системах», утвержден ФСТЭК России 11.02.2014
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Пользователи РИС ГИА должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления пользователей РИС ГИА с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА.

2. Порядок организации режима обеспечения безопасности Помещений

2.1. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки защищаемой информации (в том числе персональных данных), средств защиты информации и носителей защищаемой информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

2.2. Перечень Помещений РИС ГИА утверждается приказом Министерства образования Пензенской области.

2.3. Помещения оснащаются входными дверями с механическими замками.

2.4. Вскрытие и закрытие Помещений производится сотрудниками Министерства образования Пензенской области, имеющие права доступа в данные Помещения.

2.5. Ключи от Помещений хранятся у сотрудников Министерства образования Пензенской области либо в ином порядке, устанавливаемом Инструкцией по обеспечению внутриобъектового и пропускного режима в Министерстве образования Пензенской области.

2.6. Организация режима обеспечения безопасности Помещений, где размещены используемые криптосредства, хранятся и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств осуществляется в соответствии с Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств.

2.7. Внутренний контроль за соблюдением порядка доступа в Помещения осуществляется ответственным за организацию обработки ПДн и ответственным за защиту информации в РИС ГИА.

3. Правила доступа в контролируемую зону в рабочее, нерабочее время, в нештатных ситуациях

3.1. На период обработки информации (в том числе персональных данных), содержащей сведения, не составляющих государственную тайну (далее – защищаемая информация), в помещениях, где размещено оборудование РИС ГИА и средства защиты информации, могут находиться только лица, допущенные к обработке защищаемой информации в соответствии с утвержденным приказом Министерства образования Пензенской области.

3.2. В нерабочее время пребывание вышеуказанных лиц разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных министром образования Пензенской области.

3.3. Нахождение в помещениях контролируемых зон РИС ГИА других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии лица, допущенного к обработке защищаемой информации в настоящем помещении.

3.4. Запрещается бесконтрольное нахождение в помещениях контролируемой зоны посторонних лиц в рабочее и нерабочее время.

3.5. Министр образования Пензенской области и лица, его замещающие, могут находиться в помещениях контролируемой зоны в любое время, в том числе в нерабочие и праздничные дни.

3.6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать непосредственному руководителю структурного подразделения Министерства образования Пензенской области.

3.7. Сотрудники территориальных подразделений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой медицинской помощи» допускаются в помещения контролируемой зоны РИС ГИА для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения РИС ГИА.

4. Ответственность

4.1. Сотрудники Министерства образования Пензенской области АСТИ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 19
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция
по управлению программным обеспечением
государственной информационной системы Пензенской области
«Региональная информационная система обеспечения проведения
государственной итоговой аттестации обучающихся, освоивших
основные образовательные программы основного общего и
среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по управлению программным обеспечением РИС ГИА в Министерстве образования Пензенской области (далее – Инструкция) определяет порядок действий администратора РИС ГИА, администратора безопасности РИС ГИА и ответственного за защиту информации в РИС ГИА при реализации ограничений в применении программного обеспечения РИС ГИА, установке разрешенного программного обеспечения ГИС, его настройке и обновлении.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система
ПО	Программное обеспечение

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрирование (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России, «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	Методический документ ФСТЭК России, «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Компонент программного	Составная часть (программный модуль) программного	Методический документ ФСТЭК России «Меры

Термин	Определение	Источник
обеспечения	обеспечения, выполняющий определенную функцию	защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- - Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Администратор безопасности РИС ГИА (далее- администратор безопасности) и администратор РИС ГИА (далее- администратор) должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления вышеуказанных лиц с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА (далее – Ответственный за защиту информации).

2. Программное обеспечение РИС ГИА

2.1 ПО РИС ГИА подразделяется на:

– прикладное ПО РИС ГИА;

– общесистемное ПО РИС ГИА;

– специальное программное (микропрограммное) обеспечение;

– ПО средств защиты информации РИС ГИА.

2.2. Состав общесистемного и прикладного ПО РИС ГИА, состав средств защиты информации, используемых в РИС ГИА, определяются в Техническом паспорте РИС ГИА.

2.3. Перечень ПО и (или) его компонентов, разрешенных к использованию в РИС ГИА, и Перечень ПО и (или) его компонентов, запрещенных к использованию в РИС ГИА, формируются администратором безопасности и согласуются с Ответственным за защиту информации (формы Перечней программного обеспечения и (или) его компонентов, разрешенных и запрещенных к использованию в РИС ГИА, приведены в Приложениях №1 и №2 соответственно).

3. Порядок установки (обновления) ПО РИС ГИА

3.1. Организация мероприятий по установке (инсталляции) ПО и (или) его компонентов, обновлению программного обеспечения РИС ГИА регламентируются «Порядком управления конфигурацией государственной информационной системы «РИС ГИА и ее системы защиты информации в Министерстве образования Пензенской области.

3.2. Установка (инсталляция) ПО и (или) его компонентов, обновление программного обеспечения РИС ГИА согласуются с Ответственным за защиту информации и осуществляются администратором и администратором безопасности, имеющими необходимые полномочия в соответствии с Матрицей доступа.

3.3. Установка (инсталляция) ПО и (или) его компонентов, обновлений программного обеспечения РИС ГИА осуществляется только от имени администратора и в соответствии с эксплуатационной документацией.

3.4.Установка (инсталляция) в РИС ГИА ПО (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом Перечня ПО и (или) его компонентов, разрешенных к использованию в РИС ГИА и Перечня ПО и (или) его компонентов, запрещённых к использованию в РИС ГИА.

3.5. Устанавливаемое в РИС ГИА ПО предварительно проверяется на отсутствие опасных функций в соответствии с Инструкцией по антивирусной защите РИС ГИА в Министерстве образования Пензенской области.

3.6. При установке (инсталляции) компонентов ПО РИС ГИА администратором безопасности и администратором осуществляются:

– определение компонентов ПО (состава и конфигурации), подлежащих установке в РИС ГИА после загрузки ОС;

– настройка параметров установки компонентов ПО, обеспечивающая исключение установки (если осуществимо) компонентов ПО, использование которых не требуется для реализации информационной технологии РИС ГИА (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов ПО);

– выбор конфигурации устанавливаемых компонентов ПО;

– определение и применение параметров настройки компонентов ПО, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей ГИС, приводящих к возникновению угроз безопасности информации.

3.7. Контроль за установкой компонентов ПО РИС ГИА (состав компонентов, параметры установки, конфигурация компонентов) осуществляет администратор безопасности.

3.8. Контроль установленного (инсталлированного) в РИС ГИА ПО на предмет соответствия его перечню ПО, разрешенному к установке в ГИС, на предмет отсутствия ПО, запрещенного к установке, а также контроль установки обновлений программного обеспечения осуществляются администратором безопасности не реже 1

раза в полгода в соответствии с Инструкцией по контролю (анализу) защищенности РИС ГИА.

3.9. Документирование внесений изменений в Технический паспорт РИС ГИА и в эксплуатационную документацию определяется «Порядком управления конфигурацией РИС ГИА и ее системы защиты информации в Министерстве образования Пензенской области».

4. Ответственность

4.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.

Приложение №1
к Инструкции по управлению программным
обеспечением РИС ГИА в Министерстве
образования Пензенской области

**Перечень ПО и (или) его компонентов,
разрешенных к использованию в РИС ГИА**

Тип	Программное обеспечение и его компоненты

Приложение №2
к Инструкции по управлению программным
обеспечением РИС ГИА в Министерстве
образования Пензенской области

**Перечень ПО и (или) его компонентов,
запрещенных к использованию в РИС ГИА**

Тип	Программное обеспечение и его компоненты

Приложение № 20
Утверждено
приказом Министерства образования
Пензенской области
от 26.01.2026 № 99/01-04

Инструкция

по обеспечению целостности государственной информационной системы Пензенской области «Региональная информационная система обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» (РИС ГИА)

Оглавление

1. Общие положения

1.1. Настоящая Инструкция по обеспечению целостности 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 – Инструкция) определяет в Министерстве образования Пензенской области порядок действий администратора безопасности РИС ГИА, администратора РИС ГИА и ответственного за защиту информации в РИС ГИА при восстановлении работоспособности РИС ГИА в случае возникновения нештатной ситуации.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ГИС	Государственная информационная система
ПО	Программное обеспечение

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» утвержден приказом ФСТЭК России 11.02.2014
Администратор	Пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) ГИС в соответствии с установленной ролью	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных

Термин	Определение	Источник
		системах», утвержден ФСТЭК России 11.02.2014
Инцидент	Непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- - Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации. информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

- приказ ФСТЭК России от 29.04.2021 №77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

1.4. Администратор безопасности РИС ГИА (далее - администратор безопасности) и администратор РИС ГИА (далее- администратор) должны быть ознакомлены с настоящей Инструкцией до начала работы в РИС ГИА под подпись. Обязанность по организации ознакомления вышеуказанных лиц с настоящей Инструкцией возлагается на ответственного за защиту информации в РИС ГИА (далее – ответственный за защиту информации).

2. Восстановление работоспособности РИС ГИА при возникновении нештатных ситуаций

2.1. Для обеспечения восстановления информации, ПО РИС ГИА, включая ПО средств защиты информации, в случае возникновения нештатной ситуации применяются следующие меры:

– принятие ответственным за защиту информации в РИС ГИА планов по действиям администратора безопасности и администратора при возникновении нештатных ситуаций;

– применение средств резервного копирования для восстановления данных РИС ГИА;

– проведение периодического обучения персонала по вопросам информационной безопасности.

2.2. В ходе восстановления работоспособности РИС ГИА при возникновении нештатной ситуации администратором безопасности совместно с администратором, в части кающейся в соответствии с Матрицей доступа к РИС ГИА, осуществляется:

– восстановление ПО, включая ПО средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

– восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

– возврат РИС ГИА в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей РИС ГИА, определенных ответственным за защиту информации, позволяющих решать задачи по обработке информации.

2.2. В случае, когда восстановление работоспособности системы зашиты информации невозможно, ответственным за защиту информации применяются компенсирующие меры, позволяющие снизить возможность негативного влияния на обеспечение конфиденциальности, целостности и доступности информации, обрабатываемой в РИС ГИА.

2.3. В РИС ГИА запрещается проводить обработку информации в случае обнаружения неисправностей в системе защиты информации, а также в случае обнаружения инцидента информационной безопасности.

2.4. Реагирование на инциденты информационной безопасности, проведение служебных расследований и мероприятий, нацеленных на предотвращение наступления повторных инцидентов информационной безопасности, осуществляется в соответствии с Порядком по выявлению инцидентов в РИС ГИА в Министерстве образования Пензенской области.

3. Ответственность

3.1. Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.

Приложение № 21
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-04

Положение
по использованию средств криптографической защиты информации в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящее Положение по использованию средств криптографической защиты информации (далее - Положение) в Министерстве образования Пензенской области определяет порядок обращения со средствами криптографической защиты информации (далее - криптосредствами).

1.2. Сокращения, термины и определения:

В настоящем Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ПДн	Персональные данные
ИС	Информационная система
СКЗИ, криптосредство	Средство криптографической защиты информации
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФЗ от 06.04.2011 №63-ФЗ	Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи»
Приказ ФАПСИ от 13.06.2001 № 152	Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации»
Приказ ФСБ России от 09.02.2005 № 66 (Положение ПКЗ-2005)	приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»,

Термин	Определение	Источник
		утвержден ФСТЭК России 11.02.2014
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам	Приказ ФАПСИ от 13.06.2001 № 152
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	ГОСТ Р 56115-2014
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
	информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	

1.3. Перечень нормативных правовых актов, на основании которых разработано настоящее Положение:

- приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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»;

- приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

2. Порядок применения криптосредств

2.1. Для обеспечения безопасности информации (в том числе ПДн), содержащей сведения, не составляющие государственную тайну (далее – защищаемая информация), при их обработке в ИС должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства.

Класс криптосредства определяется в соответствии с приказами ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИС с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности» и от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

2.2. Ответственность за эксплуатацию средств криптографической защиты информации в ИС возлагается на ответственного пользователя криптосредств.

2.3. Ответственный пользователь криптосредств назначается приказом Министерства образования Пензенской области. При смене ответственного пользователя криптосредств вносятся изменения в приказ Министерства образования Пензенской области «О назначении ответственного пользователя средств криптографической защиты информации в Министерстве образования Пензенской области».

2.4. Ответственный пользователь криптосредств должен быть ознакомлен с настоящим документом, Инструкцией ответственного пользователя средств криптографической защиты информации, Инструкцией пользователя средств криптографической защиты информации и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности защищаемой информации с использованием криптосредств.

По результатам ознакомления осуществляется соответствующая запись в Журнале ознакомления сотрудников с нормативными правовыми актами Российской Федерации и локальными актами Министерства образования Пензенской области по обеспечению безопасности защищаемой информации с использованием криптосредств (Приложение №1).

2.5. Основанием для предоставления доступа к работе с криптосредствами является внесение сотрудника в Перечень лиц, допущенных к работе со средствами

криптографической защиты информации в Министерстве образования Пензенской области, утверждаемый приказом Министерства образования Пензенской области.

2.6. Пользователи криптосредств допускаются к работе с криптосредствами после прохождения обучения правилам работы с СКЗИ и ознакомления с настоящим Положением, Инструкцией пользователя криптосредств и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности информации с использованием криптосредств.

По результатам прохождения обучения правилам работы с криптосредствами оформляется Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации (Приложение №2). По результатам ознакомления сотрудников осуществляется соответствующая запись в Журнале ознакомления сотрудников с нормативными правовыми актами Российской Федерации и локальными актами Министерства образования Пензенской области по обеспечению безопасности информации с использованием криптосредств.

2.7. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.8. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей криптосредств должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

2.9. Системные блоки технических средств (или иные аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, аппаратные и аппаратно-программные СКЗИ) с установленными СКЗИ должны оборудоваться средствами контроля за их вскрытием (опечатываться, опломбироваться). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

2.10. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствии лиц, не допущенных к работе с данными криптосредствами.

2.11. Криптосредства, а также другое оборудование, функционирующее с криптосредствами, на время отсутствия пользователей, при наличии такой технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае предусматриваются организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

2.12. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

2.13. Эксплуатационную и техническую документацию к СКЗИ разрешается пересылать заказными или ценными почтовыми отправлениями.

3. Обязанности ответственного пользователя криптосредств[1]

3.1. Ответственный пользователь криптосредств обязан:

- проводить обучение пользователей криптосредств правилам работы с криптосредствами с оформлением Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и отметкой в Журнале ознакомления сотрудников с нормативными правовыми актами Российской Федерации и локальными актами Министерства образования Пензенской области по обеспечению безопасности защищаемой информации с использованием криптосредств;

- вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с документальным оформлением в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов по установленной форме (Приложение № 4);

- контролировать заполнение Акта установки и ввода в эксплуатацию средств криптографической защиты информации (Приложение №3), делать отметку Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- хранить Акты установки и ввода в эксплуатацию средств криптографической защиты информации;

- организовать надежное хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации, ключей от металлических хранилищ (сейфов);

- вести учет лиц, допущенных к работе с СКЗИ. Формировать и актуализировать приказом Министерства образования Пензенской области Перечень лиц, допущенных к работе со средствами криптографической защиты информации в Министерстве образования Пензенской области;

- заводить и вести лицевые счета на каждого пользователя СКЗИ, в котором регистрировать числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы (Приложение №5);

- вести учет металлических хранилищ (сейфов), предназначенных для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением в Журнале учета металлических хранилищ (сейфов) (Приложение №6);

- проводить не реже одного раза в год проверку создаваемой приказом Министерства образования Пензенской области комиссии соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации (Приложение 7);

---

[1] Ответственный пользователь криптосредств в своей деятельности руководствуется Инструкцией ответственного пользователя средств криптографической защиты информации, утверждаемой приказом Министерства образования Пензенской области

- осуществлять контроль за ведением пользователем криптосредства технического (аппаратного) журнала (Приложение №8) в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ;

- проводить периодический контроль за состоянием технических средств охраны (при их наличии) совместно с представителем службы охраны или дежурным по организации с отметкой в Журнале контроля состояния охранной сигнализации;

- осуществлять контроль за проведением работ по размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ в спецпомещениях пользователей СКЗИ;

- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ пользователей криптосредств;

- контролировать наличие и актуальность Перечня помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом Министерства образования Пензенской области;

- контролировать наличие и актуальность Перечня лиц, имеющих право доступа в Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом Министерства образования Пензенской области;

- соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения должностных обязанностей, в том числе сведений о криптоключах, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;

- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемых в ИС с использованием СКЗИ;

- немедленно уведомлять министра образования Пензенской области о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

- организовывать мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передаваемой (хранящейся) с использованием СКЗИ.

4. Обязанности пользователей криптосредств[2]

4.1. Пользователь криптосредств обязан:

- получить у Ответственного пользователя криптосредства СКЗИ, эксплуатационную и техническую документацию, ключевые документы с

[2] Пользователь криптосредств в своей деятельности руководствуется Инструкцией пользователя средств криптографической защиты информации, утверждаемой приказом Министерства образования Пензенской области

документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- получить у Ответственного пользователя криптосредств ключ от металлического хранилища (сейфа) для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов);

- хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Хранить резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, раздельно от действующих ключевых документов;

- вести технический (аппаратный) журнал в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ. Регистрировать в техническом (аппаратном) журнале разовый ключевой носитель или электронную запись соответствующего криптоключа, а также отражать данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. Самостоятельно уничтожать разовые ключевые носители, электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, и делать об этом отметку под расписку в техническом (аппаратном) журнале;

- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой в ИС с использованием СКЗИ;

- контролировать целостность печатей (пломб) на системных блоках технических средствах с установленными СКЗИ;

- осуществлять уничтожение ключевых документов с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) после окончания срока действия, не позднее 10 суток после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ;

- сообщать Ответственному пользователю криптосредств и непосредственному руководителю структурного подразделения Министерства образования Пензенской области о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- немедленно уведомлять Ответственного пользователя криптосредств министру образования Пензенской области о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений

конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений:

- немедленно выводить из действия криптоключи, в отношении которых возникло подозрение в компрометации, с уведомлением Ответственного пользователя криптосредств и министра образования Пензенской области с последующим их уничтожением.

5. Пользователям криптосредств запрещается

- разглашать информацию о ключевых документах и информацию ограниченного доступа;

- вносить любые изменения в программное обеспечение СКЗИ, изменять настройки СКЗИ;

- допускать к использованию СКЗИ посторонних лиц;

- осуществлять вскрытие системных блоков технических средств с установленными СКЗИ, подключать к ним дополнительные устройства;

- использовать криптоключи, в отношении которых возникло подозрение в компрометации;

- оставлять ключевые носители без контроля, выносить их за пределы служебных помещений;

- снимать копии с ключевых документов;

- записывать на ключевой носитель информацию, не предусмотренную правилами пользования СКЗИ (служебные файлы, текстовые и мультимедийные файлы и т.п.);

- допускать установку ключевых документов в другие ПЭВМ;

- выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.).

6. Порядок учета криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов действия при компрометации

6.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документации к ним, ключевые документы подлежат поэкземплярному учету в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Заполнение, ведение и хранение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляет ответственный пользователь криптосредств.

6.2. Пользователям криптосредств выдаются все экземпляры ключевых документов, СКЗИ, эксплуатационная и техническая документация к криптосредствам под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. В случае увольнения или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, пользователи криптосредств обязаны сдать все экземпляры ключевых документов, криптосредства, эксплуатационную и техническую документацию к ним под расписку

в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов Ответственному пользователю криптосредств.

6.3. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств запрещена.

6.4. Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящиеся за ним криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

6.5. Программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются с соответствующими аппаратными средствами.

6.6. Единицей поэкземплярного учета ключевых документов является ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз регистрируют отдельно.

6.7. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа регистрируются в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

6.8. Не реже одного раза в год осуществляется проверка создаваемой приказом Министерства образования Пензенской области комиссией (в состав комиссии включается Ответственный за организацию обработки персональных данных, Ответственный пользователь криптосредств), соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации.

6.9. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

7. Порядок уничтожения криптосредств

7.1. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой

информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

7.2. Криптоключи (исходную ключевую информацию) стираются по технологии, принятой для соответствующих ключевых носителей многократного использования. Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

7.3. Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

7.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

7.5. СКЗИ уничтожаются (утилизируются) на основании приказа Министерства образования Пензенской области.

7.6. Подлежащие к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств. В Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов проставляется отметка об изъятии СКЗИ из аппаратных средств.

7.7. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

7.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним.

ключевых документов. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

7.9. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

7.10. Ключевые документы уничтожаются пользователями СКЗИ под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

8. Охрана, специальное оборудование и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

8.1. Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность информации, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

8.2. Спецпомещения выделяются с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

8.3. Спецпомещения оборудуются прочными входными дверями с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Двери спецпомещений должны быть постоянно закрыты на замок и открываться только для санкционированного прохода, оборудованы приспособлениями для опечатывания или техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

8.4. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, оснащаются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения. Для предотвращения просмотра извне спецпомещений окна должны быть защищены.

8.5. По окончании рабочего дня спецпомещения должны быть закрыты, опечатаны. Ключи от спецпомещений нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в помещение. Дубликаты ключей от входных дверей

спецпомещений хранятся в опечатанной упаковке в сейфе Ответственного пользователя криптосредств.

8.6 Периодический контроль за состоянием технических средств охраны (при их наличии) проводится Ответственным пользователем криптосредств совестно с представителем службы охраны с отметкой в Журнале контроля состояния охранной сигнализации.

8.7. Режим охраны помещений в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, определен в документации о внутрипропускном и объектовом режимах в Министерстве образования Пензенской области.

9. Порядок доступа к хранилищам криптосредств

9.1. Пользователи криптосредств хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в металлических хранилищах (ящиках, шкафах), сейфах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

9.2. Металлические хранилища (сейфы), предназначенные для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов (далее – хранилища) должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

9.3. Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения, в случае компрометации действующих ключевых документов.

9.4. Все ключи от механических замков хранилищ нумеруются и учитываются Ответственным пользователем криптосредств в Журнале учета металлических хранилищ (сейфов).

9.5. Рабочий ключ от хранилища предоставляется сотруднику, ответственному за данное хранилище, с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов)).

9.6. Дубликаты ключей от хранилищ в опечатанной упаковке хранятся в сейфе Ответственного пользователя криптосредств Дубликаты ключей от хранилища Ответственного пользователя криптосредств передаются на хранение министру образования Пензенской области под расписку в Журнале учета металлических хранилищ (сейфов).

9.7. При необходимости доступа к содержимому хранилища сотрудник, ответственный за данное хранилище, проверяет его целостность, открывает механический замок с использованием ключа, а по окончании рабочего дня закрывает и опечатывает хранилище, за которое он ответственен.

9.8. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников, ответственных за данные е хранилища.

9.9. При утрате ключа от хранилища пользователь криптосредства немедленно уведомляет Ответственного пользователя криптосредств и непосредственного руководителя структурного подразделения Министерства образования Пензенской области.

9.10. Замок от данного хранилища необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь криптосредств.

9.11. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилище посторонних лиц, о случившемся немедленно сообщается Ответственному пользователю криптосредств и министру образования Пензенской области. Ответственный пользователь криптосредств должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств, составить акт и принять, при необходимости, меры к локализации последствий.

10. Ответственность пользователей криптосредств

Ответственный пользователь криптосредств и пользователи криптосредств несут ответственность за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для защиты конфиденциальной информации, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Положению по использованию средств
криптографической защиты информации
в Министерстве образования Пензенской области

Журнал
ознакомления сотрудников с нормативными правовыми актами Российской Федерации и локальными актами Министерства образования Пензенской области по обеспечению безопасности информации с использованием криптосредств

Журнал начат _____

Журнал окончен ____ - ___

Листов (_____)

№ п/п	ФИО сотрудника	Занимаемая должность	Дата ознакомления	Подпись за ознакомление									Примечание
				ФЗ от 06.04.2011 №63-ФЗ	Приказ ФАПСИ от 13.06.2001 №152	Приказ ФСБ от 09.02.2005 №66 (Положение ПКЗ-2005)	Приказ ФСБ От 10.07.2014 №378	Приказ ФСБ От 18.03.2025 №117	Положение по использованию средств криптографической защиты информации	Инструкция ответственного пользователя средств криптографической защиты информации	Инструкция пользователя средств криптографической защиты информации	Эксплуатационная и техническая документация к криптосредству	
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Приложение № 2
к Положению по использованию средств
криптографической защиты информации в
Министерстве образования Пензенской области

Заключение
о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации

_____
(должность, Фамилия, имя, отчество сотрудника)

_____

_____
(основание для подготовки)

_____
(наименование криптосредства)

Подготовка начата _____ , окончена _____

Подготовка проводилась в соответствии с требованиями эксплуатационной и технической документации к криптосредству

Заключение:
Допустить пользователя к самостоятельной работе со средствами криптографической защиты информации

_____
(наименование криптосредства)

С заключением ознакомлен (а)

_____ _____
(подпись обучавшегося) (Фамилия, Инициалы)

Ответственный пользователь криптосредств:

_____ _____
(подпись) (Фамилия, Инициалы)

«____» _____ 20__г

Приложение № 3
к Положению по использованию средств
криптографической защиты информации в
Министерстве образования Пензенской области

АКТ №_____
установки и ввода в эксплуатацию средства криптографической защиты информации (СКЗИ)

«_____» _____ 20___ г. г. _____

_____ __(
(наименование должности ФИО лица, устанавливающего СКЗИ)

_____ __
и

_____
(наименование должности ФИО пользователя СКЗИ организации, в которой устанавливается СКЗИ)

_____

на основании договора от «__» _____ 20__ г., заключенного между

_____
(указываются реквизиты договора и наименование сторон по договору, в случае отсутствия лицензии на данный

_____
вид деятельности)
составили настоящий акт о том, что средство криптографической защиты информации установлено и введено в эксплуатацию в Министерстве образования Пензенской области в соответствии с требованиями эксплуатационной и технической документации:

Место установки	Наименование СКЗИ	Серийный номер оборудования (при наличии)	Регистрационный номер СКЗИ
Адрес: г. _____ ул. _____ дом № _____ корп._____ помещение № _____			

Наименование должности, ФИО лица организации, осуществлявшего установку СКЗИ

_____/_____/
(подпись) ФИО

М.П.

Наименование должности, ФИО пользователя СКЗИ Министерства образования Пензенской области

_____/_____/
(подпись) ФИО

М.П.

Приложение № 4
к Положению по использованию средств
криптографической защиты информации
в Министерстве образования Пензенской области

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
Министерства образования Пензенской области

Журнал начат _____ __

Журнал окончен _____ _

Листов (_____)

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 5
к Положению по использованию средств
криптографической защиты информации
в Министерстве образования Пензенской области

Лицевой счет пользователя СКЗИ

Пользователь _____ _____ _____

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Дата получения	Примечание

Приложение № 6
к Положению по использованию средств
криптографической защиты информации
в Министерстве образования Пензенской области

Журнал

учета металлических хранилищ (сейфов)
в Министерстве образования Пензенской области

Журнал начат _____ _____

Журнал окончен _ _____

Листов (___ ____)

Тип хранилища _____ _____

(сейф. металлический шкаф)

Заводской номер _____ _____

Инвентарный номер___ _____

Количество ключей и их номера _____ _____

№ п/п	Местонахождение хранилища	Фамилия и инициалы ответственного	Расписка в получении ключей и дата	Место нахождения дубликатов ключей, расписка за получение и дата	№ печати	Расписка в обратном приеме ключей и дата	Примечание
1	2	3	4	5	6	7	8

Приложение № 7
к Положению по использованию средств
криптографической защиты информации в
Министерстве образования Пензенской области

Акт №_____
проверки соблюдения условий использования
средств криптографической защиты информации

г. _____ «_____» _____ _____ г.

Комиссия в составе:
Председатель комиссии: _____
(должность. ФИО)

Члены комиссии: _____
(должность. ФИО)

_____
(должность. ФИО)

на основании _____ произвела проверку
(приказ о назначении комиссии)

соблюдения условий использования криптосредств в Министерстве образования Пензенской области в соответствии с требованиями Положения по использованию средств криптографической защиты информации.

В ходе работы комиссии установлено:

1. Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к ним в электронном виде и на бумажных носителях согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера) _____
_____ в наличии;
(оказались/не оказались)

2. Криптосредства, установленные на технические средства пользователей согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера) _____ в наличии _____ ;
(оказались/ не оказались)

3. Ключевые документы пользователей криптосредств согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера _____)
_____ в наличии;
(оказались/не оказались)

4. Лицевые счета пользователей криптосредств находятся в _____ состоянии;
(актуальном /неактуальном)

5. Перечень лиц, допущенных к работе со средствами криптографической защиты информации в Министерстве образования Пензенской области, утвержден приказом от _____ №___ и находится в _____ состоянии;
(актуальном /неактуальном)

6. Перечень Помещений, в которых размещены используемые СКЗИ, в которых размещены используемые СКЗИ, хранятся СКЗИ (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в Министерстве образования Пензенской области утвержден приказом от _____ №___ и находится в _____ состоянии;
(актуальном /неактуальном)

7. В Помещениях, в которых размещены используемые СКЗИ, хранятся СКЗИ (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, требования по обеспечению режима, препятствующего возможности неконтролируемого проникновения или пребывания в них _____;
(выполняются/не выполняются)

8. Режим хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документацию к криптосредствам, ключевых документов в металлических хранилищах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, их непреднамеренное уничтожение _____;
(соблюдается /не соблюдается)

9. Металлические хранилища (сейфы) пользователей криптосредств и ключи от них согласно Журналу учета металлических хранилищ (сейфов) (Учетные номера _____) _____ в наличии;
(оказались/не оказались)

10. Техническое состояние СКЗИ и оборудование, функционирующее с СКЗИ требованиям эксплуатационной документации на СКЗИ, информационную систему и систему защиты информации _____;
(соответствует/ не соответствует)

11. Пользователи криптосредств с нормативными правовыми актами Российской Федерации и локальными актами Министерства образования Пензенской области _____;
(ознакомлены/ не ознакомлены)

12. Пользователями криптосредств требования правил хранения, использования и защиты СКЗИ _____;
(выполняются / не выполняются)

13. Случаи компрометации СКЗИ _____.
(установлены/ не установлены)

Действия по устранению причин и локализации последствий компрометации СКЗИ:

_____

(в случае установления фактов компрометации СКЗИ)

В ходе работы комиссии выявлены следующие недостатки:

_____

_____

_____

Заключение комиссии:

Соблюдение условий использования средств криптографической защиты информации _____ требованиям к условиям использования
(соответствует/ не соответствует)

в Министерства образования Пензенской области.

Председатель комиссии:

_____	_____	_____
(должность)	(подпись)	(ФИО)

Члены комиссии:

_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)

Приложение № 8
к Положению по использованию средств
криптографической защиты информации
в Министерстве образования Пензенской области

Технический (аппаратный) журнал

Журнал начат _____

Журнал окончен _____

Листов(_____)

№ п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тим ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	1

Приложение № 22
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-04

Порядок доступа
в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1 Настоящий Порядок доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в (далее – Порядок) определяет в Министерстве образования Пензенской области порядок осуществления доступа в помещения Министерства образования Пензенской области, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, (далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

1.2. Перечень нормативных правовых актов, на основании которых разработан Порядок:

- приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

1.3. Ответственный за организацию обработки персональных данных, ответственный пользователь криптосредств, пользователи криптосредств, а также сотрудники Министерства образования Пензенской области, находящиеся в данных помещениях в связи с исполнением своих трудовых (служебных) обязанностей в соответствии с утвержденным приказом Министерства образования Пензенской области «Об утверждении Перечня лиц, имеющих право доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители

ключевой, аутентифицирующей и парольной информации криптосредств» должны быть ознакомлены с настоящей Порядком под подпись.

2. Организация режима обеспечения безопасности в Помещениях

2.1. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

2.2. Помещения должны оснащаться входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода, а также опечатывание Помещений по окончании рабочего дня или оборудования Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений.

2.3. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, оснащаются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения. Для предотвращения просмотра извне Помещений окна должны быть защищены.

2.4. Перечень Помещений определен приказом Министерства образования Пензенской области «Об утверждении Перечня помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Министерстве образования Пензенской области».

3. Правила доступа в Помещения в рабочее, нерабочее время, в нештатных ситуациях

3.1. Доступ в Помещения в рабочее время имеют сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, в соответствии с приказом Министерства образования Пензенской области «Об утверждении Перечня лиц, имеющих право доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в Министерстве образования Пензенской области».

3.2. В нерабочее время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных министром образования Пензенской области.

3.3. Бесконтрольное нахождение в Помещениях посторонних лиц в рабочее и нерабочее время запрещается.

3.4. Министр образования Пензенской области и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

3.5. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю структурного

подразделения Министерства образования Пензенской области и ответственному пользователю криптосредств.

3.6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать непосредственному руководителю структурного подразделения Министерства образования Пензенской области.

3.7. Сотрудники территориальных подразделений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой медицинской помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Министерства образования Пензенской области.

4. Ответственность

4.1 Сотрудники Министерства образования Пензенской области несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 23
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2016 № 99/01-04

Инструкция
ответственного пользователя средств криптографической защиты информации в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации (далее - Инструкция) определяет в Министерстве образования Пензенской области права и обязанности ответственного за организацию эксплуатации средств криптографический защиты информации (далее – ответственный пользователь криптосредств), используемых для обеспечения безопасности информации (в том числе персональных данных), содержащей сведения, не составляющие государственной тайну (далее – защищаемая информация), в информационных системах Министерства образования Пензенской области.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
СКЗИ, криптосредство	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
	несанкционированным лицам и (или) процессам	
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

1.4. Ответственный пользователь криптосредств назначается приказом Министерства образования Пензенской области. При смене Ответственного пользователя криптосредств должны быть внесены соответствующие изменения в приказ «О назначении ответственного пользователя криптосредств в Министерстве образования Пензенской области.

1.5. Ответственный пользователь криптосредств должен быть ознакомлен с настоящей Инструкцией под подпись.

2. Обязанности ответственного пользователя криптосредств

2.1. Ответственный пользователь криптосредств при эксплуатации СКЗИ должен выполнять требования нормативных и правовых актов Российской Федерации, Положения по использованию средств криптографической защиты информации, настоящей Инструкции, эксплуатационной, технической, и организационно-распорядительной документации для информационных систем Министерства образования Пензенской области, в том числе для СКЗИ.

2.2. Ответственный пользователь криптосредств обязан:

- проводить обучение пользователей криптосредств правилам работы с криптосредствами с оформлением Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и отметкой в Журнале ознакомления сотрудников с нормативными правовыми актами

Российской Федерации и локальными актами Министерства образования Пензенской области по обеспечению безопасности защищаемой информации с использованием криптосредств;

- вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с документальным оформлением в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- контролировать заполнение Акта установки и ввода в эксплуатацию средств криптографической защиты информации (Приложение №3 к Положению по использованию средств криптографической защиты информации в Министерстве образования Пензенской области, делать отметку Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- хранить Акты установки и ввода в эксплуатацию средств криптографической защиты информации;

- организовать надежное хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации, ключей от металлических хранилищ (сейфов);

- вести учет лиц, допущенных к работе с СКЗИ. Формировать и актуализировать приказом Министерства образования Пензенской области Перечень лиц, допущенных к работе со средствами криптографической защиты информации в Министерстве образования Пензенской области;

- заводить и вести лицевые счета на каждого пользователя СКЗИ, в котором регистрировать числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы;

- выдавать СКЗИ, эксплуатационную и техническую документацию, ключевые документы пользователям криптосредств с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- принимать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя криптосредств при их увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- контролировать результаты уничтожения ключевых документов пользователями СКЗИ после окончания срока действия, не позднее 10 дней после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ (Факт уничтожения оформляется под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- вести учет металлических хранилищ (сейфов), предназначенных для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к

криптосредствам, ключевых документов с документальным оформлением в Журнале учета металлический хранилищ (сейфов);

- хранить в опечатанной упаковке дубликаты ключей от металлических хранилищ (сейфов);

- передать дубликаты ключа от металлического хранилища (сейфа) ответственного пользователя криптосредств министру образования Пензенской области с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов);

- хранить в опечатанной упаковке дубликаты ключей от входных дверей спецпомещений в металлическом хранилище (сейфе);

- выдавать ключ от металлического хранилища (сейфа) пользователю криптосредства с документальным оформлением (под расписку в Журнале учета металлический хранилищ (сейфов);

- принимать ключ от металлического хранилища (сейфа) при увольнении или отстранении от исполнения обязанностей сотрудника, связанных с использованием СКЗИ, с документальным оформлением в Журнале учета металлический хранилищ (сейфов);

- проводить не реже одного раза в год проверку создаваемой приказом Министерства образования Пензенской области комиссии (в состав комиссии включается Ответственный за организацию обработки персональных данных, Ответственный пользователя криптосредств), соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации;

- осуществлять контроль за соблюдением условий использования СКЗИ, предусмотренной эксплуатационной и технической документации к ним, обеспечением функционирования и безопасности СКЗИ и ключевых документов в пределах своих полномочий;

- осуществлять контроль за выполнением пользователями СКЗИ требований к обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах с использованием СКЗИ;

- осуществлять контроль за ведением пользователем криптосредства технического (аппаратного) журнала в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ;

- осуществлять контроль за установлением режима охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время;

- проводить периодический контроль за состоянием технических средств охраны (при их наличии) совместно с представителем службы охраны или дежурным по организации с отметкой в Журнале контроля состояния охранной сигнализации;

- осуществлять контроль за проведением работ по размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ в спецпомещениях пользователей СКЗИ;

- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ пользователей криптосредств;

- контролировать наличие и актуальность Перечня помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом Министерства образования Пензенской области;

- контролировать наличие и актуальность Перечня лиц, имеющих право доступа в Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом Министерства образования Пензенской области;

- соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения трудовых (служебных) обязанностей, в том числе сведений о криптоключах, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;

- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах Министерства образования Пензенской области с использованием СКЗИ;

- немедленно уведомлять министра образования Пензенской области о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

- своевременно выявлять попытки посторонних лиц получить сведения о защищаемой информации, об используемых криптосредствах или ключевых документах к ним;

- организовывать мероприятия по розыску и локализации последствий компрометации защищаемой информации в информационных системах, передаваемой (хранящейся) с использованием СКЗИ.

3. Права ответственного пользователя криптосредств

3.1. Ответственный пользователь СКЗИ имеет право:

- требовать от пользователей СКЗИ соблюдения положений Положения по использованию средств криптографической защиты информации и Инструкции пользователя средств криптографической защиты информации;

- обращаться к министру с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

- инициировать проведение служебных проверок по фактам нарушения порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ защищаемой информации.

4. Ответственность

4.1. Ответственный пользователь криптосредств несет ответственность в соответствии с действующим законодательством Российской Федерации за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для обеспечения безопасности защищаемой информации при ее обработке в информационных системах Министерства образования Пензенской области.

Приложение № 24
Утверждено
приказом Министерства образования
Пензенской области
от 26.02.2026 № 99/01-04

Инструкция
пользователя средств криптографической защиты информации в Министерстве образования Пензенской области

Оглавление

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (далее - Инструкция) определяет в Министерстве образования Пензенской области (действия и обязанности сотрудников при обработке информации (в том числе персональных данных), содержащей сведения, не составляющие государственной тайну (далее – защищаемая информация), в информационных системах Министерства образования Пензенской области с использованием средств криптографической защиты информации.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
СКЗИ, криптосредство	Средство криптографической защиты информации

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержден ФСТЭК России 11.02.2014
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
	несанкционированным лицам и (или) процессам	
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

- приказ Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

- приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 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 требованиям к защите персональных данных для каждого из уровней защищенности»;

- приказ Федеральной службы безопасности Российской Федерации от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

1.4. Пользователи криптосредств допускаются к работе с СКЗИ приказом Министерства образования Пензенской области с последующим обязательным ознакомлением Ответственного пользователя криптосредств.

1.5. Пользователи криптосредств должны быть ознакомлены с настоящей Инструкцией, Положением по использованию средств криптографической защиты информации в Министерстве образования Пензенской области под подпись.

2. Обязанности Пользователя криптосредств

2.1. Пользователь криптосредств при эксплуатации СКЗИ, используемых для обеспечения безопасности защищаемой информации в информационных системах Министерства образования Пензенской области должен выполнять требования нормативных и правовых актов Российской Федерации, Положения по использованию средств криптографической защиты информации, настоящей Инструкции, эксплуатационной, технической, и организационно-распорядительной документации, в том числе для СКЗИ.

2.2. Пользователь криптосредств обязан:

- пройти обучение правилам работы с СКЗИ и знакомиться с Положением по использованию средств криптографической защиты информации, Инструкцией пользователя криптосредств и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности защищаемой информации с использованием криптосредств.

- получить у Ответственного пользователя криптосредств СКЗИ, эксплуатационную и техническую документацию, ключевые документы с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);

- получить у Ответственного пользователя криптосредств ключ от металлического хранилища (сейфа) для хранения инсталлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением (под расписку в Журнале учета металлический хранилищ (ссйфов));

- хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Хранить резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, раздельно от действующих ключевых документов;

- вести технический (аппаратный) журнал в случае, если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ. Регистрировать в техническом (аппаратном) журнале разовый ключевой носитель или электронную запись соответствующего криптоключа, а также отражать данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. Самостоятельно уничтожать разовые ключевые носители, электронные записи ключевой информации, соответствующей выведенным из действия криптоключам и делать об этом отметку под расписку в техническом (аппаратном) журнале;

- соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения должностных обязанностей, в том числе сведений о криптоключах, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;

- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой в информационных системах Министерства образования Пензенской области с использованием СКЗИ;

- контролировать целостность печатей (пломб) на системных блоках технических средств с установленными СКЗИ;

- осуществлять уничтожение ключевых документов с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) после окончания срока действия, не позднее 10 суток после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ;

- сообщать Ответственному пользователю криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- сдать с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы Ответственному пользователю криптосредств при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- сдать с документальным оформлением (под расписку в Журнале учета металлический хранилищ (сейфов)) ключ от металлического хранилища (сейфа) Ответственному пользователю криптосредств при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- немедленно уведомлять Ответственного пользователя криптосредств и министра образования Пензенской области о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

- немедленно выводить из действия криптоключи, в отношении которых возникло подозрение в компрометации, с уведомлением Ответственного пользователя криптосредств и министра образования Пензенской области с последующим их уничтожением.

2.3. Пользователям криптосредств запрещается:

- разглашать информацию о ключевых документах и информацию ограниченного доступа;

- вносить любые изменения в программное обеспечение СКЗИ, изменять настройки СКЗИ;

- допускать к использованию СКЗИ посторонних лиц;

- осуществлять вскрытие системных блоков технических средств с установленными СКЗИ, подключать к ним дополнительные устройства;

- использовать криптоключи, в отношении которых возникло подозрение в компрометации;

- оставлять ключевые носители без контроля, выносить их за пределы служебных помещений;

- снимать копии с ключевых документов;

- записывать на ключевой носитель информацию, не предусмотренную правилами пользования СКЗИ (служебные файлы, текстовые и мультимедийные файлы и т.п.);

- допускать установку ключевых документов в другие ПЭВМ;

- выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.).

3. Ответственность

3.1. Пользователь криптосредств несет ответственность в соответствии с действующим законодательством Российской Федерации за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для обеспечения безопасности защищаемой информации при ее обработке в информационных системах Министерства образования Пензенской области.