АКАДЕМИЯ СОЦИАЛЬНОГО УПРАВЛЕНИЯ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
«АКАДЕМИЯ СОЦИАЛЬНОГО УПРАВЛЕНИЯ»

ПРИКАЗ

21.02.2022 № 235-04

г. Мытищи

О мерах по обеспечению информационной безопасности в РЦОИ

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы безопасности 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 требований к защите персональных данных для каждого из уровней защищенности», приказом Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом 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»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за эксплуатацию информационных систем персональных данных в Региональном центре обработки информации АСОУ (далее - РЦОИ) Репало А.В., руководителя РЦОИ.

2. Назначить ответственным за защиту информации ограниченного доступа в РЦОИ Никулину А.В., заместителя руководителя РЦОИ.

3. Назначить ответственным за организацию обработки персональных данных в РЦОИ Нерослова А.С., заместителя руководителя РЦОИ.

4. Возложить функции и обязанности администратора информационных систем персональных данных РЦОИ на Алешина К.В., начальника отдела информационных технологий РЦОИ.

5. Возложить функции и обязанности администратора информационной безопасности РЦОИ на:

5.1. Щеглова М.А., начальника отдела технического сопровождения ГИА РЦОИ, в части обеспечения безопасности информации при работе с персональными данными и иной информацией ограниченного доступа в РИС ГИА-11;

5.2. Голубева А.И., электроника 2 категории отдела технического сопровождения ГИА-9 РЦОИ, в части обеспечения безопасности информации при работе с персональными данными и иной информацией ограниченного доступа в РИС ГИА-9.

6. Назначить ответственным за эксплуатацию средств криптографической защиты информации в РЦОИ Насырова Р.Р., инженера отдела информационных технологий РЦОИ.

7. Утвердить:

7.1. Концепцию безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ;

7.2. Положение по организации и проведении работ по обеспечению безопасности персональных данных при их обработке в РЦОИ;

7.3. Политику безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ;

7.4. Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения в целях обеспечения защиты технических средств;

7.5. Положение о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ;

7.6. Порядок доступа работников РЦОИ в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, и размещены информационные системы;

7.7. Перечень процессов и сведений ограниченного доступа, обрабатываемых в РЦОИ;

7.8. Описание технологического процесса обработки информации в информационных системах персональных данных РЦОИ;

7.9. Инструкцию ответственного за эксплуатацию информационных систем персональных данных;

7.10. Инструкцию ответственного за защиту информации ограниченного доступа;

7.11. Инструкцию администратора информационных систем персональных данных;

7.12. Инструкцию администратора информационной безопасности (ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных);

7.13. Инструкцию ответственного за организацию обработки персональных данных;

7.14. Инструкцию по работе пользователей в информационных системах персональных данных;

7.15. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей;

7.16. Правила обработки персональных данных;

7.17. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

7.18. Регламент выявления инцидентов информационной безопасности и реагирование на них;

7.19. Положение о порядке рассмотрения запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных;

7.20. Инструкцию о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных;

7.21. Положение о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники;

7.22. Инструкцию по организации резервного копирования;

7.23. Инструкцию по идентификации, аутентификации;

7.24. Инструкцию по управлению доступом к информации;

7.25. Инструкцию по защите машинных носителей информации;

7.26. Инструкцию по управлению событиями информационной безопасности;

7.27. Инструкцию по организации антивирусной защиты;

7.28. Инструкцию по организации парольной защиты;

7.29. Инструкцию по управлению программным обеспечением;

7.30. Инструкцию по управлению конфигурацией в ИСПДн;

7.31. Инструкцию по контролю защищенности информации;

7.32. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований;

7.33. Инструкцию ответственного за эксплуатацию средств криптографической защиты информации в информационных системах РЦОИ;

7.34. Инструкцию пользователя средств криптографической защиты информации;

7.35. Правила по работе с средствами криптографической защиты информации;

7.36. Инструкцию по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты

информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах РЦОИ, и криптоключами к ним;

7.37. Порядок доступа работников РЦОИ в помещения, в которых ведется обработка информации ограниченного доступа и расположены средства криптографической защиты информации;

7.38. Инструкцию по восстановлению конфиденциальной связи в случае компрометации действующих ключей к криптосредствам в информационных системах РЦОИ;

7.39. Форму журнала учета средств защиты информации;

7.40. Форму журнала учета паролей пользователей государственной информационной системы «АИС РЦОИ РИС МО»;

7.41. Форму журнала учета паролей пользователей информационной системы персональных данных «АИС ГИА»;

7.42. Форму журнала учета печати конфиденциальной информации;

7.43. Форму журнала учета выдачи аппаратных лицензионных электронных ключей ABBYY;

7.44. Форму журнала активации электронных ключей;

7.45. Форму журнала проведения инструктажей по информационной безопасности.

8. Приказ довести до всех работников РЦОИ в части их касающейся под подпись.

9. Признать утратившим силу приказ АСОУ от 11.02.2020 № 65-07 «О мерах по обеспечению информационной безопасности в деятельности РЦОИ».

10. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор АСОУ **А.А. Лубский**

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Концепция
безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ

1. Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не распространять их без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор персональных данных – 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.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъекты персональных данных – работники, обучающиеся, участники единого государственного экзамена, граждане, привлекаемые к проведению государственной итоговой аттестации, члены предметных комиссий, общественные наблюдатели, слушатели и другие лица.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Введение

Настоящая Концепция безопасности персональных данных, обрабатываемых в информационных системах персональных данных и государственных информационных системах (далее вместе – информационные системы персональных данных) РЦОИ (далее – Концепция), является официальным документом, в котором определена система взглядов на обеспечение безопасности персональных данных.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов при обработке информации в целом и персональных данных в частности, а также необходимостью соответствия требованиям законодательства Российской Федерации в области защиты персональных данных.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных в РЦОИ. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз безопасности персональных данных и разработку системы защиты персональных данных с позиции комплексного применения технических и организационных мер, и средств защиты.

Под безопасностью персональных данных понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам персональных данных) или инфраструктуре. Задачи безопасности персональных данных сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению безопасности персональных данных

обрабатываемых в информационных системах РЦОИ, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности персональных данных в информационных системах персональных данных РЦОИ;

– принятия управленческих решений, разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса, согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз персональных данных;

– координации деятельности при проведении работ по развитию и эксплуатации информационных систем персональных данных с соблюдением требований обеспечения безопасности персональных данных;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных в информационных системах РЦОИ.

Область применения Концепции распространяется на эксплуатацию технических и программных средств информационных систем персональных данных, в которых осуществляется автоматизированная обработка персональных данных, и сопровождение, обслуживание и обеспечение нормального функционирования информационных систем персональных данных.

Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных.

3. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных РЦОИ, в соответствии с Перечнем информационных систем персональных данных в РЦОИ. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности персональных данных.

Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

Структура, состав и основные функции системы защиты персональных данных определяются исходя из уровня защищенности персональных данных в информационных системах персональных данных. Система защиты персональных

данных включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

– конфиденциальность информации (защита от несанкционированного ознакомления);

– целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания системы защиты персональных данных включают:

– предпроектная стадия, включающая предпроектное обследование информационной системы персональных данных, разработку технического задания на ее создание;

– стадия проектирования (разработки проектов) и реализации информационных систем персональных данных, включающая разработку системы защиты персональных данных в составе информационных систем персональных данных;

– стадия ввода в действие системы защиты персональных данных, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия информационной системы персональных данных требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) локальных нормативных актов в области обработки и защиты персональных данных в информационных системах персональных данных РЦОИ.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

4. Цель и задачи системы защиты персональных данных

Основной целью системы защиты персональных данных является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Для достижения основной цели система защиты персональных данных в информационных системах персональных данных должна обеспечивать эффективное решение следующих задач:

– защиту от вмешательства в процесс функционирования информационной системы персональных данных посторонних лиц (возможность использования объектов вычислительной техники и доступ к его ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационной системы персональных данных (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационной системы персональных данных для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в информационных системах персональных данных;
- средствам вычислительной техники информационной системы персональных данных;
- аппаратным, программным и криптографическим средствам защиты, используемым в информационных системах персональных данных;

– регистрацию действий пользователей при использовании защищаемых ресурсов информационных систем персональных данных в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

– контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

– защиту от несанкционированной модификации и контроль целостности используемых в информационных системах персональных данных программных средств, а также защиту системы от внедрения несанкционированных программ;

– защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

– защиту персональных данных хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

– обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

– своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

5. Перечень элементов информационных систем персональных данных, подлежащих защите

Обработка персональных данных в РЦОИ производится в информационных системах персональных данных.

Перечень информационных систем персональных данных определяется приказом АСОУ.

Персональные данные, обрабатываемые в информационных системах персональных данных, являются сведениями конфиденциального характера и подлежат защите. Перечень персональных данных, подлежащих защите, определен в Правилах обработки персональных данных.

Кроме того, в информационных системах персональных данных защите подлежат:

– технологическая информация;
– программно-технические средства обработки;
– средства защиты персональных данных;
– каналы информационного обмена и телекоммуникации;
– объекты и помещения, в которых размещены компоненты информационной системы персональных данных.

6. Классификация пользователей информационных систем персональных данных

Пользователем информационной системы персональных данных является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем информационной системы персональных данных является работник РЦОИ, имеющий доступ к информационной системе персональных данных и ее ресурсам в соответствии с установленным порядком доступа и служебными обязанностями.

Пользователи информационной системы персональных данных делятся на следующие основные категории, уровень доступа и знаний которых отражен в Политике безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ:

– Администратор информационной системы персональных данных;
– Администратор информационной безопасности;
– Пользователь информационной системы персональных данных.

7. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности персональных данных в информационных системах персональных данных РЦОИ и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;
– системность;
– комплексность;
– непрерывность;
– своевременность;
– преемственность и непрерывность совершенствования;
– персональная ответственность;
– минимизация полномочий;

- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

7.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных РЦОИ в соответствии с действующим законодательством в области защиты персональных данных и других нормативных актов по безопасности информации, утвержденных органами государственной власти в пределах их компетенции.

Пользователи информационной системы персональных данных РЦОИ должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение требований данного порядка.

7.2. Системность

Системный подход к построению системы защиты персональных данных в РЦОИ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных в информационных системах персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

7.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств для построения целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того,

чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

7.4. Непрерывность защиты персональных данных

Защита персональных данных – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем персональных данных.

Информационные системы персональных данных должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационных систем персональных данных в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты.

7.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационной системы персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационной системы персональных данных в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

7.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы

персональных данных и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требованиях по её защите.

7.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко определен или сведен к минимуму.

7.8. Принцип минимизации полномочий

Означает предоставление пользователям минимально необходимых прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в тех целях и объемах, которые необходимы работнику для выполнения его должностных обязанностей.

7.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе, обеспечивающем деятельность информационных системах персональных данных, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие лицам, ответственным за защиту информации.

7.10. Гибкость системы защиты персональных данных

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

7.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже

разработчикам системы). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

7.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

7.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности персональных данных и должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

7.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами.

7.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации, и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

8. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

8.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся правила обращения с персональными данными, установленные действующими нормативно-правовыми актами, которые, закрепляют права и обязанности участников информационных отношений, а также устанавливают ответственность за нарушения этих правил. Правовая база создает препятствия неправомерному использованию персональных данных и является сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями системы.

8.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения вычислительной техники в стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе соответствующей организации. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

8.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования информационной системы персональных данных, использование ресурсов

информационной системы персональных данных, а также порядок взаимодействия пользователей с информационными системами персональных данных таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать Политику безопасности персональных данных, отражающую подходы к защите персональных данных, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики безопасности персональных данных в информационных системах персональных данных состоит из мер административного уровня и организационных (процедурных) мер защиты персональных данных.

К административному уровню относятся решения руководства, затрагивающие функционирование информационной системы персональных данных в целом. Эти решения закрепляются в Политике безопасности персональных данных. Примером таких решений могут быть:

– назначение администратора информационной безопасности;

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, назначение лиц, ответственных за ее реализацию;

– формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;

– принятие решений по вопросам реализации программы безопасности;

– обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные ресурсы, персонал) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем персональных данных.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики безопасности персональных данных. Эти правила определяют:

– какова область применения Политики безопасности персональных данных;

– каковы роли и обязанности должностных лиц, отвечающих за проведение Политики безопасности персональных данных, а также их ответственность;

– кто имеет права доступа к персональным данным;

– какими мерами и средствами обеспечивается защита персональных данных;

– какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

– предусматривать порядок информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;

– определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты, и другими защитными механизмами;

– организовать меры противодействия несанкционированным действиям пользователей на этапах аутентификации, идентификации, обеспечивающие гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

– регламентации доступа в помещения, где расположены элементы информационных систем персональных данных;

– порядка допуска работников к использованию ресурсов информационных систем персональных данных;

– регламентации процессов ведения баз данных и осуществления модификации информационных ресурсов;

– регламентации процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационных систем персональных данных;

– принятия инструкций ответственных лиц за обеспечение безопасности персональных данных;

– принятия инструкций пользователей информационных систем персональных данных.

–

8.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления системы охраны, включающую посты охраны, технические средства охраны, которая всеми способами, предотвращает или существенно затрудняет проникновение в здания, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, а также исключает нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

8.5. Аппаратно-программные средства защиты персональных данных

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ,

входящих в состав информационных систем персональных данных и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных в информационных системах персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационной системы персональных данных;

– средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационной системы персональных данных;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства защиты персональных данных.

Успешное применение технических средств защиты на основании принципов, изложенных в разделе 7, предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

– обеспечена физическая целостность всех компонентов информационной системы персональных данных;

– каждый работник (пользователь информационной системы персональных данных) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– в информационных системах персональных данных разработка и отладка программных средств осуществляется за пределами информационных систем персональных данных;

– все изменения конфигурации технических и программных средств информационных систем персональных данных производятся в строго установленном порядке (регистрируются и контролируются) только на основании соответствующих распоряжений;

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

– уполномоченными лицами РЦОИ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

9. Контроль эффективности системы защиты персональных данных

Контроль эффективности системы защиты персональных данных в РЦОИ должен осуществляться на периодической основе. Целью контроля эффективности

является своевременное выявление ненадлежащих режимов работы системы защиты персональных данных (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

Контроль может проводиться как администратором информационной безопасности, так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором информационной безопасности как с помощью штатных средств системы защиты персональных данных, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям безопасности.

10. Сферы ответственности за безопасность персональных данных

Сотрудники РЦОИ, ответственные за обработку персональных данных с использованием средств автоматизации назначаются приказом ректора АСОУ.

Сфера ответственности данных работников включает следующие направления обеспечения безопасности персональных данных:

– планирование и реализация мер по обеспечению безопасности персональных данных;

– анализ угроз безопасности персональных данных;

– внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности персональных данных;

– обучение и информирование пользователей информационных систем персональных данных о порядке работы с персональными данными и средствами защиты;

– предотвращение, выявление, реагирование и расследование нарушений безопасности персональных данных.

11. Модель нарушителя безопасности и Модель угроз безопасности

Описание потенциального нарушителя безопасности, угроз, вероятность их реализации, опасность и актуальность представлены в частной Модели нарушителя безопасности и частной Модели угроз безопасности персональных данных каждой информационной системы персональных данных РЦОИ.

12. Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

– федеральных законов в области обеспечения информационной безопасности и защиты информации;

– постановлений Правительства Российской Федерации;

– руководящих, организационно-распорядительных и методических документов ФСБ России, ФСТЭК России, Роскомнадзора;

– потребностей информационной системы персональных данных в средствах обеспечения безопасности информации.

13. Ожидаемый эффект от реализации Концепции

Реализация Концепции позволит:

– разработать распорядительные и нормативно-методические документы применительно к информационным системам персональных данных;

– оценить состояние безопасности персональных данных, выявить источники внутренних и внешних угроз безопасности персональных данных, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

– провести определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных;

– провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в информационных системах персональных данных;

– обеспечить необходимый уровень безопасности элементов информационных систем персональных данных, подлежащих защите.

Осуществление вышеизложенных мероприятий обеспечит создание единой, целостной и скоординированной системы защиты персональных данных и создаст условия для ее дальнейшего совершенствования.

14. Список использованных источников

1. Конституция Российской Федерации;
2. Трудовой кодекс Российской Федерации;
3. Семейный кодекс Российской Федерации;
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
5. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. 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»;
7. 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».

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Положение
по организации и проведении работ по обеспечению безопасности персональных данных при их обработке в РЦОИ

1. Общие положения

Положение по организации и проведении работ по обеспечению безопасности персональных данных при их обработке в РЦОИ (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области обеспечения безопасности персональных данных.

Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных в РЦОИ и учитывает требования основных нормативных правовых актов в области защиты персональных данных, а именно:

– Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

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

– приказа Федеральной службы по техническому и 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»;

– иных нормативных правовых актов Российской Федерации.

Положение может уточняться и корректироваться по мере необходимости. Все изменения в Положение вносятся приказом.

Ответственным за пересмотр настоящего Положения и составление рекомендаций по его изменению является ответственный за защиту информации ограниченного доступа в РЦОИ.

Все работники РЦОИ, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

Настоящее Положение вступает в силу с даты его утверждения ректором АСОУ и действует бессрочно, до замены его новым Положением.

В настоящем Положении используются следующие термины и определения:

Информация – сведения (сообщения, данные) независимо от формы их представления;

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту

персональных данных);

Субъекты персональных данных – работники, обучающиеся, участники единого государственного экзамена, граждане, привлекаемые к проведению государственной итоговой аттестации, члены предметных комиссий, общественные наблюдатели, слушатели и другие лица.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Доступ к информации – возможность получения информации, содержащей персональные данные и ее использования;

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Конфиденциальность персональных данных – обязательное для соблюдения работниками, иными получившим доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

В соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» РЦОИ является оператором персональных данных.

РЦОИ осуществляется обработка персональных данных следующих категорий

субъектов персональных данных: работников, обучающихся, участников единого государственного экзамена (за исключением обучающихся), граждан, привлекаемых к проведению государственной итоговой аттестации, членов предметных комиссий, общественных наблюдателей, слушателей и других лиц, данные которых получены в процессе осуществления своей деятельности.

Цель данного Положения – определение порядка организации и проведения работ в РЦОИ для построения эффективной системы защиты информации от несанкционированного доступа (далее – НСД), и её последующей эксплуатации. В частности, с целью обеспечения защиты прав и свобод субъектов персональных данных при обработке их персональных данных в информационных системах РЦОИ.

Информационная система персональных данных является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, относящиеся к специальным, биометрическим и общедоступным категориям персональных данных.

Положение предназначено для практического использования должностными лицам, ответственными за защиту информации.

Требования настоящего Положения распространяются на все процессы обработки информации в РЦОИ с использованием средств автоматизации и являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами РЦОИ.

За общее состояние защиты информации в РЦОИ отвечает его руководитель.

Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях РЦОИ возлагается на руководителей этих подразделений.

Руководители структурных подразделений:

– лично отвечают за защиту информации в структурных подразделениях, сохранность машинных и иных носителей информации;

– организуют выполнение мероприятий по защите информации при использовании технических средств;

– участвуют в определении мест установки и количества АРМ, необходимых для обработки информации;

– участвуют в определении правил разграничения доступа к информации в информационных системах, используемых в РЦОИ.

Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с Инструкцией по работе пользователей в информационной системе персональных данных, утвержденной ректором АСОУ.

Проведения работ по защите информации в информационных системах, с помощью встроенных средств безопасности, сертифицированных лицензионных операционных систем и антивирусного программного обеспечения, возлагается на администратора информационных систем персональных данных.

При необходимости для оказания услуг в области аттестации информационных систем можно привлекать специализированные организации, имеющие лицензию на этот вид деятельности.

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту информации ограниченного доступа.

Все работники, допущенные к обработке информации, обязаны соблюдать конфиденциальность информации в течение срока действия трудового договора.

Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

2. Организация работ по обеспечению безопасности персональных данных

Под организацией работ по обеспечению безопасности персональных данных в РЦОИ понимается формирование и всестороннее обеспечение реализации совокупности согласованных по целям, задачам организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности персональных данных и осуществляемых в целях:

– предотвращения возможных (потенциальных) угроз безопасности персональных данных;

– нейтрализации и/или парирования реализуемых угроз безопасности персональных данных;

– ликвидации последствий реализации угроз безопасности персональных данных.

Целью технической защиты информации в РЦОИ является предотвращение НСД к информации при её обработке в информационных системах, связанного с действиями нарушителей, включая пользователей информационных систем, реализующих угрозы непосредственно в информационных системах, а также нарушителей, не имеющих доступ к таким системам, реализующих угрозы из сетей международного информационного обмена с целью разрушения, искажения, уничтожения, блокировки и несанкционированного копирования информации.

Организация и выполнение мероприятий по обеспечению безопасности персональных данных, обрабатываемых с использованием средств автоматизации, осуществляются в рамках системы защиты персональных данных в информационной системе персональных данных в процессе ее создания или модернизации.

Система защиты персональных данных представляет собой совокупность организационных мер и технических средств зашиты информации, а также используемых в информационной системе персональных данных информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности персональных данных.

Структура, состав и основные функции системы защиты персональных данных определяются в соответствии с уровнем защищенности персональных данных при их обработке в информационной системе персональных данных и моделью угроз и нарушителя безопасности персональных данных.

Замыслом достижения целей защиты информационной системы от НСД является обеспечение защиты информации путем выполнения требований нормативных правовых актов, принятыми ФСТЭК России в исполнении части 4 статьи 19 Федерального закона «О персональных данных» для третьего уровня защищённости персональных данных.

Целями организационных мероприятий по защите информации в РЦОИ являются:

– организация режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (установка замков, систем сигнализации и видеонаблюдения и т.п.);

– исключение непреднамеренных действий работников РЦОИ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации информационных систем;

– сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием информационных систем (физический вынос информации на электронных или бумажных носителях);

– исключение ознакомления работников с такими сведениями, если это не предусмотрено их должностными обязанностями;

– обеспечение безопасного хранения материальных носителей персональных данных (закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.);

– использование средств гарантированного уничтожения материальных носителей персональных данных (средства измельчения, сжигания, размагничивания и т.п.);

– использование систем пожарной сигнализации и пожаротушения.

3. Охраняемые сведения и актуальные угрозы

Охраняемые сведения – информация, обрабатываемая в информационных системах РЦОИ в соответствии с Перечнем процессов и сведений ограниченного доступа, обрабатываемых в РЦОИ.

Объектами защиты являются:

– информационные системы различного назначения, участвующие в обработке информации, в соответствии с Перечнем информационных систем персональных данных в РЦОИ;

– помещения, где установлены информационные системы (контролируемая зона, утвержденная приказом ректора АСОУ. Технические средства, позволяющие осуществлять обработку персональных данных, размещаются в пределах контролируемой зоны).

В соответствии с моделями угроз и нарушителя безопасности персональных данных в информационных систем персональных данных актуальными являются только угрозы НСД к информационным ресурсам информационной системы с

целью получения, разрушения, искажения и блокирования информации. Данный вид угроз в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» относится к угрозам 3-го типа.

Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности реализуются без применения сложных технических средств:

– обрабатываемой в информационных системах от НСД нарушителей и непреднамеренных действий сотрудников РЦОИ;

– выводимой на экраны мониторов компьютеров;

– хранящейся на физических носителях;

– циркулирующей в локальных вычислительных сетях РЦОИ при несанкционированном подключении к данной сети.

4. Выполнение работ по обеспечению безопасности персональных данных

В целях выполнения работ по обеспечению безопасности персональных данных в РЦОИ определяется состав и перечень мер, необходимых для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных РЦОИ.

К таким мерам могут, в частности, относиться:

– назначение ответственных лиц за организацию защиты информации;

– принятие локальных актов, определяющих политику в отношении обработки персональных данных в РЦОИ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

Приказом ректора АСОУ назначаются:

– уполномоченное лицо, ответственное за защиту информации ограниченного доступа;

– уполномоченное лицо, ответственное за организацию обработки персональных данных;

– уполномоченное лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных (администратор информационных систем персональных данных);

– уполномоченное(ые) лицо(а), ответственное(ые) за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными и поддержание необходимого уровня информационной безопасности (администратор информационной безопасности);

– уполномоченные лица, допущенные к обработке персональных данных.

Указанные лица исполняют свои обязанности по обеспечению безопасности обрабатываемых персональных данных в соответствии с требованиями своих должностных инструкций и иных нормативных правовых актов Российской Федерации и локальных актов АСОУ.

Доступ к персональным данным регламентируется Положением о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ.

Работники РЦОИ, участвующие в обработке персональных данных, должны быть проинформированы:

– о факте обработки ими персональных данных – реализуется путем ознакомления лиц, обрабатывающих персональные данные, с Положением о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ;

– о категориях и составе обрабатываемых персональных данных – реализуется путем ознакомления с утвержденным Перечнем процессов и сведений ограниченного доступа, обрабатываемых в РЦОИ;

– о правилах осуществления обработки персональных данных – реализуется путем ознакомления с Правилами обработки персональных данных в РЦОИ;

– о правилах обеспечения безопасности персональных данных, обрабатываемых РЦОИ.

При обработке персональных данных в РЦОИ должны соблюдаться следующие меры:

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрация действий пользователей, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование защищенных каналов связи;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;

– восстановление персональных данных, при их модификации или уничтожении вследствие несанкционированного доступа к ним в соответствии с Положением о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники.

5. Обращение с материальными носителями персональных данных

Персональные данные в РЦОИ хранятся на съемных и несъемных машинных носителях информации (далее – МНИ).

При использовании и в целях обеспечение сохранности МНИ, а также предотвращения разрушения и утери обрабатываемой на компьютере информации пользователь информационных систем персональных данных должен осуществлять копирование необходимой информации по мере ее обновления на учтенные в установленном порядке МНИ (такие как: внешние жесткие диски, гибкие магнитные диски, USB флэш-накопители, карты флэш-памяти, оптические носители и др.). Эти носители должны быть учтены в Журнале учёта машинных носителей информации (далее – Журнал).

В Журнале указывают:

– Номер машинного носителя;
– Тип носителя;
– Ф.И.О. работника;
– Дата получения и подпись работника;
– Ф.И.О. администратора информационной безопасности;
– Дата возврата и подпись администратора информационной безопасности;
– Отметка об уничтожении.

Кроме того, в этом Журнале необходимо учесть МНИ с электронной цифровой подписью (далее – ЭЦП), а также те, которые используются для передачи персональных данных третьей стороне.

Ответственность за ведение и хранение Журнала несёт администратор информационной безопасности, который в конце каждого года проверяет наличие МНИ у пользователей.

В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки такой носитель уничтожается или с него стираются персональные данные (способом исключающим возможность восстановление данных).

Вынос резервных копий баз данных информационных систем персональных данных, содержащих информацию персонального характера, из РЦОИ запрещен. Передача и копирование их допустима только для прямого использования с целью технологической поддержки информационных систем персональных данных.

Пользователи информационных систем персональных данных должны обеспечивать сохранность съемных носителей, содержащих персональные данные. В случае утраты носителя, пользователи должны немедленно сообщить об этом администратору информационной безопасности.

Если при работе с персональными данными работнику РЦОИ необходимо покинуть рабочее место, материальные носители персональных данных должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

6. Контроль выполнения работ по обеспечению безопасности персональных данных

В целях оценки уровня защищенности обрабатываемых в РЦОИ персональных данных, своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, устранения несоответствий требованиям законодательства Российской Федерации в области зашиты персональных данных в РЦОИ не реже одного раза в год проводится контроль за соблюдением требований по обеспечению безопасности персональных данных.

Контроль выполнения работ по обеспечению безопасности персональных данных в РЦОИ (далее – Контроль) реализуется путем проведения периодических контрольных проверок и аудитов по фактам произошедших инцидентов информационной безопасности. При проведении контроля осуществляется анализ изменений процессов защиты персональных данных.

Контролю подлежат как принятые меры организации обработки информации, так и меры по обеспечению её безопасности.

В рамках проведения контрольных мероприятий выполняются:

– проверка целей и состава обрабатываемых персональных данных;

– проверка актуальности описания процессов обработки информации и перечня информационных систем персональных данных;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных, ознакомления работников с документами РЦОИ, устанавливающими порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;

– проверка перечня лиц, доступ которых к информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

– проверка состава используемого комплекса средств защиты персональных данных и механизмов идентификации, аутентификации и разграничения прав доступа пользователей информационной системы персональных данных на уровне операционных систем, баз данных и прикладного программного обеспечения;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных;

– проверка процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения персональных данных;

– проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

– проверка физических мер защиты персональных данных, организация пропускного режима;

– проверка соответствия организационно-распорядительной документации, определяющей порядок обработки и защиты персональных данных в РЦОИ, по обеспечению безопасности персональных данных действующим требованиям законодательства Российской Федерации, руководящих документов ФСБ России, ФСТЭК России, Роскомнадзора.

Контрольные мероприятия проводятся как периодически, так и внепланово в случае возникновения инцидентов информационной безопасности.

Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений РЦОИ, периодический контроль за эффективностью

средств защиты информации осуществляет лицо, ответственное за информационную безопасность.

Ответственный за информационную безопасность или лицо, его заменяющее, обязан присутствовать при всех проверках по вопросам защиты информации.

Ремонтно-восстановительные работы технических средств обработки информации проводятся под контролем и в присутствии администратора информационной безопасности с привлечением администратора информационных систем персональных данных.

По результатам проверок контролирующими органами ответственный за информационную безопасность с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением. При обнаружении нарушений ректор АСОУ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении норм, регулирующих обработку персональных данных, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

Прекращение доступа к персональным данным и/или увольнение не освобождает работника РЦОИ от принятых обязательств по неразглашению персональных данных, ставших доступными при выполнении должностных обязанностей.

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как сама организация и ее должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Политика
безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ

1. Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование обработки персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и ее использования.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не распространять их без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

Оператор персональных данных – 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.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной

информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Субъекты персональных данных – работники, обучающиеся, участники единого государственного экзамена, граждане, привлекаемые к проведению государственной итоговой аттестации, члены предметных комиссий, общественные наблюдатели, слушатели и другие лица.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Введение

Настоящая Политика безопасности персональных данных, обрабатываемых в информационных системах персональных данных и государственных информационных системах (далее вместе – информационные системы персональных данных) РЦОИ (далее – Политика), является официальным документом и разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных РЦОИ.

В Политике определены требования к работникам, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных РЦОИ.

3. Общие положения

Целью настоящей Политики является обеспечение безопасности персональных данных РЦОИ от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей информационной системы, содержащей соответствующую информацию. В информационных системах персональных данных должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности персональных данных.

В информационных системах персональных данных необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень персональных данных, подлежащих защите, определен в Правилах обработки персональных данных.

4. Система защиты персональных данных

Система защиты персональных данных строится на основании:

– Перечня персональных данных, подлежащих защите;

– Перечня информационных систем персональных данных;

– Акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных;

– Частной модели угроз и нарушителя безопасности персональных данных;

– Положения о разграничении прав доступа к обрабатываемым персональным данным;

– Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности персональных данных в каждой информационной системе персональных данных РЦОИ. Для каждой информационной системы персональных данных должен быть составлен список используемых технических средств, а также программного обеспечения, участвующего в обработке персональных данных, подлежащих защите.

В зависимости от уровня защищенности персональных данных в информационной системе персональных данных и актуальных угроз, система защиты персональных данных может включать следующие технические и программные средства:

– антивирусные средства для объектов вычислительной техники;

– средства межсетевого экранирования;

– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами информационной системы персональных данных и операционных систем, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

– управление доступом и разграничение доступа пользователей;

– регистрацию и учет действий с информацией;

– обеспечение целостности данных;

– обнаружение вторжений.

Список используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава системы защиты персональных данных или элементов информационных систем персональных данных должны быть согласованы с администратором информационной безопасности.

5. Требования к подсистемам системы защиты персональных данных

Система защиты персональных данных включает в себя следующие подсистемы:

– управления доступом, регистрации и учета;

– обеспечения целостности и доступности;

– антивирусной защиты;
– межсетевого экранирования;
– анализа защищенности;
– обнаружения вторжений;
– криптографической защиты.

Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от уровня защищенности персональных данных при их обработке в информационной системе персональных данных, определенного в Акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

6. Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

– идентификации и проверки подлинности субъектов доступа при входе в информационную систему персональных данных;

– идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

– идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

– регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова;

– регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки персональных данных (операционных систем, приложений). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

7. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем персональных данных РЦОИ, а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов информационных систем персональных данных.

8. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты объектов вычислительной техники РЦОИ.

Средства антивирусной защиты предназначены для реализации следующих функций:

– резидентный антивирусный мониторинг;

– антивирусное сканирование;

– централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения во все элементы информационных систем персональных данных.

9. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

– фильтрации IP-трафика;

– идентификации и аутентификации администратора информационной безопасности при его локальных запросах на доступ;

– контроля целостности своей программной и информационной части;

– фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

– регистрации и учета запрашиваемых сервисов прикладного уровня;

– блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

– контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе сети.

10. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

11. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в информационных системах персональных данных РЦОИ, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

12. Пользователи информационных систем персональных данных

В Концепции безопасности персональных данных определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей информационных систем персональных данных, определен их уровень доступа и возможности.

В информационных системах персональных данных РЦОИ можно выделить следующих пользователей, участвующих в обработке персональных данных:

- Администратор информационной системы персональных данных;
- Администратор информационной безопасности;
- Пользователь информационной системы персональных данных.

Данные о группах пользователей, уровне их доступа и информированности отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ.

12.1. Администратор информационной системы персональных данных

Администратор информационной системы персональных данных, ответственный за настройку, внедрение и сопровождение информационной системы персональных данных. Обеспечивает функционирование подсистемы управления доступом информационной системы персональных данных и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (пользователя информационной системы персональных данных) к элементам, хранящим персональные данные.

Администратор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

– обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;

– обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных;

– имеет доступ ко всем техническим средствам обработки информации средствам защиты и данным в информационной системе персональных данных;

– обладает возможностями внесения изменений в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения;

– обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

12.2. Администратор информационной безопасности

Администратор информационной безопасности, ответственный за функционирование системы защиты персональных данных, включая обслуживание и настройку административной, серверной и клиентской части компонентов.

Администратор информационной безопасности обладает следующим уровнем доступа и знаний:

– обладает полной информацией об информационных системах персональных данных;

– имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы персональных данных;

– не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор информационной безопасности уполномочен:

– реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов и систем обнаружения вторжений, в соответствии с которыми пользователь информационной системы персональных данных получает возможность работать с элементами информационной системы персональных данных;

– осуществлять аудит средств защиты информации;

– осуществлять контроль за действиями пользователей информационной системы персональных данных при их работе с персональными данными;

– устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений.

12.3. Пользователь информационной системы персональных данных

Пользователь информационной системы персональных данных, это работник РЦОИ, осуществляющий обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных в информационную систему персональных

данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных.

Пользователь информационной системы персональных данных не имеет полномочий для управления подсистемами обработки данных и системы защиты персональных данных.

Пользователь информационной системы персональных данных обладает следующим уровнем доступа и знаний:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;

– располагает конфиденциальными данными, к которым имеет доступ.

13. Требования к работникам по обеспечению защиты персональных данных

Все работники РЦОИ, являющиеся пользователями информационных систем персональных данных, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности персональных данных.

При вступлении в должность нового работника непосредственный руководитель структурного подразделения обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем персональных данных.

Работник должен быть ознакомлен с настоящей Политикой, установленными процедурами работы с элементами информационной системы персональных данных и системой защиты персональных данных.

Работники РЦОИ, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а также исключать возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники РЦОИ должны:

– следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства идентификации и аутентификации).

– обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи информационной системы персональных данных должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Работникам РЦОИ запрещается:

– устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

– разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с персональными данными в информационной системе персональных данных работники РЦОИ обязаны исключить возможность просмотра персональных данных третьими лицами с мониторов объектов вычислительной техники.

Работники РЦОИ должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, нарушающих принятые Политику и процедуры безопасности персональных данных.

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководителю РЦОИ и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

14. Должностные обязанности пользователей информационной системы персональных данных

Должностные обязанности пользователей информационной системы персональных данных описаны в следующих документах:

– Инструкция администратора информационной системы персональных данных;

– Инструкция администратора информационной безопасности (ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных);

– Инструкция пользователя информационной системы персональных данных.

15. Ответственность пользователей информационной системы персональных данных

В соответствии со статьями 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти

действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

Пользователи информационной системы персональных данных несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях работниками РЦОИ – Пользователями информационной системы персональных данных правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в локальных нормативных и правовых актах РЦОИ.

16. Список использованных источников

1. Конституция Российской Федерации;
2. Трудовой кодекс Российской Федерации;
3. Семейный кодекс Российской Федерации;
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
6. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
7. 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»;
8. 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».

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Положение
об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения в целях обеспечения зашиты технических средств

1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений РЦОИ, в которых размещены информационные системы персональных данных, в том числе государственные информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения в целях обеспечения зашиты технических средств (далее – Положение) разработано в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом 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 требований к защите персональных данных для каждого из уровней защищенности».

1.2. Настоящее Положение определяет порядок действий администратора информационной безопасности и пользователей информационных систем персональных данных при защите технических средств информационных систем персональных данных, в том числе технических средств системы защиты информации.

1.3. Защита от проникновения посторонних лиц в помещения РЦОИ обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Границы контролируемой зоны

2.1. Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

2.2. Технические средства, позволяющие осуществлять обработку персональных данных, размещаются в пределах контролируемой зоны.

2.3. Контролируемая зона помещений, в которых производится обработка конфиденциальной информации в информационных системах персональных данных РЦОИ определяется в соответствии с Перечнем помещений, в которых размещено оборудование информационных систем персональных данных.

2.4. Перемещение стационарного оборудования информационных систем персональных данных 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. Несанкционированный внос пользователями информационных систем персональных данных неучтенных машинных носителей, мобильных технических средств запрещен.

3. Порядок доступа в помещения

3.1. На период обработки защищаемой информации в помещениях, где размещено оборудование информационных систем персональных данных и средств защиты информации, могут находиться только пользователи, допущенные к обработке информации, нахождение которых в пределах границы контролируемой зоны необходимо для выполнения ими служебных (трудовых обязанностей).

3.2. Нахождение в помещениях контролируемых зон других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии пользователя, допущенного к обработке информации.

4. Правила размещения устройств вывода информации

4.1. При размещении в помещениях контролируемых зон технических средств отображения информации должен быть исключен несанкционированный просмотр выводимой на них информации.

4.2. Размещение средств отображения информации указано в эксплуатационной документации на информационные системы персональных данных и эксплуатационной документации на системы защиты информации.

4.3. Выполнение требований к размещению устройств вывода информации в контролируемых зонах обеспечивает администратор информационной безопасности.

5. Заключительные положения

5.1. Пользователи информационных систем персональных данных, должны быть предупреждены об ответственности за действия, нарушающие требования настоящего Положения.

5.2. Пользователи информационных систем персональных данных должны быть ознакомлены с настоящим Положением до начала работы в информационных

системах персональных данных, под роспись. Обязанность ознакомления пользователей информационных систем персональных данных с настоящим Положением лежит на администраторе информационной безопасности.

5.3. Работники РЦОИ осуществляют контроль за действиями посторонних лиц при их нахождении в помещениях, являющихся контролируемой зоной РЦОИ.

5.4. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением, в пределах, определенных действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Положение
о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ

Настоящее Положение о разграничении прав доступа к обрабатываемым персональным данным в РЦОИ (далее – Положение), разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет уровень доступа должностных лиц к персональным данным участников государственной итоговой аттестации, лиц, привлекаемых к проведению государственной итоговой аттестации, членов конфликтной и предметных комиссий, общественных наблюдателей и других лиц.

Под действиями с персональными данными понимается следующее:

- **сбор** – процесс получения, взятия персональных данных у субъектов, персональных данных;
- **запись** – действия, в результате которых фиксируется, регистрируется содержание персональных данных о субъекте персональных данных в информационную систему персональных данных и (или) на материальный носитель.
- **систематизация** – произведение действий по сортировке персональных данных для выполнения целей обработки;
- **накопление** – произведение действий по хранению персональных данных после их сбора;
- **хранение** – длительное хранение персональных данных для выполнения целей обработки;
- **уточнение** (обновление, изменение) – внесение изменений о субъекте персональных данных;
- **извлечение** – действия, направленные на извлечение информации из информационной системы персональных данных и (или) материальных носителей содержащих персональные данные;
- **использование** – осуществление с помощью персональных данных основной (производственной) и сопутствующей деятельности;
- **предоставление** – действия, направленные на передачу (предоставления) персональных данных определенному кругу лиц;
- **доступ** – действия, направленные на ознакомление с персональными данными;
- **распространение** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **блокирование** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **удаление** – действия, в результате которых, возможно восстановить содержание персональных данных в информационной системе персональных данных и (или) восстановить содержание информации с материальных носителей.
- **уничтожение** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Разграничение прав доступа осуществляется исходя из характера и режима обработки персональных данных в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн).

Перечень групп, участвующих в обработке персональных данных в ИСПДн, а также их уровень прав доступа для ИСПДн вместе с Системой разграничения доступа в информационных системах РЦОИ, в соответствии с Перечнем информационных систем персональных данных в РЦОИ, представлен в Приложениях 1-2 к настоящему Положению.

Приложение 1

Перечень групп, участвующих в обработке персональных данных в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
Администратор ИСПДн	- Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. - Обладает полной информацией о технических средствах и конфигурации ИСПДн. - Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. - Обладает правами конфигурирования и административной настройки технических средств ИСПДн. - Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных
Пользователь ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных

Приложение 2

Система разграничения доступа в информационных системах РЦОИ

1. В РЦОИ для управления доступом используется ролевой метод.

2. В информационных системах (далее – ИС) субъектами доступа являются сотрудники РЦОИ или запускаемые от их имени процессы. Для субъектов доступа определены роли, приведенные в Таблице 1.

Таблица 1

Роли субъектов доступа.

Идентификатор роли	Наименование роли	Примечание
Р1	Администратор ИСПДн	Привилегированная роль в ИС, которой разрешены действия (операции) по управлению (администрированию) ИС.
Р2	Администратор информационной безопасности	Привилегированная роль в ИС, которой разрешены действия (операции) по управлению (администрированию) системой защиты информации ИС.
Р3	Пользователь ИСПДн (внутренний)	Непривилегированная роль в ИС, которой разрешены действия (операции) по обработке информации в ИС с использованием технологии локального доступа.

3. В Таблице 2 представлены уровни доступа ролей к объектам ИС.

Таблица 2

Уровни доступа ролей к объектам ИС.

Идентификатор	Уровень доступа	Примечание
УД.1	Полный	Уровень доступа, при котором не устанавливаются ограничения на взаимодействие роли и ИС. Допускает выполнение любых действий (операций) по изменению состава, размещению, конфигурированию компонентов ИС и системы защиты информации и выполнению действий (операций) по обработке информации.
УД.2	Ограниченный	Уровень доступа, при котором устанавливаются ограничения на взаимодействие роли и ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС. Допускает выполнение действий (операций) по обработке информации.

4. Уровень доступа роли к объектам ИС приведен в Таблице 3.

Таблица 3

Уровень доступа роли к объектам ИС.

Объект доступа	Роль		
	Р1	Р2	Р3
Устройства			
Принтеры	УД.1	УД.1	УД.2
Сканеры	УД.1	УД.1	УД.2
Автоматизированное рабочее место (АРМ)	УД.1	УД.1	УД.2

Объект доступа	Роль		
	Р1	**Р2**	**Р3**
Серверы	УД.1	УД.1	УД.2
Объекты системы хранения данных	УД.1	УД.1	УД.2
Сетевое и коммутационное оборудование	УД.1	УД.1	УД.2
Компакт-диски CD/DVD	УД.1	УД.1	УД.2
Флеш-накопители	УД.1	УД.1	УД.2
Переносные гибкие магнитные диски	УД.1	УД.1	УД.2
Объекты файловой системы			
Жесткий диск, личный каталог	УД.1	УД.1	УД.1
Жесткий диск, все каталоги	УД.1	УД.1	УД.2
Запускаемые и исполняемые модули			
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно участвующего в обработке информации	УД.1	УД.1	УД.2
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно не участвующего в обработке информации	УД.1	УД.1	УД.2
Объекты системы управления базами данных			
Базы данных	УД.1	УД.1	УД.2
Таблицы	УД.1	УД.1	УД.2
Представления	УД.1	УД.1	УД.2
Хранимые процедуры	УД.1	УД.1	УД.2
Объекты виртуальной инфраструктуры			
Система управления виртуальной инфраструктурой	УД.1	УД.1	УД.2
Гипервизор	УД.1	УД.1	УД.2
Виртуальные машины, виртуальные контейнеры	УД.1	УД.1	УД.2
Средства защиты виртуальной инфраструктуры	УД.1	УД.1	УД.2

– Роль 1 – «Администратор ИСПДн» имеют сотрудники, которым разрешены действия по внесению изменений в базовую конфигурацию информационных систем и системы защиты информации в РЦОИ.

– Роль 2 – «Администратор информационной безопасности» имеет сотрудник, назначенный ответственным за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах РЦОИ.

– Роль 3 – «Пользователь ИС» имеют сотрудники, осуществляющие обработку информации в информационных системах РЦОИ.

5. Учет имеющихся у сотрудников ролей, а также их изменений ведется ответственным за организацию обработки персональных данных в информационных системах РЦОИ.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Порядок
доступа работников РЦОИ в помещения, в которых осуществляется обработка защищаемой информации, не содержащей сведения, составляющие государственную тайну, и размещены информационные системы

1. Настоящий Порядок регламентирует условия и порядок осуществления доступа работников РЦОИ в помещения, в которых осуществляется обработка защищаемой информации, содержащей персональные данные, и размещены информационные системы (далее – Помещения), в целях организации контролируемой зоны и режима обеспечения безопасности защищаемой информации, содержащей персональные данные (далее – защищаемая информация), препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа.

2. Настоящий Порядок разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и 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», приказа 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».

3. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки защищаемой информации, средств защиты информации и носителей защищаемой информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

4. В помещения, где размещены информационные системы, позволяющие осуществлять обработку защищаемой информации, а также хранятся носители защищаемой информации, допускаются только работники РЦОИ и лица, привлекаемые к обработке защищаемой информации и имеющие доступ к защищаемой информации. Перечень работников, уполномоченных на обработку защищаемой информации и имеющих доступ к защищаемой информации (далее – Работники), утверждается приказом АСОУ. При обработке защищаемой

информации в информационных системах должна обеспечиваться сохранность носителей защищаемой информации.

5. Нахождение в Помещениях посторонних лиц допускается только в сопровождении Работников РЦОИ.

6. Уборка и техническое обслуживание Помещений допускаются только в присутствии Работников РЦОИ.

7. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю РЦОИ.

8. Двери Помещений должны быть оборудованы механическими замками.

9. Перед началом обработки защищаемой информации Работники РЦОИ берут ключи от Помещений на посту охраны с внесением записи в журнал.

10. В течение обработки защищаемой информации ключи от Помещений хранятся у Работников РЦОИ.

11. По окончании обработки защищаемой информации Работники РЦОИ закрывают Помещения и сдают ключи на пост охраны с внесением записи в журнал.

12. Внутренний контроль за соблюдением порядка доступа в Помещения проводится лицом, ответственным за организацию обработки персональных данных.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Перечень
процессов и сведений ограниченного доступа, обрабатываемых в РЦОИ

Сокращения и определения:

ГИС	- государственная информационная система;
ИС	- информационная система;
ИСПДн	- информационная система персональных данных;
ПДн	- персональные данные;
Перечень НПА	- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
1.	**Наименование процесса:** организация и проведение государственной итоговой аттестации (далее – ГИА). **Цели обработки персональных данных:** формирование региональной информационной системы обеспечения проведения ГИА, индивидуального учета результатов освоения обучающимися образовательных программ, а также хранение данных об этих результатах на электронных носителях. **Способ обработки:** автоматизированный, сведения обрабатываются в ГИС «АИС РЦОИ РИС МО».			
1.1.	-обучающиеся, освоившие образовательные программы основного	*Участники государственной итоговой аттестации:* ФИО; данные документа, удостоверяющего личность; СНИЛС; дата рождения;	• Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; • Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;	Отдел технического сопровождения ГИА-11/ отдел технического

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
	общего и среднего общего образования; - лица, привлекаемые к организации и проведению ГИА	пол; гражданство; телефон; место учебы; класс; категория выпускника; форма обучения; сведения о действующих результатах ГИА; сведения о действующем зачете ИС, ИС(И); сведения о принципе рассадки; сведения о регионе, в котором закончил ОО; допуск к ГИА; наличие/отсутствие ограничений возможностей здоровья; наличие/отсутствие образования, полученного в иностранном государстве; дата сдачи ИС, ИС(И); место сдачи ИС, ИС(И); сведения об результатах ИС, ИС(И); дата сдачи ГИА; сведения об экзаменах и результатах; предметы; сведения об апелляциях; информация о прохождении обучения в учреждении закрытого типа; информация о наличии статуса беженца или переселенца; информация о профильных предметах. *Эксперты предметных комиссий:* ФИО; дата рождения;	• Постановление Правительства РФ от 29.11.2021 № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования».	сопровождения ГИА-9

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
		пол; данные документа, удостоверяющего личность; СНИЛС; место работы; уровень профессионального образования; ученая степень; адрес электронной почты; квалификация по документу об образовании; должность; стаж работы; предметная специализация. *Работники ППЭ:* ФИО; пол; контактные телефоны; адрес электронной почты; данные документа, удостоверяющего личность; СНИЛС; год рождения; место работы; должность; уровень профессионального образования; квалификация по документу об образовании; предметная специализация; общий преподавательский стаж; возможная должность в ППЭ; сведения об аккредитации. *Руководитель МСУ*: ФИО;		

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
		должность. *Руководитель ОО:* ФИО; должность. *Ответственный за проведения ГИА в ОО*: ФИО. *Ответственный за проведения ГИА АТЕ/МСУ*: ФИО; телефон; адрес электронной почты.		
2.	**Наименование процесса:** организация и проведение ГИА. **Цели обработки персональных данных:** формирование региональной информационной системы обеспечения проведения ГИА. **Способ обработки:** автоматизированный, сведения обрабатываются в ИСПДн «АИС ГИА».			
2.1.	-обучающиеся, освоившие образовательные программы основного общего и среднего общего образования; - лица, привлекаемые к организации и проведению ГИА	*Участники государственной итоговой аттестации:* ФИО; данные документа, удостоверяющего личность; СНИЛС; дата рождения; пол; гражданство; телефон; место учебы; класс; категория выпускника; форма обучения; сведения о действующих результатах ГИА; сведения о действующем зачете ИС, ИС(И); сведения о принципе рассадки; сведения о регионе, в котором закончил ОО; допуск к ГИА;	• Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; • Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; • Постановление Правительства РФ от 29.11.2021 № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных	Отдел технического сопровождения ГИА-11/ отдел технического сопровождения ГИА-9

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
		наличие/отсутствие ограничений возможностей здоровья; наличие/отсутствие образования, полученного в иностранном государстве; дата сдачи ИС, ИС(И); место сдачи ИС, ИС(И); сведения об результатах ИС, ИС(И); дата сдачи ГИА; сведения об экзаменах и результатах; предметы; сведения об апелляциях; информация о прохождении обучения в учреждении закрытого типа; информация о наличии статуса беженца или переселенца; информация о профильных предметах. *Эксперты предметных комиссий:* ФИО; дата рождения; пол; данные документа, удостоверяющего личность; СНИЛС; место работы; уровень профессионального образования; ученая степень; адрес электронной почты; квалификация по документу об образовании; должность; стаж работы; предметная специализация.	информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования».	

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
		Работники ППЭ: ФИО; пол; контактные телефоны; адрес электронной почты; данные документа, удостоверяющего личность; СНИЛС; год рождения; место работы; должность; уровень профессионального образования; квалификация по документу об образовании; предметная специализация; общий преподавательский стаж; возможная должность в ППЭ; сведения об аккредитации. *Руководитель МСУ*: ФИО; должность. *Руководитель ОО:* ФИО; должность. *Ответственный за проведения ГИА в ОО*: ФИО. *Ответственный за проведения ГИА АТЕ/МСУ*: ФИО; телефон; адрес электронной почты.		

№ п/п	Категория субъектов персональных данных	Содержание сведений	Правовое основание для обработки	Подразделения РЦОИ, использующие в работе сведения ограниченного доступа
3.	**Наименование процесса:** рассмотрение апелляций конфликтной комиссией Московской области (далее – КК) при проведении государственной итоговой аттестации по образовательным программам среднего общего образования. **Цели обработки персональных данных:** формирование апелляционных комплектов для обеспечения проведения КК. **Способ обработки:** автоматизированный, сведения обрабатываются в ИСПДн «АИС КК».			
3.1.	-участники ГИА, подавшие апелляции в КК	ФИО; дата рождения; пол; данные документа, удостоверяющего личность; наличие/отсутствие ограничений возможностей здоровья.	• Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»; • Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; • Постановление Правительства РФ от 29.11.2021 № 2085 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования».	Отдел технического сопровождения ГИА-11/ отдел технического сопровождения ГИА-9

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Описание
технологического процесса обработки информации в информационных системах персональных данных РЦОИ

Принятые сокращения

ИС	–	информационная система;
АРМ	–	автоматизированное рабочее место;
НСД	–	несанкционированный доступ;
СЗИ	–	средства защиты информации;
СЗИНСД	–	средства защиты информации от несанкционированного доступа;

1. Термины и определения

Технологический процесс обработки конфиденциальной информации (ТП) – последовательность действий пользователей при работе с конфиденциальной информацией, включающая следующие этапы: ввод, обработку (преобразование, хранение), передачу, вывод, администрирование (резервирование, управление доступом).

Машинные носители информации (МНИ) – магнитные, оптические и прочие хранилища информации, используемые в средствах вычислительной техники, в т.ч. съемные (НГМД, CD, DVD, Flash, магнитные ленты и др.) и несъемные.

Бумажные носители информации (БН) – документы, полученные в результате распечатывания на принтере и других печатающих средствах, а также размножения на копировальных аппаратах.

Ввод информации – этап технологического процесса, на котором производится создание либо перемещение информации с внешних носителей (БН и съемных МН) на внутренние носители (несъемные МН) с помощью клавиатуры, мыши, приводов съемных носителей, сканеров, беспроводных внешних устройств. Не считается вводом информации передача ее между различными ресурсами локальной вычислительной сети по сетевому кабелю. Также не считается вводом информации ее восстановление с внешних МН.

Хранение информации – этап технологического процесса, на котором информация размещается в структурированном виде в период между двумя любыми этапами технологического процесса.

Обработка информации – этап технологического процесса, на котором производится преобразование информации, полученной на этапе ввода или хранимой в структурированном виде, для последующего ее вывода или хранения.

Вывод информации – этап технологического процесса, на котором производится перемещение информации с внутренних МН на внешние носители

(БН и съемные МН). Не считается выводом информации передача ее между различными ресурсами локальной вычислительной сети по сетевому кабелю. Также не считается выводом информации ее перенос на внешние МН с целью резервирования.

Администрирование – этап технологического процесса, на котором производятся служебные операции как с хранимой информацией (резервирование и восстановление), так и с программными средствами обработки и защиты информации.

Техническое обслуживание – этап технологического процесса, на котором производятся служебные операции с аппаратными средствами обработки и защиты информации в рамках ИС.

2. Описание информационных потоков в ИС

ФЦТ - федеральный центр тестирования

ФИС - федеральная информационная система

РИС - региональная информационная система

РЦОИ - региональный центр обработки информации

МОУО - муниципальный отдел управления образованием

ОО - образовательная организация

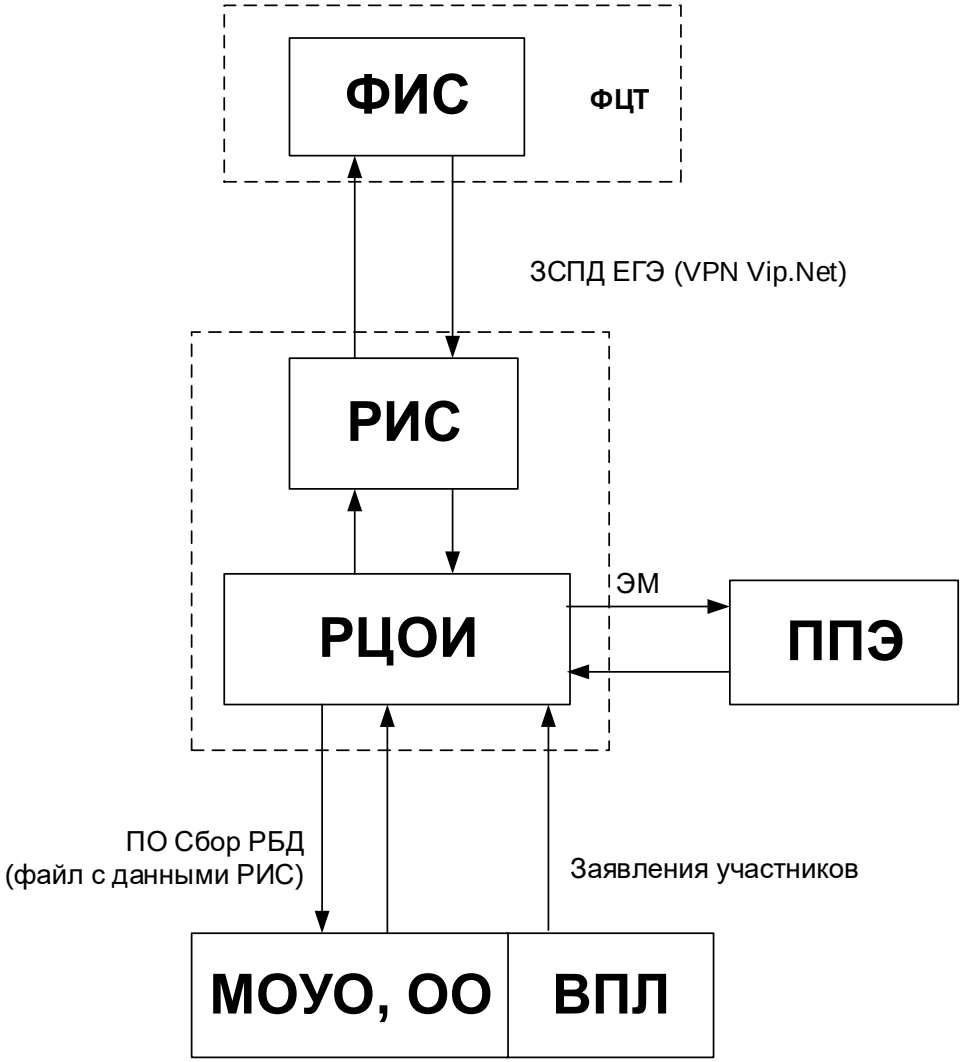
ППЭ - пункт проведения экзамена

ВПЛ - выпускники прошлых лет

ЭМ - экзаменационные материалы

ЗСПД ЕГЭ - защищенная сеть Передачи данных ЕГЭ

ПО Сбор РБД - функциональный модуль подсистемы сбора региональной информационной системы



3. Описание технологического процесса

3.1. Ввод информации.

Ввод информации может осуществляться следующим образом:

– ввод информации на уровне РЦОИ осуществляется с БН с помощью специализированного ПО в рамках ИС;

– ввод информации может осуществляться с МНИ, учтенных соответствующим образом для использования в рамках ИС.

3.2. Хранение и обработка информации.

Информация о персональных данных используется для формирования региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, на территории Московской области.

На жестких дисках хранятся файлы базы данных ИС.

На съемных внешних МН хранятся файлы резервных копий.

3.3. Вывод информации.

Вывод информации в ИС осуществляется следующим образом.

3.3.1. Вывод документов на бумажные носители.

Вывод информации на бумажные носители из ИС не осуществляется. Вывод на печать конфиденциальных документов не предусмотрен.

3.3.2. Вывод документов на машинные носители.

Вывод конфиденциальной информации на МН может осуществляться только на учтенные МН соответствующего уровня конфиденциальности.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее соответственно – ответственный, ИСПДн) в РЦОИ назначается ректором АСОУ.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в РЦОИ.

Ответственный за эксплуатацию ИСПДн в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для соответствующей ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством Российской Федерации.

2. Функции ответственного за эксплуатацию ИСПДн

- Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.
- Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.
- Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.
- Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.
- Представление на утверждение ректором АСОУ списка пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации, устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.
- Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

- Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
- Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.
- Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.
- Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн.
- Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.
- Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.
- Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
ответственного за защиту информации ограниченного доступа

1. Общие положения

Настоящая Инструкция определяет функции, права и обязанности ответственного за защиту информации ограниченного доступа в РЦОИ.

Ответственный за защиту информации ограниченного доступа назначается ректором АСОУ и осуществляет контроль за выполнением комплекса организационных мероприятий по обеспечению безопасности информации, в том числе требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных в РЦОИ.

В своей работе ответственный за защиту информации ограниченного доступа руководствуется настоящей Инструкцией, организационно-распорядительными документами АСОУ, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации, а также иными нормативными документами в части защиты информации.

Ответственный за защиту информации ограниченного доступа несет ответственность за свои действия в соответствии с действующим законодательством Российской Федерации.

2. Функции ответственного за защиту информации ограниченного доступа

- Контроль ознакомления работников с документами РЦОИ, устанавливающими порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области.
- Контроль за соблюдением пользователями информационных систем персональных данных требований по обеспечению безопасности персональных данных при работе в информационных системах.
- Контроль соответствия организационно-распорядительной документации, определяющей порядок обработки и защиты персональных данных в РЦОИ, по обеспечению безопасности персональных данных действующим требованиям законодательства Российской Федерации, руководящих документов ФСБ России, ФСТЭК России, Роскомнадзора.
- Организация повышения уровня осведомленности пользователей информационных систем персональных данных по вопросам информационной безопасности.
- Контроль учета применяемых средств защиты информации, эксплуатационной и технической документации к ним.

- Контроль эффективности мер и средств защиты персональных данных на предмет соответствия установленным требованиям безопасности.

3. Обязанности и права ответственного за защиту информации ограниченного доступа

- Разработка организационно-распорядительных документов по вопросам защиты информации при её обработке с помощью информационных систем персональных данных.
- Контроль исполнения приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации.
- Организация ознакомления работников РЦОИ, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите обрабатываемых персональных данных.
- Проведение инструктажа пользователей информационных систем персональных данных по выполнению требований по обеспечению защиты персональных данных.
- Организация работы по декларированию (аттестации) информационных систем на соответствие нормативным требованиям.
- Внесение предложений по совершенствованию существующей системы защиты информации на рассмотрение руководства.
- Присутствие при проверках по вопросам защиты информации.

Ответственный за защиту информации ограниченного доступа требует от руководителей структурных подразделений РЦОИ устранения нарушений и недостатков в случае их выявления, дает обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации.

Об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток несанкционированного доступа к информации или попыток хищения, копирования, изменения информации незамедлительно докладывает руководителю РЦОИ и принимает меры пресечения.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
администратора информационных систем персональных данных

1. Общие положения

Настоящая Инструкция определяет основные функции, права и обязанности Администратора информационных систем персональных данных (далее – администратор) при их обработке в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ.

Администратор назначается приказом ректора АСОУ из числа работников РЦОИ и отвечает за обеспечение устойчивой работоспособности и нормальное функционирование установленной системы защиты информации (далее - СЗИ) в ИСПДн.

Администратор несет ответственность за свои действия в соответствии с действующим законодательством Российской Федерации.

2. Основные функции, обязанности и права администратора

- Выполнение требований действующих нормативных документов по вопросам обеспечения защиты сведений конфиденциального характера при проведении работ на автоматизированных рабочих местах (далее - АРМ), входящих в состав ИСПДн.
- Обеспечение защиты информации, циркулирующей на объектах информатизации.
- Организация работ по предотвращению несанкционированного, непреднамеренного и неправомерного доступа лиц к защищаемой информации.
- Выявление возможных каналов утечки защищаемой информации в процессе деятельности РЦОИ и функционирования ИСПДн, внесение предложений по их закрытию.
- Осуществление контроля за целевым использованием ИСПДн.
- Контроль работы СЗИ и выполнение комплекса организационных мероприятий по обеспечению безопасности информации.
- Обеспечение функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИСПДн, антивирусная защита, резервное копирование данных и т.д.).
- Контроль порядка учета, хранения и обращения с машинными носителями информации.
- Вести учет СЗИ, используемых в ИСПДн в соответствующем журнале.

- Обеспечение контроля действий представителей сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации.
- Участие в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн.
- Обеспечение хранения дистрибутивов программного обеспечения средств обработки информации.
- Незамедлительное информирование руководителя РЦОИ об имеющихся недостатках и выявленных нарушениях СЗИ, а также в случае выявления попыток НСД к охраняемым сведениям или попыток их хищения, копирования или изменения.
- Обеспечение настройки и бесперебойной эксплуатации программных и технических средств обработки персональных данных, входящих в состав информационных систем.
- Обеспечение настройки, бесперебойной эксплуатации и мониторинг СЗИ.
- Настраивание прав доступа работников к персональным данным и средствам их обработки в соответствии с ролевой моделью доступа.
- Проведение инструктажа пользователей информационных систем по правилам эксплуатации программных и технических средств обработки персональных данных, а также СЗИ, входящих в состав ИСПДн.
- Контроль изменения паролей у пользователей информационных систем не реже двух раз в год либо при компрометации паролей.
- Оказание содействия работникам, участвующим в процессах обработки и обеспечения безопасности персональных данных, по вопросам использования средств обработки информации в информационных системах, в рамках своей компетенции.
- Предоставление необходимой информации при проведении проверок регулирующими органами.

3. Контролируемые параметры при проверке СЗИ ИСПДн

- Наличие лицензионного программного обеспечения (операционная система, антивирусная программа и офисный пакет) на АРМ ИСПДн.
- Наличие на компьютере у пользователя прав, соответствующих исполняемой обязанности.
- Наличие пароля на вход в BIOS материнской платы компьютера с целью невозможности изменения настроек.
- Наличие периодического обновления вирусной базы антивирусного ПО.
- Наличие бесперебойного источника питания для штатного завершения процесса обработки информации на серверах в случае отключения электропитания.
- Отсутствие со стороны пользователя АРМ следующих нарушений:

– записи паролей в очевидных местах, внутренности ящика стола, на мониторе компьютера, на обратной стороне клавиатуры и т.д.;

– хранения паролей в записанном виде на отдельных листах бумаги;

– сообщения посторонним лицам своих паролей, а также сведений о применяемой системе защиты ИСПДн от НСД.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
администратора информационной безопасности
(ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных)

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных и государственных информационных системах (далее вместе, соответственно – ИСПДн, администратор информационной безопасности).

Администратор информационной безопасности – это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности назначается приказом ректора АСОУ из числа работников РЦОИ и осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест, и несет ответственность за свои действия в соответствии с действующим законодательством Российской Федерации.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

- Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн.
- Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.
- Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование.
- Регулировать процесс осуществления резервного копирование информации, содержащей персональные данные.
- Оказывать помощь пользователям ИСПДн в отношении правил работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты.

- Осуществлять периодический контроль за выполнением работниками, эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн.
- Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации.
- Участвовать в приемке новых программных средств.
- Обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ.
- Анализировать состояние защиты каждой информационной системы и их отдельных подсистем, докладывать результаты анализа руководителю РЦОИ.
- Проводить проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей (в случае изменения) к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку.
- Контролировать неизменность состояния средств защиты их параметров и режимов защиты.
- В случае отказа работоспособности технических средств и программного обеспечения информационных систем, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
- При выявлении фактов нарушения физической сохранности технических средств информационных систем и средств защиты информации докладывать руководителю РЦОИ.
- Вести журнал учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.
- Своевременно анализировать журнал учета событий безопасности, регистрируемых средствами защиты, с целью выявления возможных нарушений и при подозрении на инцидент немедленно докладывать руководителю РЦОИ.
- Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.
- Докладывать руководителю РЦОИ при выявлении случаев работы на элементах информационных систем посторонних лиц;
- Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ.
- Проводить мероприятия по организации антивирусной защиты.
- Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно Инструкции по организации парольной защиты в ИСПДн.

- Немедленно сообщать руководителю РЦОИ, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– установить причины, по которым стал возможным НСД;

– установить последствия, к которым привел НСД;

– зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий.

- Немедленно докладывать руководителю РЦОИ при возникновения всех внештатных и аварийных ситуаций в части безопасности персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

- Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.
- Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за защиту информации ограниченного доступа в РЦОИ.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая Инструкция определяет основные функции, права и обязанности ответственного за организацию обработки персональных данных в РЦОИ.

Ответственный за организацию обработки персональных данных назначается приказом ректора АСОУ из числа работников РЦОИ и обеспечивает выполнение требований по защите персональных данных при обработке персональных данных в информационной системе.

Ответственный за организацию обработки персональных данных должен знать:

– законодательство Российской Федерации в области персональных данных;

– порядок систематизации, учета и ведения документации с использованием современных информационных технологий;

– средства вычислительной техники, коммуникаций и связи;

– перечень и условия обработки персональных данных в РЦОИ;

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и настоящей Инструкцией.

Ответственный за организацию обработки персональных данных несет ответственность за сохранность сведений ограниченного доступа в соответствии с функциональными обязанностями, определенными настоящей Инструкцией в рамках требований законодательства в области защиты персональных данных.

2. Обязанности ответственного за организацию обработки персональных данных

- Осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
- Доводить до сведения работников РЦОИ положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
- Организовать инструктаж должностных лиц, уполномоченных на обработку персональных данных.

- Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.
- Предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных.
- Организовать ведение журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных.
- Обеспечивать постоянный контроль выполнения установленного комплекса мероприятий по обеспечению безопасности информации пользователями информационной системы персональных данных.

3. Права ответственного за организацию обработки персональных данных

- Требовать от должностных лиц, уполномоченных на обработку персональных данных, безусловного соблюдения установленных правил обработки и защиты персональных данных.
- Требовать от должностных лиц, уполномоченных на обработку персональных данных прекращения обработки персональных данных, в случаях их неправомерного использования и нарушения установленного порядка обработки.
- Инициировать проведение служебных расследований по фактам нарушения установленных правил обработки и защиты персональных данных.
- Вносить на рассмотрение руководства предложения по совершенствованию мер защиты персональных данных, разработке и принятии мер по предотвращению возможных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.
- Подписывать и визировать документы в пределах своей компетенции.
- Осуществлять взаимодействие с руководителями структурных подразделений РЦОИ, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.
- Требовать от руководства оказания содействия в исполнении своих должностных обязанностей и прав.
- Вести переписку с организациями по вопросам, входящим в его компетенцию.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по работе пользователей в информационных системах персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет общие положения работы пользователей информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн) при обработке (наборе, редактировании и печати) информации ограниченного доступа (далее – информация).

1.2. Учет работы пользователей в ИСПДн производится ответственным за организацию обработки персональных данных (далее – ответственным).

1.3. Допуск пользователей для работы в ИСПДн осуществляется в соответствии со списком постоянных пользователей ИСПДн, предназначенных для обработки персональных данных (далее – ПДн).

1.4. К самостоятельной работе на АРМ, входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и Правил работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходимых для выполнения ими служебных (трудовых) обязанностей, а также освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки администратором ИСПДн (или ответственным) знания пользователем настоящей Инструкции, Правил и практических навыков в работе.

1.5. Пользователи имеют право отрабатывать информацию в соответствии с полномочиями доступа «Пользователь» к ресурсам компьютера, присвоенными администратором ИСПДн каждому пользователю.

1.6. Работа в ИСПДн должна осуществляться на базе общесистемного лицензионного программного обеспечения.

1.7. Технические средства ИСПДн в помещении размещаются таким образом, чтобы исключить визуальный просмотр экрана видеомонитора лицами, не имеющими отношения к обрабатываемой информации.

1.8. Уборка помещения, где расположены АРМ, входящие в состав ИСПДн, проводятся только под контролем пользователя ИСПДн. При проведении этих работ обработка защищаемой информации запрещается.

1.9. Настоящая Инструкция доводится до пользователей под подпись.

2. Порядок работы пользователей на АРМ ИСПДн

2.1. Пароль на вход в АРМ пользователь получает от администратора ИСПДн с фиксацией в журнале учета паролей.

2.2. После включения компьютера пользователь должен ввести свои имя пользователя и пароль.

2.3. Для сохранности информации пользователь обязан корректно выключать (перезагружать) свой компьютер. Обязательно дождаться пока компьютер не выключиться самостоятельно!

2.4. В папке «Мои документы» и на «Рабочем столе» может находиться только информация, связанная с текущей работой.

2.5. При временном отсутствии пользователя на рабочем месте компьютер должен быть выключен или заблокирован.

2.6. В целях предотвращения разрушения и утери обрабатываемой на компьютере информации пользователь должен осуществлять проверку программой «антивирусом» машинных носителей информации (далее – МНИ), поступивших из других подразделений и сторонних организаций.

2.7. Пользователь должен хранить МНИ в местах, исключающих несанкционированный доступ к ним. В конце года он должен предъявить их администратору информационной безопасности в ходе проводимой им ежегодной проверки.

2.8. При любом сбое АРМ, нестабильности в работе компьютера, сети, и т. д. пользователь должен сообщать администратору информационной безопасности.

2.9. При обнаружении компьютерного вируса пользователь обязан немедленно прекратить какие-либо действия на компьютере и поставить в известность администратора ИСПДн.

2.10. Пользователь обязан ставить в известность администратора ИСПДн в случае появления сведений или подозрений о фактах несанкционированного доступа к информации.

3. Ограничения

3.1. Пользователю запрещается:

- Передавать кому-либо пароль, используемый на компьютере.
- Осуществлять ввод пароля в присутствии посторонних лиц.
- Оставлять записанные пароли в доступных для других сотрудников местах.
- Оставлять без личного присмотра на рабочем месте или где бы то ни было МНИ и распечатки, содержащие защищаемую информацию.
- Изменять самостоятельно конфигурацию аппаратно-программных средств компьютера, не предусмотренных техническим паспортом ИСПДн или проводить обновление установленного программного обеспечения.
- Осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц.
- Знакомить других сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями.
- Оставлять бесконтрольно включенный компьютер, на столе - магнитные носители и распечатанные листы с информацией.
- Записывать и хранить персональные данные на неучтенных МНИ.

- Выключать (приостанавливать защиту) антивирусный сканер на компьютере.
- Использовать для обработки информации компьютер, не предназначенный для этих целей.
- Использовать компьютер другого пользователя для обработки информации без разрешения администратора ИСПДн.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Правила
работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

1. Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее –пользователи ИСПДн).

2. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

3. Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

4. Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

5. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и поставить в известность администратора ИСПДн.

6. Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

– Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

– Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

– Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

7. Пользователю АРМ категорически запрещается:

– Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

– Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

– Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации;

– Оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

– Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

– Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Правила
обработки персональных данных

1. Общие положения

1.1. Настоящие правила обработки персональных данных устанавливают порядок обработки персональных данных (далее – ПДн) в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ.

1.2. Настоящие правила разработаны на основании и в соответствии с требованиями следующих законодательных и нормативных правовых актов Российской Федерации:

– Трудовой кодекс Российской Федерации (Глава 14);

– Гражданский кодекс Российской Федерации, Часть 1 (ст. ст. 150, 152, 152.1, 152.2) от 30.11.1994 № 51-ФЗ;

– 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 РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.3. Настоящие правила устанавливают и определяют в РЦОИ:

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

– цели обработки ПДн;

– содержание обрабатываемых ПДн для каждой цели обработки ПДн;

– категории субъектов, ПДн которых обрабатываются;

– сроки обработки и хранения обрабатываемых ПДн;

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

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

1.5. Правила являются обязательными для исполнения всеми пользователями ИСПДн РЦОИ, имеющими доступ к ПДн.

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

2. Требования к обработке ПДн

2.1. РЦОИ 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 сборе ПДн и при обращении субъектов ПДн РЦОИ руководствуется главой 4 Федерального закона № 152-ФЗ.

2.4. РЦОИ принимает меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ в частности:

– назначает ответственного за организацию обработки ПДн в ИСПДн РЦОИ приказом ректора АСОУ;

– издает документы, определяющие политику РЦОИ в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

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

– осуществляет внутренний контроль соответствия обработки ПДн Федеральному закону № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам РЦОИ;

– знакомит пользователей ИСПДн РЦОИ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн и настоящими Правилами;

– запрещает обработку ПДн пользователям ИСПДн РЦОИ, не допущенными к их обработке.

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. Письменное согласие на обработку своих персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– наименование и адрес оператора, получающего согласие субъекта ПДн;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

– срок, в течение которого действует согласие, а также порядок его отзыва;

– подпись субъекта персональных данных.

2.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя ректора АСОУ.

2.8. РЦОИ не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни.

2.9. Безопасность ПДн, при их обработке в ИСПДн РЦОИ, контролирует ответственный за организацию обработки ПДн.

2.10. При обработке ПДн соблюдаются следующие требования:

– к работе с ПДн допускаются только работники, занимающие должности, которые предполагают обработку ПДн для исполнения служебных обязанностей и подписавшие обязательство о неразглашении персональных данных по форме Приложения 3 к настоящим Правилам;

– на период обработки ПДн в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации.

2.11.Особенности обработки ПДн:

- Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объем обрабатываемых РЦОИ ПДн соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.
- При обработке ПДн обеспечивается их точность, достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. РЦОИ принимает необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных ПДн.
- Машинные носители информации подлежат обязательной регистрации и учету.

2.12. Обработка ПДн осуществляется при условии выполнения требований к защите информации, утвержденных:

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

– приказом ФСТЭК России от 15.02.2017 № 27 «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17»;

– приказом 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».

2.13. РЦОИ при обработке ПДн принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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.

3. Цели обработки ПДн

3.1. РЦОИ обрабатывает ПДн, содержащиеся в ИСПДн РЦОИ.

3.2. Целями обработки ПДн в ИСПДн РЦОИ являются:

- формирование региональной информационной системы обеспечения проведения государственной итоговой аттестации, индивидуального учета результатов освоения обучающимися образовательных программ, а также хранение данных об этих результатах на электронных носителях;
- организационно-информационное обеспечение и сопровождение проведения государственной итоговой аттестации обучающихся, освоивших образовательные программы основного общего и среднего общего образования, в том числе в форме единого государственного экзамена.

4. Перечень персональных данных, обрабатываемых в ИСПДн РЦОИ, являющихся сведениями конфиденциального характера

4.1. Сведения об участниках государственной итоговой аттестации:

– фамилия, имя, отчество;

– реквизиты документа, удостоверяющего личность;

– наименование образовательной организации, в которой освоена общеобразовательная программа;

– номер класса (группы) обучающегося;

– форма обучения;

– уровень общего образования;

– форма государственной итоговой аттестации;

– страховой номер индивидуального лицевого счёта;

– телефонный номер;

– гражданство;

– сведения о принципе рассадки;

– сведения о регионе, в котором участник закончил ОО;

– пол;

– перечень учебных предметов, выбранных для сдачи государственной итоговой аттестации;

– отнесение обучающегося к категории лиц с ограниченными возможностями здоровья, детей-инвалидов или инвалидов;

– отнесение обучающегося к категории лиц, обучающихся по образовательным программам среднего общего образования в специальных учебно-воспитательных учреждениях закрытого типа, в учреждениях, исполняющих наказание в виде лишения свободы, лиц, получающих среднее общее образование в

рамках освоения образовательных программ среднего профессионального образования, в том числе образовательных программ среднего профессионального образования, интегрированных с основными образовательными программами основного общего и среднего общего образования;

– наличие допуска у обучающегося к государственной итоговой аттестации;

– место сдачи государственной итоговой аттестации;

– результаты обработки экзаменационных работ обучающихся, участников единого государственного экзамена;

– сведения об апелляциях (номер и дата протокола, содержащего решение о результатах рассмотрения апелляции; содержание решения о результатах рассмотрения апелляции).

4.2. Сведения о лицах, привлекаемых к проведению государственной итоговой аттестации:

– фамилия, имя, отчество;

– реквизиты документа, удостоверяющего личность;

– страховой номер индивидуального лицевого счёта;

– адрес электронной почты;

– стаж работы;

– пол;

– год рождения;

– контактный телефон;

– место работы;

– должность;

– образование и квалификация;

– виды работ, к которым привлекается работник во время проведения государственной итоговой аттестации;

– место и время выполнения работ, к которым привлекается работник во время проведения государственной итоговой аттестации.

4.3. Сведения о гражданах, аккредитованных в качестве общественных наблюдателей:

– фамилия, имя, отчество;

– реквизиты документа, удостоверяющего личность;

– дата аккредитации;

– место работы;

– пол;

– год рождения;

– контактный телефон;

– страховой номер индивидуального лицевого счёта;

– образование и квалификация;

– наименование органа исполнительной власти субъекта Российской Федерации, учредителя, загранучреждения, осуществившего аккредитацию;

– реквизиты удостоверения общественного наблюдателя;

– срок действия удостоверения;

– информация о близких родственниках, сдающих ГИА;

– дата и место проведения экзамена, при проведении которого будет присутствовать общественный наблюдатель;

– информация о нарушениях, выявленных общественным наблюдателем при проведении государственной итоговой аттестации.

5. Категории ПДн

Категории ПДн, обрабатываемых в ИСПДн РЦОИ:
- Специальные и иные категории персональных данных.

6. Сроки обработки и хранения 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 3-5 статьи 21 Федерального закона № 152-ФЗ.

6.4. Основанием (условием) прекращения обработки ПДн также является ликвидация организации.

6.5. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в частях 3-5 статьи 21 Федерального закона № 152-ФЗ, АСОУ осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Организации) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.6. Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах АСОУ.

7. Порядок уничтожения ПДн

7.1. При уничтожении материальных носителей, содержащих ПДн, исключается ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

7.2. При необходимости уничтожения части ПДн уничтожается материальный носитель с предварительным копированием сведений, не подлежащих

уничтожению, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

7.3. Уничтожение части ПДн, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

7.4. По результатам уничтожения персональных данных составляется Акт по форме Приложения 4 к настоящим Правилам. Уничтожение персональных данных производится в присутствии ответственного за организацию обработки персональных данных.

8. Ответственность за нарушения при обработке ПДн

8.1. Работники РЦОИ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в пределах, определенных действующим законодательством Российской Федерации.

9. Заключительные положения

9.1. Работники РЦОИ, участвующие в обработке ПДн, должны быть ознакомлены с настоящими Правилами обработки ПДн.

9.2. Обязанность доводить до сведения сотрудников РЦОИ требования нормативно - правовых актов о ПДн и внесенные в них изменения, локальных актов по вопросам обработки ПДн, требования к защите ПДн, лежит на ответственном за организацию обработки ПДн в РЦОИ.

Приложение 1

СОГЛАСИЕ 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 организации АСОУ, зарегистрированной по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 на обработку своих персональных данных.

1. Цель обработки персональных данных:

_____.

2. Перечень персональных данных, передаваемых на обработку:

_____.

3. Перечень действий с персональными данными, передаваемыми на обработку: *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*.

4. Настоящее согласие вступает в силу со дня его подписания и действует до истечения определяемых в соответствии с Федеральным законодательством 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 2

РАЗЪЯСНЕНИЕ

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 в организацию АСОУ, зарегистрированной по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13.

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

ОБЯЗАТЕЛЬСТВО

Я, _____,
паспорт _____ серии _____ номер _____, выданный «___» _____ _____ года в период трудовых отношений с организацией АСОУ и в течении 10 (десяти) лет после их прекращения в соответствии с Политикой в отношении обработки персональных данных и требованиям к защите информации в Региональном центре обработки информации АСОУ 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 обработку 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 обработку персональных данных;

4) не производить преднамеренных действий, нарушающих достоверность, целостность или конфиденциальность персональных данных, хранимых и обрабатываемых в Региональном центре обработки информации АСОУ.

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

Мне известно, что нарушение этого обязательства может повлечь ответственность, предусмотренную трудовым, административным и уголовным законодательством Российской Федерации.

«____» _____20___ г. _____
(подпись)

Приложение 4

АКТ № _____
уничтожения персональных данных

Проведен отбор персональных данных, обрабатываемых в информационной системе персональных данных, и установлено, что отобранные персональные данные в соответствии с действующим законодательством Российской Федерации, подлежат уничтожению:

№ п/п	Дата	Субъект ПДн	Перечень ПДн	Носитель ПДн (тип, номер)	Примечание

Всего субъектов персональных данных

_____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем

_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Ответственный за организацию обработки персональных данных:

_____ _____
(ФИО) (подпись)

«____» _____20___ г.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие правила определяют основания, форму и порядок осуществления в РЦОИ внутреннего контроля соответствия обработки персональных данных (далее ПДн) в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ требованиям к защите ПДн и политике в отношении обработки ПДн.

1.2. Настоящие правила разработаны в соответствии с:

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

– постановлением 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 № 1119).

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

2. Основание проведения и сроки

2.1. В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям к защите ПДн организовывается проведение периодических проверок.

2.2. Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ (п. 4 части 1, статьи 18.1) и постановления Правительства № 1119 (п. 17).

2.3. Внутренний контроль осуществляется путем проведения плановых и внеплановых проверок, а также контроля выполнения требований постановления Правительства № 1119 не реже 1 раза в год.

2.4. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки ПДн, либо ответственного за обеспечение безопасности ПДн в ИСПДн на основании требования Федерального закона № 152-ФЗ (часть 1, статья 18.1) и постановления Правительства № 1119 (п. 17).

2.5. Основанием для проведения проверки служит издание приказа АСОУ «О проведении внутреннего контроля соответствия обработки ПДн требованиям к защите персональных данных».

3. Проведение внутреннего контроля

3.1. Внутренний контроль, а также контроль выполнения требований постановления Правительства № 1119 проводит комиссия (далее – Комиссия) в составе не менее 3-х человек, включая ответственного за организацию обработки ПДн и ответственного за обеспечение безопасности ПДн. Все члены комиссии при принятии решения обладают равными правами.

3.2. Комиссия при проведении проверки обязана:

3.2.1. провести анализ:

– реализации мер, направленных на обеспечение выполнения РЦОИ обязанностей, предусмотренных Федеральным законом № 152-ФЗ (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами в отношении обработки ПДн в ИСПДн РЦОИ;

– выполнения РЦОИ требований по определению и обеспечению уровня защищенности ПДн, утвержденных постановлением Правительства № 1119 для ИСПДн РЦОИ;

– реализации РЦОИ организационных и технических мер по обеспечению безопасности информации, утвержденных приказами ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и от 15.02.2017 № 27 «О внесении изменений в Требования о защите информации, на составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17»;

– состава оборудования, программных средств, включая средства защиты, входящих в состав ИСПДн РЦОИ на соответствие техническим паспортам ИСПДн РЦОИ;

3.2.2. установить:

– соответствие целей обработки ПДн;

– соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки;

– соблюдение правил доступа к персональным данным;

3.2.3. своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите информации (в том числе ПДн), установленных законодательными и нормативными правовыми актами Российской Федерации.

3.3. Комиссия при проведении проверки вправе:

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

– принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований к защите информации;

– вносить ректору АСОУ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

– вносить ректору АСОУ предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите информации, установленных законодательными и нормативными правовыми актами Российской Федерации.

3.4. 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.

3.5. По результатам проверки составляется Акт проверки (Приложение 1), который подписывается членами Комиссии и представляется руководителю РЦОИ.

3.6. 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 ПДн), об их характере и о лицах, допустивших указанные нарушения (если такие имеются).

3.7. Акт должен содержать заключение о соответствии или несоответствии обработки ПДн требованиям к защите информации и политике РЦОИ в отношении обработки ПДн, установленным Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

4. Заключительные положения

4.1. Пользователи ИСПДн РЦОИ, участвующие в обработке ПДн, должны ознакомиться с настоящими правилами проведения внутреннего контроля.

4.2. Обязанность доводить до сведения работников РЦОИ правила внутреннего контроля лежит на ответственном за организацию обработки ПДн.

4.3. Сотрудники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

АКТ № _____

проведения внутренней проверки условий обработки персональных данных в РЦОИ

Дата составления: «____» _____ 20 ___г.

Место проведение проверки: _____

Комиссия 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 РЦОИ в отношении обработки персональных данных проведена проверка условий обработки персональных данных в РЦОИ.

В ходе проверки:

- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом № 152-ФЗ (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами оператора определяющих его политику в отношении обработки персональных данных;

- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства № 1119;

- проведен анализ реализации оператором организационных и технических мер по обеспечению безопасности информации, 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 информационных систем персональных данных РЦОИ на соответствие их техническим паспортам;

- установлено соответствие целей обработки персональных данных, объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки, соблюдение правил доступа к персональным данным;

Выявленные нарушения:
_____
_____
_____

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует/ не соответствует (верное подчеркнуть) требованиям к защите информации 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)

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Регламент
выявления инцидентов информационной безопасности и реагирование на них

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок действий по управлению инцидентами информационной безопасности в РЦОИ.

1.2. Под инцидентом информационной безопасности (далее - инцидент) понимается событие или совокупность событий, указывающие на свершившуюся, предпринимаемую или вероятную реализацию угрозы информационной безопасности.

1.3. Инциденты информационной безопасности информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн) РЦОИ разделены на категории:

- категория 1 – отказ технических средств ИСПДн и средств защиты информации (далее – СЗИ) (отказ в обслуживании сервисов, средств обработки информации, оборудования);
- категория 2 – системные сбои или перегрузки технических средств ИСПДн и СЗИ;
- категория 3 – сбои программного обеспечения ИСПДн и СЗИ;
- категория 4 – неконтролируемые изменения конфигурации ИСПДн и СЗИ;
- категория 5 – нарушение физических мер защиты информации ИСПДн;
- категория 6 – нарушение правил доступа к информации, содержащейся в ИСПДн;
- категория 7 – несоблюдение пользователями ИСПДн требований организационно-распорядительной документации по защите информации;
- категория 8 – ошибки пользователей ИСПДн.

1.4. Любое событие (группа событий) информационной безопасности, приводящее к реализации или вероятности реализации любой из категорий п. 1.3. должны квалифицироваться как инциденты.

2. Порядок выявления инцидентов

2.1. В качестве источников информации об инцидентах могут использоваться:

- журналы и оповещения системного и прикладного программного обеспечения информационных систем, обрабатывающих защищаемую информацию, не содержащую сведения, составляющие государственную тайну (далее – ИС);
- журналы и оповещения СЗИ;

- оповещения средств обнаружения вторжений;
- информация, получаемая от сотрудников РЦОИ;
- информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

2.2. Выявление и учет инцидентов организует администратор информационной безопасности на основе сообщений пользователей ИСПДн и анализа событий информационной безопасности.

2.3. Если администратор информационной безопасности определяет текущее событие безопасности как инцидент, то он незамедлительно принимает в установленном порядке меры для устранения последствий инцидента в рамках своих должностных полномочий.

2.4. При выявлении инцидента администратор информационной безопасности осуществляет оповещение руководителя РЦОИ, ответственного за организацию обработки персональных данных и пользователей ИСПДн об инциденте. Форму и порядок оповещения устанавливает администратор информационной безопасности.

3. Порядок реагирования на инциденты

3.1. При реагировании на инциденты:

3.1.1. осуществляют анализ инцидента:

3.1.1.1. проводят оценку нанесенного материального ущерба;

3.1.1.2. выявляют неучтенные в системе защиты информации угрозы безопасности;

3.1.1.3. опасность угрозы;

3.1.1.4. области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;

3.1.1.5. потенциальные нарушители, цели и причины реализации угрозы;

3.1.2. расследуют причины возникновения инцидента;

3.1.3. устраняют причины и последствия инцидента;

3.1.4. формируют перечень мероприятий по недопущению инцидента в будущем.

3.2. Анализ инцидента организует администратор информационной безопасности с привлечением пользователей - непосредственных участников инцидента.

3.3. Анализ проводит комиссия, состав которой определяет администратор информационной безопасности.

3.4. Сроки анализа инцидента определяются по категории инцидента. Анализ инцидентов 1 – 3 категорий проводят немедленно после возникновения инцидента в целях максимального ускорения устранения последствий инцидента. Анализ инцидентов 4 – 8 категорий проводят не позднее 1 рабочего дня с момента возникновения инцидента.

3.5. Анализ инцидента оформляется Актом расследования инцидента информационной безопасности по форме Приложения 1 к настоящему Регламенту.

3.6. Устранение причин и последствий инцидента осуществляет администратор информационной безопасности совместно с ответственным за организацию обработки персональных данных.

4. Порядок разбирательства по инциденту

4.1. Внутреннее расследование (разбирательство) – деятельность комиссии, направленная на сбор, анализ и оценку информации и документов в целях установления причин и виновных лиц в совершении деяния, повлекшего неблагоприятные последствия для РЦОИ, его подразделений или отдельных работников.

4.2. Внутреннее расследование проводится при получении сведений о фактах нарушения режима конфиденциальности информации, обрабатываемой в ИСПДн, либо о фактах приготовления или попыток к его нарушению.

4.3. Проведение внутреннего расследования осуществляет комиссия, назначаемая администратором информационной безопасности.

4.4. Администратор информационной безопасности организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений РЦОИ, готовит и ведёт заседания комиссии, подписывает протоколы заседаний.

4.5. При проведении внутреннего расследования устанавливаются:

4.5.1. наличие самого факта совершения деяния, служащего основанием для вынесения соответствующего решения;

4.5.2. время, место и обстоятельства совершения противоправного деяния, а также оценка его последствий;

4.5.3. конкретный работник, совершивший установленное деяние;

4.5.4. наличие и степень вины работника в совершении деяния;

4.5.5. цели и мотивы совершения деяния и их оценки, оценки обстоятельств, смягчающих или отягчающих ответственность, в том числе причин и условий, способствовавших совершению данного деяния.

4.6. В целях внутреннего расследования все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

4.7. Работник, совершивший установленное деяние, нарушивший режим защиты информации или делавший попытки (приготовления) к его нарушению, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений комиссией составляется акт.

4.8. Работник имеет право, по согласованию с администратором информационной безопасности, знакомиться с материалами расследования, касающимися лично его, и давать по поводу них свои комментарии, предоставлять

дополнительную информацию и документы. По окончании расследования работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

4.9. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом председателю комиссии.

4.10. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения внутреннего расследования и ставшие известные им обстоятельства.

4.11. В процессе проведения внутреннего расследования комиссией выясняются:

4.11.1. перечень разглашенных документов и сведений, составляющих конфиденциальную информацию;

4.11.2. причины разглашения конфиденциальной информации;

4.11.3. лица, виновные в разглашении;

4.11.4. размер (экспертную оценку) причиненного ущерба;

4.11.5. недостатки и нарушения, допущенные работниками при работе с конфиденциальной информацией;

4.11.6. иные обстоятельства, необходимые для определения причин разглашения конфиденциальной информации, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

4.12. По завершении внутреннего расследования комиссией составляется заключение. В заключении указываются:

4.12.1. основание для проведения внутреннего расследования;

4.12.2. состав комиссии и время проведения внутреннего расследования;

4.12.3. сведения о времени, месте и обстоятельствах совершения противоправного деяния;

4.12.4. сведения о работнике, совершившем противоправное деяние (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемой должности);

4.12.5. мотивы и цели совершения работником противоправного деяния;

4.12.6. причины и условия совершения деяния;

4.12.7. данные о характере и размерах причиненного в результате противоправного деяния ущерба, причинную связь деяния и причиненного ущерба;

4.12.8. предложения о мере ответственности работника, совершившего противоправное деяние.

4.13. На основании заключения выносится решение о применении мер ответственности к работнику, виновному в разглашении конфиденциальной информации, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

4.14. Все материалы внутренних расследований относятся к конфиденциальным сведениям и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам внутреннего расследования приобщаются к личному делу работника, в отношении которого оно проводилось.

5. Порядок устранения последствий инцидента

5.1. Ответственным лицом за устранение последствий инцидента в РЦОИ является администратор информационной безопасности. При устранении последствий инцидента администратор информационной безопасности вправе привлекать к работам по устранению инцидента системного администратора.

5.2. При нарушении конфиденциальности информации, обрабатываемой в ИСПДн или подозрении в ее нарушении администратор информационной безопасности:

5.2.1. проводит процедуру смены паролей пользователям;

5.2.2. пересматривает и обновляет, с учетом содержания инцидента, матрицу доступа к ресурсам ИСПДн.

5.3. При нарушении целостности и доступности информации администратор информационной безопасности:

5.3.1. организует переустановку программного обеспечения ИСПДн и системы защиты информации с дистрибутивных носителей используемого программного обеспечения;

5.3.2. организует переустановку обрабатываемой информации с резервных копий.

5.3.3. проверяет конфигурацию ИСПДн и ее системы защиты информации (при необходимости совместно с администратором ИСПДн восстанавливает конфигурацию в соответствии с эксплуатационной документацией).

6. Порядок устранения причин инцидента

6.1. Причины инцидентов в ИСПДн разделяют на типы:

6.1.1. аппаратно–программные причины;

6.1.2. организационные причины;

6.2. К аппаратно–программным причинам относятся все причины, связанные с недостатками аппаратной и программной частей ИСПДн и ее системы защиты информации (ошибки кода, ошибки настроек, неисправности оборудования, электромагнитная совместимость и т.п.).

6.3. К организационным причинам относятся недостатки организационно-распорядительной документации, ошибки пользователей, недостатки физической защиты доступа, дисциплинарные, злой умысел и т.п.

6.4. Устранение аппаратно–программных причин инцидентов осуществляет администратор информационной безопасности. Сроки и состав действий определяются индивидуально по каждому инциденту.

6.5. Устранение организационных причин осуществляет администратор информационной безопасности. Сроки и состав действий устанавливаются индивидуально по каждому инциденту.

7. Заключительные положения

7.1. Администратор информационной безопасности должен быть предупрежден об ответственности за действия, нарушающие требования настоящего Регламента и прилагаемой к нему Инструкцией.

7.2. Администратор информационной безопасности должен быть ознакомлен с настоящим Регламентом и прилагаемой к нему Инструкцией до начала работы с ИСПДн под роспись.

7.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Регламентом и прилагаемой к нему Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

АКТ № _____

расследования инцидента информационной безопасности ИСПДн РЦОИ

Дата составления: «____» _____ 20 ___г.

Место проведение проверки: _____

Комиссия в составе:

Председатель

_____(Ф.И.О.)

Члены комиссии:

_____(Ф.И.О.)

_____(Ф.И.О.)

Провела расследование инцидента информационной безопасности: _____

_____

В ходе расследования выявлен нанесенный организации ущерб: _____

_____

и причины инцидента: _____

_____

Заключения и выводы комиссии:

_____

_____

Предписания:

_____

Председатель комиссии _____ (подпись)

Члены комиссии _____ (подпись)

_____ (подпись)

Приложение 2

Инструкция
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в РЦОИ возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это.

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя ИСПДн или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных, в соответствии с решением руководителя РЦОИ может быть наложено дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами РЦОИ, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Положение
о порядке рассмотрения запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных

1. В настоящем Положении о порядке рассмотрения запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных (далее – Положение) в РЦОИ определяются порядок учета (регистрации), рассмотрения запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных (далее – запросы).

2. Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Трудового кодекса Российской Федерации и другими нормативно-правовыми актами АСОУ.

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона), в том числе содержащей:

- подтверждение факта обработки персональных данных в РЦОИ;
- правовые основания и цели обработки персональных данных;
- цели и применяемые в РЦОИ способы обработки персональных данных;
- наименование и место нахождения РЦОИ, сведения о лицах (за исключением работников РЦОИ), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании закона Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению РЦОИ, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

Типовые варианты запросов субъектов персональных данных представлены в приложениях № 3-6 к настоящему Положению.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничен в соответствии с положениями части 8 статьи 14 Федерального закона.

5. Субъект персональных данных вправе требовать от РЦОИ уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Предоставление персональных данных третьим лицам осуществляется только с предварительного письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством Российской Федерации.

9. Письменный запрос должен быть адресован на оператора персональных данных АСОУ, ректора АСОУ или уполномоченного ректором лицо. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с АСОУ (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных РЦОИ, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

10. Рассмотрение запросов является служебной обязанностью лица, ответственного за организацию обработки персональных данных РЦОИ, при необходимости, уполномоченных должностных лиц РЦОИ, в чьи обязанности входит обработка персональных данных.

11. Доступ к персональным данным должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей. Доступ работников РЦОИ к информационным системам персональных данных ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты

персональных данных с использованием технических и организационных мероприятий.

12. Общие действия по реагированию на запросы субъектов персональных данных и их законных представителей, обоснованные требованиями законодательства Российской Федерации представлены в приложении № 1 к настоящему Положению.

13. Должностные лица РЦОИ обеспечивают:

- объективное, всестороннее и своевременное рассмотрение запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;
- направление письменных ответов по существу запроса.

14. Копии документов, содержащих персональные данные субъекта персональных данных, выдаются РЦОИ в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче. При выдаче документов для ознакомления, а также запрашиваемых копий и справок, уполномоченный сотрудник, занимающийся обработкой персональных данных, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

15. Все поступившие запросы регистрируются в день их поступления. На запросе проставляются входящий номер и дата регистрации.

16. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в РЦОИ или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в РЦОИ или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

17. РЦОИ в праве отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

18. Прошедшие регистрацию запросы в тот же день докладываются руководителю РЦОИ либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них указание исполнителям.

19. После регистрации запроса субъекта персональных данных или его законного представителя, лицу, ответственному за организацию обработки персональных данных в РЦОИ необходимо зарегистрировать запрос в Журнале учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных (приложение № 2 к настоящему Положению).

20. Лицо, ответственное за организацию обработки персональных данных в РЦОИ и уполномоченные должностные лица РЦОИ, в чьи обязанности входит обработка персональных данных РЦОИ при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться по существу запроса, в случае необходимости истребовать дополнительные материалы или направить сотрудников РЦОИ на места для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;
- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса – разъяснять также порядок обжалования принятого решения.

Типовые варианты ответов на запросы субъектов персональных данных представлены в приложениях № 7-13 к настоящему Положению.

21. РЦОИ обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

22. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении уполномоченные должностные лица РЦОИ обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного закона Российской Федерации, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

23. РЦОИ обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

24. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные должностные лица РЦОИ обязаны внести в них необходимые изменения.

25. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица РЦОИ обязаны уничтожить такие персональные данные.

26. Ответы на запросы субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных регистрируются лицом, ответственным за организацию обработки персональных данных в РЦОИ в Журнале учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных.

27. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица РЦОИ обязаны осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных с момента такого обращения или получения указанного запроса на период проверки.

28. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица РЦОИ обязаны осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

29. В случае подтверждения факта неточности персональных данных уполномоченные должностные лица РЦОИ на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязаны уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

30. В случае выявления неправомерной обработки персональных данных уполномоченные должностные лица РЦОИ в срок, не превышающий трех рабочих

дней с даты этого выявления, обязаны прекратить неправомерную обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных невозможно, уполномоченные должностные лица РЦОИ в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных РЦОИ обязано уведомить субъекта персональных данных или его представителя, а в случае, если обращение было направлено уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

31. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

32. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения должностным лицом РЦОИ действия (бездействия), содержащего признаки административного правонарушения результаты служебной проверки незамедлительно докладываются руководителю РЦОИ.

33. Субъект персональных данных вправе обжаловать неправомерные действия или бездействия должностных лиц РЦОИ при обработке и защите его персональных данных, направив обращение в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

34. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

35. Ответы на запросы печатаются на бланке установленной формы и регистрируются в соответствии с порядком делопроизводства, установленным в АСОУ.

36. Руководитель РЦОИ:

– осуществляет непосредственный контроль за соблюдением установленного законодательством и настоящим Положением порядка рассмотрения запросов;

– осуществляет контроль за работой с запросами и организацией их приема как лично, так и через своих заместителей. На контроль берутся все запросы.

37. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

38. Нарушение установленного порядка рассмотрения запросов влечет в отношении должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 1

Сводная таблица действий уполномоченных лиц РЦОИ
в ответ на запросы субъектов персональных данных или их представителей

№	Запрос	Действия	Срок	Ответ
1. Запрос Субъекта персональных данных или его Представителя				
1.1.	Наличие персональных данных	Подтверждение обработки персональных данных	30 дней (согласно пункту 1 статьи 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ))	Подтверждение обработки персональных данных
		Отказ подтверждения обработки персональных данных	30 дней (согласно пункту 2 статьи 20 152-ФЗ)	Уведомление об отказе подтверждения обработки персональных данных
1.2.	Ознакомление с персональными данными	Предоставление информации по персональным данным	30 дней (согласно пункту 1 статьи 20 152-ФЗ)	1. Подтверждение обработки персональных данных, а также правовые основания и цели такой обработки
				2. Способы обработки персональных данных
				3. Сведения о лицах, которые имеют доступ к персональным данным
				4. Перечень обрабатываемых персональных данных и источник их получения
				5. Сроки обработки персональных данных, в том числе сроки их хранения
				6. Информация об осуществленной или о предполагаемой трансграничной передаче
		Отказ предоставления информации по персональным данным	30 дней (согласно пункту 2 статьи 20 152-ФЗ)	Уведомление об отказе предоставления информации по персональным данным

№	Запрос	Действия	Срок	Ответ
1.3.	Уточнение персональных данных	Изменение персональных данных	7 рабочих дней со дня предоставления уточняющих сведений (согласно пункту 3 статьи 20 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения персональных данных	30 дней	Уведомление об отказе изменений персональных данных
1.4.	Уничтожение персональных данных	Уничтожение персональных данных	7 рабочих дней со дня предоставления сведений о незаконном получении персональных данных или отсутствии необходимости персональных данных для заявленной цели обработки (согласно пункту 3 статьи 20 152-ФЗ)	Уведомление об уничтожении
		Отказ уничтожения персональных данных	30 дней	Уведомление об отказе уничтожения персональных данных
1.5.	Отзыв согласия на обработку персональных данных	Прекращение обработки и уничтожение персональных данных	3 рабочих дня (согласно пункту 5 статьи 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении персональных данных
		Отказ прекращения обработки и уничтожения персональных данных	30 дней	Уведомление об отказе прекращения обработки и уничтожения персональных данных
1.6.	Недостоверность персональных данных Субъекта	Блокировка персональных данных	С момента обращения Субъекта персональных данных о недостоверности его персональных данных или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных	7 рабочих дней со дня	

№	Запрос	Действия	Срок	Ответ
		данных	предоставления уточненных сведений (согласно пункту 2 статьи 21 152-ФЗ)	
		Снятие блокировки персональных данных		
		Отказ изменения персональных данных	30 дней	Уведомление об отказе изменения персональных данных
1.7.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение персональных данных в случае невозможности обеспечения Правомерности обработки	10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об уничтожении персональных данных
2. Запрос Уполномоченного органа по защите прав субъектов персональных данных				
2.1.	Информация для осуществления деятельности уполномоченного органа	Предоставление затребованной информации по персональным данным	30 дней (согласно пункту 4 статьи 20 152-ФЗ)	Предоставление затребованной информации по персональным данным
2.2.	Недостоверность персональных данных Субъекта	Блокировка персональных данных	С момента обращения Уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно пункту 1 статьи 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение персональных данных	7 рабочих дней со дня предоставления уточненных	

№	Запрос	Действия	Срок	Ответ
		Снятие блокировки персональных данных	сведений (согласно пункту 2 статьи 21 152-ФЗ)	
		Отказ изменения персональных данных	30 дней	Уведомление об отказе изменения персональных данных
2.3.	Неправомерность действий с персональными данными Субъекта	Прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно пункту 3 статьи 21 152-ФЗ)	Уведомление об уничтожении персональных данных

Приложение 2

ЖУРНАЛ
учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных

№ п/п	Дата, № и реквизит запроса	Запрашивающее лицо (ФИО, адрес)	Краткое содержание обращения	Цель запроса	Отметка о предоставлении или отказе в предоставлении информации	Дата предоставления/ отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8	9
1	*№ вх- __от __*	*Иванов И.И., РФ г. Иванов, ул. Иванова, д.1, кв. 1*	*перечень измененных персональных данных*	*уточнение персональных данных*	*отправлено почтовое уведомление №233 об уточнении ПДн*	*1.01.2021*	*_____ (Петров П.П.)*	*Пример заполнения*

Образец журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных

ПРАВИЛА
по формированию и ведению журнала учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
   1.2. Обложка журнала формируется на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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. Столбцы журнала заполняются следующим образом:
      1 – номер записи по порядку;
      2 – дата, № и реквизит запроса;
      3 – ФИО и адрес субъекта персональных данных, обратившегося по вопросу обработки его персональных данных;
      4 – краткое содержание обращения;
      5 – краткое содержание цели обращения субъекта персональных данных;
      6 – запись о действии в ответ на обращение;
      7 – дата отправки уведомления субъекту персональных данных;
      8 – подпись сотрудника, отправившего уведомление субъекту персональных данных;
      9 – любая дополнительная информация, относящаяся к обращению субъекта персональных данных.
   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 3

Форма запроса субъекта персональных данных о наличии и ознакомлении с персональными данными

Оператору персональных данных АСОУ
Адрес: 141006 г. Мытищи, ул. Индустриальная, д.13
от _____
адрес: _____
_____
паспорт серия_____№_____
выдан _____
_____

ЗАПРОС

В соответствии с положениями статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», я имею право получить от вас сведения о наличии моих персональных данных.

Прошу вас предоставить мне следующую информацию об обработке моих персональных данных:

 подтверждение факта обработки моих персональных данных;

 правовые основания и цели обработки моих персональных данных;

 цели и применяемые способы обработки моих персональных данных;

 наименование и место нахождение оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к моим персональным данным или которым могут быть раскрыты персональные данные на основании договора или на основании закона Российской Федерации;

 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;

 информацию об осуществленной или о 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, предусмотренные Федеральным законом или другими федеральными законами).

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

(указать причину направления повторного запроса)

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

Дата Подпись с расшифровкой

Приложение 4

Форма запроса субъекта персональных данных на уточнение персональных данных

Оператору персональных данных АСОУ
Адрес: 141006 г. Мытищи, ул. Индустриальная, д.13
от _____
адрес: _____
_____
паспорт серия_____№_____
выдан _____
_____

ЗАПРОС

В соответствии с положениями статьи 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с

_____

(сведения, подтверждающие факт обработки персональных данных)

прошу уточнить/внести следующие изменения в мои персональные данные:

_____

_____

по причине:

_____

(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)

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

Дата Подпись с расшифровкой

Приложение 5

Форма запроса субъекта персональных данных на уничтожение персональных данных

Оператору персональных данных АСОУ
Адрес: 141006 г. Мытищи, ул. Индустриальная, д.13
от _____
адрес: _____
_____
паспорт серия_____№_____
выдан _____
_____

ЗАПРОС

В соответствии с положениями статьи 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с

_____

(сведения, подтверждающие факт обработки персональных данных)

прошу вас уничтожить следующие мои персональные данные:

_____

_____

по причине:

_____

(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)

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

Дата Подпись с расшифровкой

Приложение 6

Форма заявления субъекта персональных данных об отзыве согласия на обработку персональных данных

Оператору персональных данных АСОУ
Адрес: 141006 г. Мытищи, ул. Индустриальная, д.13
от _____
адрес: _____
_____
паспорт серия_____№_____
выдан _____
_____

ЗАЯВЛЕНИЕ

В соответствии с положениями статьи 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с

_____
(сведения, подтверждающие факт обработки персональных данных)

прошу вас прекратить обработку моих персональных данных, осуществляемую в целях:

_____

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

по причине:

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

Дата Подпись с расшифровкой

Приложение 7

Формы ответа на запрос субъекта персональных данных о наличии и на ознакомление с персональными данными

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно обработки Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 в период с «____» _____ 20_____г. по настоящее время с целью

_____
(цели обработки персональных данных)

_____

обрабатывает следующие полученные от Вас персональные данные:

_____
(категории персональных данных)

_____

_____

Эта информация обрабатывается на основании

_____
(правовое основание обработки персональных данных)

_____

в соответствии с законодательством Российской Федерации о персональных данных, в Ваших интересах и с Вашего согласия.

Обработка Ваших персональных данных включает сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Обработкой Ваших персональных данных занимаются сотрудники нашей организации, ознакомленные с обязанностями, возложенными на них в связи с обработкой Ваших персональных данных, и давшие подписку об их неразглашении. Никто другой к обработке Ваших персональных данных не допускается. Ваши персональные данные будут обрабатываться вплоть до достижения указанных целей, но не позже_____ лет с момента Вашего обращения в нашу организацию, то есть до «____» _____ 20_____ г.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /

(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно обработки Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не осуществляет обработку Ваших персональных данных.

С уважением,

_____ /_____ /

(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно обработки Ваших персональных данных сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 Вам отказано в предоставлении сведений по запросу от _____

(дата запроса)

на основании _____

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

С уважением,

_____ /_____ /

(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 8

Формы ответа на запрос субъекта персональных данных на уточнение персональных данных

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно уточнения/внесения изменений в Ваши персональные данные сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 были уточнены/внесены изменения в Ваши персональные данные:

_____
(категории персональных данных)
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно уточнения/внесения изменений в Ваши персональные данные сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не может уточнить/внести изменения в Ваши персональные данные, так как Вами не было предоставлено необходимых документов, подтверждающих запрашиваемые Вами изменения.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 9

Формы ответа на запрос субъекта персональных данных на уничтожение персональных данных

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно уничтожения Ваших персональных данных сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 были уничтожены Ваши персональные данные:

_____
(категории персональных данных)

_____

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно уничтожения Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не может уничтожить Ваши персональные данные, так как их обработка осуществляется на основании:

_____
(правовое основание обработки персональных данных)

в целях:

_____
(цели обработки персональных данных)

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 10

Формы ответа на запрос субъекта персональных данных об отзыве согласия на обработку персональных данных

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно отзыва согласия на обработку Ваших персональных данных сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 была прекращена обработка и уничтожены Ваши персональные данные:

_____
(категории персональных данных)

_____

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно отзыва согласия на обработку Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 уведомляет Вас о невозможности отзыва согласия на обработку персональных данных в связи с тем, что оператор не может прекратить обработку и уничтожить Ваши персональные данные, так как их обработка осуществляется на основании:

_____
(правовое основание обработки персональных данных)

в целях:

_____
(цели обработки персональных данных)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /

(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 11

Формы ответа на запрос субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении недостоверности персональных данных

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно недостоверности Ваших персональных данных сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 были внесены изменения в Ваши персональные данные:

_____
(категории персональных данных)

_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно недостоверности Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не может внести изменения в Ваши персональные данные, так как факт недостоверности не подтвержден и не было предоставлено необходимых документов, подтверждающих недостоверность персональных данных.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 12

Формы ответа на запрос субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении неправомерности действий с персональными данными

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно неправомерности действий с Вашими персональными данными сообщаем следующее.

Оператором персональных данных АСОУ, находящимся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 были устранены нарушения/уничтожены Ваши персональные данные:

_____
(категории персональных данных)

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В ответ на Ваш запрос от «____» _____ 20_____ г. относительно неправомерности действий с Вашими персональными данными сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не может устранить нарушения/уничтожить Ваши персональные данные, так как факт неправомерности действий с Вашими персональными данными не подтвержден и не было предоставлено необходимых документов, подтверждающих неправомерность действий с Вашими персональными данными.

Обработка Ваших персональных данных осуществляется в соответствии с:

_____
(правовое основание обработки персональных данных)

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

Приложение 13

Формы уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при блокировании персональных данных

Субъекту персональных данных:

_____
(ФИО)

Адрес: _____

УВЕДОМЛЕНИЕ

В связи с блокированием Ваших персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 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)

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /
(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

В отношении блокирования персональных данных сообщаем следующее.

Оператор персональных данных АСОУ, находящийся по адресу: 141006 г. Мытищи, ул. Индустриальная, д.13 не может осуществить блокирование персональных данных _____
(ФИО субъекта персональных данных)

так как не было предоставлено необходимых документов, подтверждающих основания для блокирования персональных данных.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой персональных данных, пожалуйста, обращайтесь.

С уважением,

_____ /_____ /

(должность ответственного сотрудника) *(подпись)* *(расшифровка подписи)*

(дата, печать организации)

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных

1. Область действия

1.1. Настоящий документ определяет порядок взаимодействия АСОУ с уполномоченным органом по защите прав субъектов персональных данных.

1.2. Перед началом обработки персональных данных (далее – ПДн) АСОУ уведомляет уполномоченный орган по защите прав субъектов ПДн (далее – Роскомнадзор) о своем намерении осуществлять обработку ПДн.

1.3. АСОУ вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов ПДн обработку ПДн:

1.3.1. обрабатываемых в соответствии с трудовым законодательством;

1.3.2. полученных АСОУ в связи с заключением договора, стороной которого является субъект ПДн, если ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

1.3.3. сделанных субъектом общедоступными ПДн;

1.3.4. включающих в себя только фамилии, имена и отчества субъектов ПДн;

1.3.5. необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится РЦОИ;

1.3.6. обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн.

1.4. Уполномоченный орган по защите прав субъектов ПДн имеет право:

1.4.1. запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий и безвозмездно получать такую информацию;

1.4.2. осуществлять проверку сведений, содержащихся в уведомлении об обработке ПДн или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;

1.4.3. требовать от оператора уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

1.4.4. принимать в установленном законодательством Российской Федерации порядке меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований ФЗ-152 «О персональных данных».

2. Порядок взаимодействия с Роскомнадзор

2.1. В случае неполноты или изменения сведений, указанных в уведомлении об обработке ПДн, а также в случае прекращения обработки ПДн АСОУ уведомляет об изменениях уполномоченный орган по защите прав субъектов ПДн в срок, не превышающий десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн. Ответственный за организацию обработки ПДн направляет в адрес уполномоченного органа по защите прав субъектов ПДн уведомление об изменениях в реквизитах оператора ПДн.

2.2. Полученные запросы уполномоченного органа по защите прав субъектов ПДн регистрируются ответственным за организацию обработки ПДн в Журнале учета запросов и обращений субъектов персональных данных, их законных представителей и контролирующих государственных органов при обработке персональных данных (далее – Журнал).

2.3. Ответственный за организацию обработки ПДн оценивает правомерность полученных запросов в адрес АСОУ.

2.4. Ответственный за организацию обработки ПДн в течение тридцати календарных дней с момента получения запроса формирует ответ на запрос.

2.5. При получении правомерного запроса на исправление выявленных нарушений по распоряжению ответственного за организацию обработки ПДн администраторы ИС, в которых обрабатываются указанные ПДн, разрабатывают перечень действий по устранению выявленных нарушений и согласуют перечень предлагаемых действий с заинтересованными подразделениями АСОУ.

2.6. Устранение выявленных нарушений должно быть произведено в срок, не превышающий трех рабочих дней со дня выявления нарушений. По факту устранения нарушений формируется Уведомление об устранении нарушений в порядке обработки ПДн. Ответственный за организацию обработки персональных данных регистрирует уведомление в Журнале и пересылает уведомление в Роскомнадзор.

2.7. В случае если обеспечить правомерность обработки ПДн невозможно, по распоряжению ответственного за организацию обработки ПДн администраторы ИС, в которых обрабатываются указанные ПДн в срок, не превышающий десяти рабочих дней со дня издания распоряжения уничтожают указанные ПДн с составлением соответствующего Акта.

2.8. Ответственный за организацию обработки ПДн формирует уведомление об уничтожении ПДн, регистрирует уведомление в Журнале и отправляет в Роскомнадзор.

2.9. По факту внесения изменений в ПДн на основании запроса уполномоченного органа по защите прав субъектов ПДн, ответственный за организацию обработки ПДн формирует уведомление о внесении изменений в ПДн, регистрирует его в Журнале и отправляет в Роскомнадзор.

2.10. По окончании проведения Уполномоченным органом по защите прав субъектов ПДн проверок, должностное лицо Уполномоченного органа по защите прав субъектов ПДн производит запись о проведенной проверке в журнал учета проверок.

2.11. Журнал учета проверок должен быть прошит, пронумерован и удостоверен печатью Академии. Форма журнала не регламентирована.

2.12. Ответственность за ведение и хранение Журнала учета проверок возлагается на ответственного за организацию обработки ПДн.

3. Взаимодействие с Роскомнадзор через сеть internet

3.1. Официальный сайт уполномоченного органа - Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является основным средством для обеспечения возможности обращений граждан и юридических лиц в Роскомнадзор.

3.2. Для подготовки и отправки уведомлений от организаций, обрабатывающих персональные данные нужно выйти на официальный сайт Роскомнадзора в информационно-телекоммуникационной сети Интернет по адресу http://pd.rkn.gov.ru/operators-registry/notification/form/.

3.3. После того, как откроется соответствующая форма ее следует заполнить и отправить в информационную систему Роскомнадзора.

3.4. После заполнения формы уведомления о намерении осуществлять обработку ПДн и отправки ее в информационную систему Уполномоченного органа по защите прав субъектов ПДн, необходимо распечатать заполненную форму, после чего ее подписать и направить в соответствующий территориальный орган Роскомнадзора по месту регистрации АСОУ.

4. Заключительные положения

4.1. Работники, осуществляющие обработку ПДн, должны быть ознакомлены с данной инструкцией под подпись.

4.2. Обязанность организации выполнения требований данной инструкции лежит на ответственном за организацию обработки ПДн.

4.3. Работники АСОУ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Положение
о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники

1. Основные понятия, термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Общие положения

Настоящее Положение определяет порядок резервного копирования и восстановления информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники РЦОИ.

Настоящее Положение разработано на основании требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных правовых актов Российской Федерации.

Требования настоящего Положения распространяются на работников РЦОИ, в функциональные обязанности которых входит резервирование и восстановление информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники РЦОИ.

Все изменения в Положение вносятся приказом ректора (или лица, исполняющего его должностные обязанности) АСОУ.

Настоящее Положение о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники в РЦОИ, разработано с целью:

- определения порядка резервного копирования информации, содержащей персональные данные для последующего восстановления работоспособности информационных систем персональных данных, в том числе государственных

информационных систем при полной или частичной потере информации, содержащей персональные данные, вызванной сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- определения порядка восстановления информации, содержащей персональные данные в случае возникновения такой необходимости;
- упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, содержащей персональные данные.

В настоящем документе регламентируются действия ответственных лиц РЦОИ при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация, обрабатываемая в информационных системах персональных данных РЦОИ, содержащая персональные данные физических лиц (субъектов персональных данных).

Машинным носителям информации, содержащим резервную копию, присваивается степень конфиденциальности, соответствующая той, к которой отнесены персональные данные соответствующей информационной системы.

3. Порядок резервного копирования

Резервное копирование информации, содержащей персональные данные, производится на основании следующих данных:

- резервируемая информация информационных систем персональных данных в соответствии с Приложением 1 к настоящему Положению;
- максимальный срок хранения резервных копий – 10 лет;
- хранение 4-х следующих архивов;
    - архив, сделанный на текущий день
    - архив на конец текущей недели;
    - архив на 1-е число текущего месяца;
    - архив, сделанный на конец года.

Резервное копирование информации, содержащей персональные данные, производится администратором информационной безопасности.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, содержащей персональные данные, в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в Приложении 2 к настоящему Положению.

Технология создания резервных копий определяется правилами эксплуатации технических и программных средств.

Для создания резервных копий данных могут использоваться жесткие диски серверов и ПЭВМ, сменные (съемные) носители информации (CD/DVD, flash-накопители, внешние жесткие диски и т.п.), зарегистрированные в соответствии с

правилами работы с документами, содержащими информацию ограниченного доступа.

Носители созданных резервных копий данных должны быть промаркированы администратором информационной безопасности. Маркировка должна содержать номер копии, дату ее создания, наименование информационной системы персональных данных.

При создании резервных копий допускается их архивирование специальными программными средствами.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, администратор информационной безопасности сообщает руководителю РЦОИ служебной запиской после обнаружения указанного события и доводит до сведения администратора информационной системы персональных данных.

4. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется встроенными средствами контроля целостности СУБД (системы управления базами данных), отвечающей за хранение и обработку персональных данных.

В случае обнаружения ошибки при осуществлении резервного копирования, лица, ответственные за контроль результатов, осуществляют все необходимые действия по устранению ошибки. При необходимости резервное копирование осуществляется повторно.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для её хранения.

5. Замена носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации информационных систем персональных данных в случае отказа любого из устройств резервного копирования.

В случае необходимости замены испорченных носителей информации новыми, администратор информационной безопасности заблаговременно за 10 рабочих дней согласовывает спецификации новых носителей информации с администратором информационной системы персональных данных.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение осуществляются администратором информационной безопасности по запросу и в присутствии администратора информационной системы персональных данных.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна быть гарантированно уничтожена. Для гарантированного уничтожения информации допускается использование специального программного обеспечения.

Для хранения носителей резервных копий должны использоваться хранилища, создающие оптимальные условия для физической сохранности и защиты от воздействия неблагоприятных факторов.

6. Восстановление информации из резервных копий

Основанием для инициирования процедуры восстановления служит мотивированная заявка руководителя РЦОИ на имя администратора информационной безопасности. Восстановление данных производится после согласования с администратором информационной системы персональных данных.

После согласования заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы.

Восстановление данных из резервной копии осуществляется администратором информационной безопасности на специализированных рабочих местах, оснащенных необходимыми техническими средствами.

Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации (Приложение 3 к настоящему Положению).

Приложение 1

Резервируемая информация

№ п/п	Наименование информационной системы персональных данных	Размещение хранилища резервной копии информации
1.	ГИС «АИС РЦОИ РИС МО»	Серверная

Приложение 2

Методика резервного копирования

Для организации системы резервного копирования используются встроенные средства СУБД.

С помощью указанного ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Источником информации, подлежащей резервированию, являются базы данных информационных систем персональных данных.

Для резервирования информации, хранимой в базах данных информационных систем персональных данных, используются встроенные средства СУБД. В результате работы встроенных средств формируется каталог с резервной копией данных информационной системы.

Приложение 3

Методика восстановления данных

Любое восстановление информации, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы или ее компонент, выполняется администратором информационной безопасности на основании заявки руководителя РЦОИ.

В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанными в документации, прилагающейся к ПО, с помощью которого выполнялась процедура резервного копирования.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по организации резервного копирования

1. Общие положения

1.1. Настоящая Инструкция резервного копирования (далее – Инструкция) устанавливает основные требования к организации резервного копирования и восстановления персональных данных, содержащихся в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ.

1.2. Ответственность за организацию резервного копирования и восстановления персональных данных в ИСПДн возлагается на администратора информационной безопасности.

1.3. Резервное копирование осуществляется на носители, определённые в настоящей Инструкции.

1.4. Периодичность резервного копирования проводится в сроки, определённые настоящей Инструкцией.

1.5. Ответственность за надлежащее хранение резервных носителей персональных данных, возлагается на администратора информационной безопасности.

2. Информация, подлежащая резервному копированию

2.1. Информация, обрабатываемая в РЦОИ, может быть разделена на следующие типы:

- системное программное обеспечение;
- прикладное программное обеспечение общего назначения;
- специализированное программное обеспечение;
- открытая информация;
- информация ограниченного доступа (персональные данные).

2.2. Системное программное обеспечение поставляется производителем программного обеспечения и не требует организации резервного копирования. Если это программное обеспечение поставляется на других носителях, то возможность его копирования определяется лицензионным соглашением с производителем.

2.3. Прикладное программное обеспечение общего назначения также поставляется производителем данного программного обеспечения. Возможности его копирования (в том числе для резервного хранения) определяются условиями лицензионного соглашения. Как правило, современное программное обеспечение поставляется на CD\DVD-ROM и не требует резервного копирования.

2.4. Лица, имеющие доступ к носителям и отвечающие за их сохранность, не должны допускать несанкционированного копирования носителей со специализированным программным обеспечением (ПО).

2.5. Открытая информация - это информация, доступная всем лицам, а также информация, предназначенная для опубликования в открытой печати. Открытая информация подлежит обязательному резервному копированию с периодичностью, определяемой настоящей Инструкцией.

2.6. Информация ограниченного доступа (персональные данные) подлежит обязательному резервному копированию. Доступ к информации и её резервной копии должен быть ограничен. Резервное копирование персональных данных должно производиться только на носители, предназначенные для хранения персональных данных.

3. Аппаратное обеспечение резервного копирования и восстановления информации

3.1. Для резервного копирования и восстановления информации в РЦОИ должно быть оборудовано соответствующими техническими средствами.

3.2. Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные машинные носители информации.

3.3. Электронные носители, предназначенные для длительного хранения информации, должны периодически проверяться на их пригодность и отсутствие сбойных секторов. При появлении сбойных секторов на электронных носителях информация с этих носителей должна переносится на исправные. Если на неисправных носителях содержались персональные данные, то они должны уничтожаться.

4. Периодичность резервного копирования

4.1. Резервное копирование специализированного программного обеспечения производиться при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Информация (открытая и ограниченного доступа), содержащаяся в постоянно изменяемых базах данных ИСПДн, должна сохраняться в соответствии со следующим графиком:

– ежедневно должно проводиться копирование изменённой и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели.

– еженедельно должно проводиться резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца.

– ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

– ежегодно (на конец года) производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится до истечения срока хранения резервных копий.

5. Порядок восстановления работоспособности ИСПДн

5.1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и информационных систем, а также их программного обеспечения.

5.2. Данные работы осуществляются администратором информационной безопасности в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

5.3. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности и администратора информационной системы персональных данных.

6. Восстановление информации

6. Восстановление информации происходит по распоряжению руководителя РЦОИ с согласованием последовательных действий с администратором информационной безопасности и администратором информационной системы персональных данных в случаях:

6.1.1. Исчезновения или нарушения информации вследствие несанкционированного доступа в систему, воздействия вредоносного программного обеспечения, программных ошибок, ошибок персонала и аппаратных сбоев.

6.1.2. Восстановление системного программного обеспечения и прикладного программного обеспечения общего назначения производиться с их носителей в соответствии с инструкциями производителя.

6.1.3. Восстановление специализированного программного обеспечения производиться с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.1.4. Восстановление открытой информации и информации ограниченного доступа производится с резервных носителей. При этом необходимо использовать последнюю копию информации.

6.1.5. При частичном нарушении или исчезновении записей баз данных восстановление производиться с последней не нарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по идентификации, аутентификации

1. Общие положения

1.1. Настоящая инструкция определяет в РЦОИ порядок идентификации, аутентификации пользователей информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн), являющихся сотрудниками РЦОИ, порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации внешних пользователей ИСПДн, порядок идентификации/аутентификации устройств, а также обязанности пользователей ИСПДн и администратора информационной безопасности.

2. Порядок идентификации и аутентификации работников

2.1. Всем пользователям ИСПДн, являющимся работниками РЦОИ, допущенным в установленном порядке к работе в ИСПДн, присваиваются учетные записи в виде персональных идентификаторов (логины, имена пользователей). Идентификаторы определяют доступ к техническим средствам и информационным ресурсам ИСПДн и системам защиты информации.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором информационной безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в ИСПДн и пароли, обеспечивающие аутентификацию (проверку подлинности). Права пользователя по доступу к информационным ресурсам ИСПДн, определяется должностью пользователя и матрицей доступа.

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

2.4. При приеме (увольнении) на работу сотрудника РЦОИ или изменении полномочий (временное или бессрочное) действующего сотрудника, изменения в его доступе к информационным ресурсам ИСПДн и генерацию (уничтожение) идентификаторов и паролей, производит администратор информационной безопасности.

2.5. Первичные пароли генерируются администратором информационной безопасности в момент создания идентификаторов и выдаются пользователю под роспись в Журнале учета выдачи первичных паролей (Приложение 1 к настоящей Инструкции).

2.6. При первом доступе к ИСПДн пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в Инструкции по организации парольной защиты.

2.7. В случаях, предусмотренных нормативными документами по защите информации, обрабатываемой в ИСПДн РЦОИ, либо по решению руководителя при особой ценности для РЦОИ сведений, к которым необходимо обеспечить безопасный доступ, помимо паролей используются дополнительные атрибуты доступа – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надежную многофакторную аутентификацию.

2.8. Администратор информационной безопасности осуществляет настройку в ИСПДн параметров количества вводов неправильного пароля. Количество вводов неправильного пароля устанавливается равным 14. Разблокирование пароля осуществляет администратор информационной безопасности при обращении к нему пользователя с заблокированным паролем.

2.9. Администратор информационной безопасности организует настройку в ИСПДн параметров блокирования сеанса доступа при времени бездействия пользователя более 1 часа или по запросу пользователя.

3. Управление аппаратными средствами аутентификации

3.1. При использовании аппаратных средств аутентификации пользователей (смарт-карты, электронные ключи) выдачу, инициализацию, блокирование и утилизацию аппаратных средств аутентификации организует администратор информационной безопасности.

3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор информационной безопасности в Журнале учета аппаратных средств аутентификации (Приложение 2 к настоящей Инструкции).

4. Обязанности пользователя

4.1. Пользователь ИСПДн РЦОИ является частью системы защиты информации и обязан соблюдать следующие правила информационной безопасности:

4.1.1. Помнить свой идентификатор и пароль для входа в ИСПДн.

4.1.2. Обеспечивать сохранность полученных аппаратных идентификаторов. Не предоставлять доступ к личному аппаратному идентификатору никому, кроме администратора информационной безопасности.

4.1.3. Держать свои пароли в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников РЦОИ, в т.ч. руководителей) личные пароли.

4.1.4. Осуществлять ввод паролей только в условиях, исключающих их просмотр.

4.1.5. Не хранить записки-памятки с личными паролями на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.

4.1.6. Своевременно сообщать администратору информационной безопасности о фактах компрометации паролей (когда пароли стали или может быть станут известны еще кому-либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора информационной безопасности.

5. Обязанности администратора информационной безопасности

5.1. Администратор информационной безопасности осуществляет организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИСПДн РЦОИ, контроль действий пользователей при их работе с персональными идентификаторами и паролями доступа.

5.2. Администратор информационной безопасности обязан:

5.2.1. создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИСПДн;

5.2.2. обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 180 дней с момента очередной смены;

5.2.3. свой собственный пароль администратор информационной безопасности должен изменять не реже одного раза в месяц;

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

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

5.3. Действия администратора информационной безопасности при компрометации паролей и утрате аппаратных идентификаторов.

5.3.1. заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора.

5.3.2. выявить действия, произведенные в ИСПДн с использованием скомпрометированных персональных идентификаторов и паролей доступа.

5.3.3. создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИСПДн.

6. Заключительные положения

6.1. Пользователи ИСПДн РЦОИ должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

6.2. Пользователи должны быть ознакомлены с настоящей Инструкцией до начала работы в ИСПДн под роспись. Обязанность ознакомления пользователей с настоящей инструкцией лежит на администраторе информационной безопасности.

6.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

ЖУРНАЛ
учета выдачи первичных паролей

Уч. № _____
20____ год.

1	2	3	4	5	6	7	8	9
№ пп.	ФИО работника	Должность	Подразделение	Тип доступа	ИСПДн РЦОИ	Первичный пароль	Дата выдачи/блокирования	Подпись
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Лист _____

ПРАВИЛА

по формированию и ведению журнала выдачи первичных паролей

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – ФИО сотрудника.
      2.2.3. Графа 3 – занимаемая должность.
      2.2.4. Графа 4 – подразделение.
      2.2.5. Графа 5 – тип доступа (пользователь или администратор) (например – пользователь (чтение)).
      2.2.6. Графа 6 – название ИСПДн РЦОИ (при наличии нескольких ИСПДн РЦОИ).
      2.2.7. Графа 7 – пароль, назначаемый администратором информационной безопасности.
      2.2.8. Графа 8 – дата выдачи или блокирования пароля.
      2.2.9. Графа 9 – подпись сотрудника (при выдаче) или администратора информационной безопасности (при блокировании).
   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 2

ЖУРНАЛ
учета аппаратных средств аутентификации

Уч. № _____
20____ год.

1	2	3	4	5	6	7
Наименование	ИНВ.№	ИСПДн РЦОИ	Дата периодического осмотра и подпись	Дата выдачи в индивидуальное пользование	Ф.И.О. Подпись индивидуального пользователя	Примечание
ESMART Token USB 64K Metal	*инв. № 000011*	*«АИС РЦОИ РИС МО»*	*1.01.2017 АБ _____ Сидоров С.С.*	*12.06.2017*	*_____ Иванов И.И.*	*Пример заполнения*

Лист _____

ПРАВИЛА

по формированию и ведению журнала учета аппаратных средств аутентификации.

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – наименование устройства (например - ESMART Token USB 64K Metal).
      2.2.2. Графа 2 – инвентарный или серийный номер устройства (например – инв. № 000011.).
      2.2.3. Графа 3 – название ИСПДн РЦОИ.
      2.2.4. Графа 4 – дата последнего осмотра и подпись администратора информационной безопасности (например – 1.01.2017 АБ _____ Сидоров С.С.).
      2.2.5. Графа 5 – дата передачи пользователю (например – 12.06.2017).
      2.2.6. Графа 6 – подпись пользователя (например – _____ Иванов И.И.).
      2.2.7. Графа 7 – любая информация, относящаяся к записанному устройству.
   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.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по управлению доступом к информации

1. Общие положения

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, в том числе персональных данных, содержащейся в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ.

1.2. Настоящая инструкция определяет порядок действий ответственного за обеспечение безопасности персональных данных в ИСПДн (далее – администратора информационной безопасности) и пользователей ИСПДн при разграничении доступа к ресурсам и информации ИСПДн РЦОИ.

2. Матрица доступа

2.1. Разграничение доступа к ресурсам и информации ИСПДн осуществляет и контролирует администратор информационной безопасности путем настройки программно–технических средств и средств защиты информации (далее – СЗИ) ИСПДн на основании матрицы доступа и Журнала учета выдачи паролей.

2.2. В РЦОИ разработана и утверждена матрица доступа к ресурсам ИСПДн РЦОИ.

2.3. Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает администратор информационных систем персональных данных.

2.4. Контроль и актуализацию доступа пользователей к ресурсам и информации ИСПДн, а также соответствующие настройки программно–технических средств, соответствующих СЗИ осуществляет администратор информационной безопасности периодически, один раз в месяц или на основании приказов ректора АСОУ.

3. Доступ до идентификации и аутентификации

3.1. Вход и действия с ресурсами ИСПДн до процедур идентификации и аутентификации разрешен только администратору информационной безопасности для восстановления после сбоев и аварий технических средств.

3.2. Доступ к ресурсам ИСПДн до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4. Удаленный доступ

4.1. Указанные в п.4 требования следует соблюдать только в случае, если РЦОИ использует или планирует использовать удаленный доступ (через сеть Интернет) к ресурсам ИСПДн РЦОИ.

4.2. Удаленный доступ пользователей к информационным ресурсам ИСПДн возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью АСОУ и внесенных в Журнал учета разрешенных средств удаленного доступа (Приложение 1 к настоящей Инструкции).

4.3. Выдачу, учет, хранение, настройку программного обеспечения, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор информационной безопасности. Все данные по конфигурации и настройкам должны быть записаны в Журнал учета разрешенных средств удаленного доступа.

4.4. При настройке средств удаленного доступа к ресурсам ИСПДн администратор информационной безопасности осуществляет возможность удаленного доступа с автоматической аутентификацией средств удаленного доступа.

4.5. Периодически, не реже одного раза в месяц администратор информационной безопасности контролирует состояние средств удаленного доступа к ресурсам ИСПДн и их использование. При обнаружении нарушений в исходной конфигурации и при обнаружении попыток доступа, не включенных в разрешенные для пользователя, устройство и пользователь блокируются администратором информационной безопасности.

5. Мобильные технические средства

5.1. Указанные в п.5 требования следует соблюдать только в случае, если РЦОИ использует или планирует использовать мобильные технические средства для доступа к ресурсам ИСПДн РЦОИ.

5.2. К мобильным техническим средствам РЦОИ отнесены все переносные технические устройства, на которые может быть записана и с которых может быть считана информация, содержащаяся в ИСПДн.

5.3. Все мобильные технические средства РЦОИ должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор информационной безопасности в Журнале учета разрешенных мобильных технических средств (Приложение 2 к настоящей Инструкции).

5.4. Контроль исправности и назначения использования мобильных технических средств для доступа к ресурсам ИСПДн производит администратор информационной безопасности. В случае обнаружения неисправности или использования не по назначению, мобильное устройство изымается у пользователя и администратором информационной безопасности предпринимаются действия по устранению инцидента.

5.5. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор информационной безопасности полностью очищает их от информации, имеющей отношение к ИСПДн РЦОИ.

6. Заключительные положения

6.1. Все пользователи ИСПДн должны быть предупреждены об ответственности за действия с получением доступа к ресурсам ИСПДн РЦОИ, нарушающие требования настоящей Инструкции.

6.2. Пользователи должны быть ознакомлены с настоящей Инструкцией до начала работы в ИСПДн РЦОИ под роспись. Обязанность ознакомления пользователей информационной системы с настоящей инструкцией лежит на администраторе информационной безопасности.

6.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

ЖУРНАЛ
учета разрешенных средств удаленного доступа

Уч. № _____
2_____ год.

1	2	3	4	5	6	7
№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ подпись	Дата возврата/ подпись
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*Иванов И.И.*	*1.01.2017_____ (Иванов И.И.)*	*12.06.2017 АБ Сидоров С.С._____*

Лист ___

ПРАВИЛА

по формированию и ведению журнала учета разрешенных средств удаленного доступа

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – наименование оборудования или программного средства (например – ноутбук Lenovo B590.).
      2.2.3. Графа 3 – инвентарный или серийный номер (например – инв. № 1000013).
      2.2.4. Графа 4 – указывается состояние оборудования или ПО на момент записи (исправно, неисправно, в ремонте, для ПО актуально или требуется обновление) (например – исправен).
      2.2.5. Графа 5 – пользователь оборудования или ПО (например – Иванов И.И.).
      2.2.6. Графа 6 – дата выдачи и подпись пользователя (например – 1.01.2017_____ Иванов И.И.).
      2.2.7. Графа 7 – дата возврата оборудования и подпись администратора информационной безопасности (например – 12.06.2017 АБ Сидоров С.С._____).
   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 несколько строк.

Приложение 2

ЖУРНАЛ
учета разрешенных мобильных технических средств

учетный № _____
2_____ год.

1	2	3	4	5	6	7
№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ подпись	Дата возврата/ подпись
1	*ноутбук Lenovo B590*	*инв. № 1000013*	*исправен*	*Иванов И.И.*	*1.01.2017_____ (Иванов И.И.)*	*12.06.2017 АБ Сидоров С.С._____*

Лист _____

ПРАВИЛА

по формированию и ведению журнала учета разрешенных мобильных технических средств

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – наименование оборудования (например – ноутбук Lenovo B590.).
      2.2.3. Графа 3 – инвентарный или серийный номер (например – инв. № 1000013).
      2.2.4. Графа 4 – указывается состояние оборудования на момент записи (исправно, неисправно, в ремонте) (например – исправен).
      2.2.5. Графа 5 – пользователь оборудования (например – Иванов И.И.).
      2.2.6. Графа 6 – дата выдачи и подпись пользователя (например – 1.01.2017_____ Иванов И.И.).
      2.2.7. Графа 7 – дата возврата оборудования и подпись администратора безопасности (например – 12.06.2017 АБ Сидоров С.С._____).
   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 несколько строк.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по защите машинных носителей информации

1. Общие положения

1.1. Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в РЦОИ.

1.2. Машинный носитель информации (далее – МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных) в электронном виде. МНИ делятся на съемные и несъемные носители:

1.2.1. Несъемные МНИ являются частью автоматизированного рабочего места (далее – АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.

1.2.2. К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

2. Учет машинных носителей информации

2.1. Все используемые в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ МНИ подлежат учёту.

2.2. Учет, хранение и выдачу носителей информации осуществляет администратор информационной безопасности. При увольнении администратора информационной безопасности составляется акт приема-сдачи учетных документов и носителей.

2.3. Учет всех видов и типов носителей информации производится в Журнале учета машинных носителей информации (Приложение 1 к настоящей Инструкции).

2.4. На несъемную часть носителей ИСПДн РЦОИ наносится уникальный в пределах РЦОИ учетный номер.

3. Выдача машинных носителей информации

3.1. Пользователи ИСПДн получают учтенный МНИ от администратора информационной безопасности, для выполнения работ на конкретный срок.

3.2. При получении пользователем носителя информации делается соответствующая запись в Журнале учета машинных носителей информации.

3.3. По окончании работ или установленного срока использования пользователь сдает носитель информации администратору информационной безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации.

4. Использование машинных носителей информации

4.1. На МНИ записываются исключительно информация и программные средства обработки информации, содержащейся в ИСПДн РЦОИ.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор информационной безопасности.

4.3. Вынос учтенных носителей информации за пределы установленных мест обработки информации допустим только с письменного разрешения администратора информационной безопасности. Несанкционированный вынос за границу контролируемой зоны учтенных МНИ запрещен.

4.4. Передача носителей, содержащих информацию, которая обрабатывается в ИСПДн РЦОИ сторонним организациям или третьим лицам производится по письменному поручению руководителя РЦОИ через администратора информационной безопасности. Администратор информационной безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации.

5. Хранение машинных носителей информации

5.1. Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

5.2. МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

5.3. Запрещается хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

6. Действия при утрате и порче машинных носителей информации

6.1. В случае утраты или порчи пользователем МНИ, содержащих обрабатываемую в ИСПДн РЦОИ информацию, немедленно ставится в известность администратор информационной безопасности. Администратор информационной безопасности вносит соответствующую запись в Журнал учета машинных носителей информации.

6.2. По факту утраты или порчи МНИ администратор информационной безопасности проводит служебное расследование в установленном порядке.

6.3. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

7. Уничтожение машинных носителей информации

7.1. Уничтожение МНИ организует администратор информационной безопасности с составлением Акта уничтожения машинных носителей информации (Приложение 2 к настоящей Инструкции).

7.2. Уничтожение 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 информационной безопасности в зависимости от типа носителя и возможностей РЦОИ.

8. Ограничения и ответственность

8.1. Всем пользователям ИСПДн РЦОИ запрещено использовать учтенные МНИ в личных целях.

8.2. Пользователям запрещено передавать носители информации кому-либо.

8.3. Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИСПДн РЦОИ и неучтенными носителями информации запрещено.

8.4. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации в ИСПДн назначается служебное расследование. По результату расследования и по представлению администратора информационной безопасности, ректор АСОУ принимает решение о привлечении пользователя к ответственности согласно локальным нормативным актам АСОУ и в соответствии с действующим законодательством Российской Федерации в области защиты информации.

8.5. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

9. Заключительные положения

9.1. Пользователи ИСПДн РЦОИ должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с настоящей Инструкцией до начала работы в ИСПДн.

9.2. Обязанность ознакомления пользователей с настоящей Инструкцией лежит на администраторе информационной безопасности.

Приложение 1

ЖУРНАЛ
учета машинных носителей информации

Уч. № _____
20_____ г.

1	2	3	4	5	6	7	8
Учетный / заводской номер	Наименование (марка) носителя	Вид носителя (съемный /несъемный)	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения съемного носителя и подпись	Дата возврата съемного носителя и подпись администратора	Отметка об уничтожении носителя
инв. № 1000013	*USB flash drive Transcend JF V30/2Gb*	*съемный*	*нет*	*Иванов И.И.*	*01.01.2017_____(Иванов И.И.)*	*12.06.2017 _____(Сидоров И.И.)*	*уничтожен 20.06.2017*

Лист _____

ПРАВИЛА

по формированию и ведению журнала учета машинных носителей персональных данных

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – учетный или заводской номер носителя (например – инв. № 1000013) .
      2.2.2. Графа 2 – наименование носителя (например – USB flash drive Transcend JF V30/2Gb.).
      2.2.3. Графа 3 – указывается съемный или несъемный носитель (например – съемный).
      2.2.4. Графа 4 – для несъемных носителей указывается АРМ пользователя.
      2.2.5. Графа 5 – ФИО пользователя (например – Иванов И.И.).
      2.2.6. Графа 6 – дата получения носителя и подпись пользователя безопасности (например – 01.01.2017_____(Иванов И.И.)).
      2.2.7. Графа 7 – дата возврата носителя и подпись администратора безопасности (например – 12.06.2017 _____(Сидоров И.И.))
      2.2.8. Графа 8 – отметку делает администратор безопасности после уничтожения носителя (например – уничтожен 20.06.2017).
   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 несколько строк.

Приложение 2

АКТ № _____
уничтожения машинных носителей информации

Проведен отбор машинных носителей информации и установлено, что информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях информация уничтожена путем:
_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители уничтожены путем:
_____.
(механического уничтожения, сжигания и т.п.)

Администратор информационной безопасности:

_____ _____

(ФИО) (подпись)

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по управлению событиями информационной безопасности

1. Общие положения

1.1. Настоящая инструкция определяет для информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн) РЦОИ:

1.1.1. перечень событий информационной безопасности (далее – событий ИБ), подлежащих регистрации и сроки их хранения;

1.1.2. состав и содержание информации о событиях безопасности, подлежащих регистрации;

1.1.3. порядок сбора, записи и хранения информации о событиях безопасности в течение определенного времени хранения;

1.1.4. порядок защиты информации о событиях безопасности.

2. Регистрация событий информационной безопасности

2.1. В регистрируемые события ИБ должны быть включены события ИБ, имеющие отношение к возможности реализации угроз безопасности информации, обрабатываемой в ИСПДн, описанных в модели угроз безопасности информации для ИСПДн РЦОИ.

2.2. К регистрируемым событиям ИБ относятся события безопасности, регистрируемые в журналах операционных систем технических средств ИСПДн РЦОИ и средств защиты информации (далее – СЗИ), а также организационно-технические события ИБ в инфраструктуре ИСПДн.

2.3. Автоматически определяемые события ИБ регистрируются автоматически в электронных журналах сообщений программных средств ИСПДн и СЗИ.

2.4. События ИБ, не определяемые автоматически регистрируются в Журнале событий (инцидентов) информационной безопасности по форме Приложения 1 к настоящей Инструкции.

2.5. Перечень событий безопасности, не определяемых автоматически и которые необходимо регистрировать при их возникновении, приведен в перечне регистрируемых событий (инцидентов) ИБ (Приложение 2).

3. Порядок сбора, записи и хранения событий информационной безопасности

3.1. Настройку журналов регистрации событий ИБ в программном обеспечении ИСПДн и СЗИ осуществляет администратор ИСПДн РЦОИ на основании предоставленных полномочий и администратор информационной

безопасности, каждый в своей части. Настройка осуществляется в соответствии с эксплуатационной документацией на программно–технические средства ИСПДн.

3.2. Администратор ИСПДн и администратор информационной безопасности должны с периодичностью не реже 1 раза в неделю просматривать журналы регистрации событий безопасности ИСПДн РЦОИ.

3.3. Настройки журналов регистрации событий ИБ должны обеспечивать запись в память технических средств ИСПДн и СЗИ информации о поступающих событиях безопасности без переполнения памяти в течение 1 месяца с момента регистрации события.

3.4. Информация о событиях безопасности в ИСПДн, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором информационной безопасности при ее обнаружении в Журнале событий (инцидентов) информационной безопасности.

4. Защита информации о событиях информационной безопасности

4.1. Права доступа к файлам отчетов электронных журналов безопасности и настройкам журналов установлены администратору информационной безопасности и администратору ИСПДн.

4.2. Доступ к электронным журналам безопасности должен быть блокирован при пользовательском уровне доступа к ИСПДн.

4.3. Ответственность за сохранность Журнала событий (инцидентов) информационной безопасности по форме Приложения 1 и за конфиденциальность вносимой в него информации несет администратор информационной безопасности.

5. Заключительные положения

5.1. Администратор информационной безопасности и администратор ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей Инструкции.

5.2. Администратор информационной безопасности и администратор ИСПДн должны быть ознакомлены с настоящей Инструкцией до начала работы с ИСПДн РЦОИ под подпись.

5.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

ЖУРНАЛ
событий (инцидентов) информационной безопасности

учетный № _____
2_____ год.

1	2	3	4	5	6
№	Код события/инцидента (в соответствии с перечнем регистрируемых событий ИБ)	Место события/инцидента	Участники события/инцидента	Дата	Подпись администратора безопасности
1	*006*	*АРМ №3*	*Иванов И.И. Сидоров С.С.*	*обнаружено 01.01.2017*	*_____ (Сидоров С.С.)*

Лист _____

ПРАВИЛА

по формированию и ведению журнала событий (инцидентов) информационной безопасности

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
   1.2. Обложка журнала изготавливается на отдельном листе.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – порядковый номер записи.
      2.2.2. Графа 2 – код события/инцидента из перечня регистрируемых событий (например – пароль пользователя не соответствует требованиям – записать код 006).
      2.2.3. Графа 3 – указывается название рабочего места пользователя (например – АРМ №3).
      2.2.4. Графа 4 – указываются участники события/инцидента (например – для кода 006 это – пользователь Иванов И.И. и администратор безопасности Сидоров С.С.).
      2.2.5. Графа 5 – дата события/инцидента (например – обнаружено 01.01.2017).
      2.2.6. Графа 6 – подпись администратора информационной безопасности (например – _____(Сидоров С.С.))
   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 несколько строк.

Приложение 2

ПЕРЕЧЕНЬ
регистрируемых событий (инцидентов) информационной безопасности ИСПДн РЦОИ

№ 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 3-х кратного 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 обрабатываемой информацией
		014	Несанкционированный вынос МНИ из зоны обработки 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 ИСПДн РЦОИ 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 сотрудник, помещение не заперто.
		030	В помещении контролируемой зоны без сопровождения присутствует сотрудник, не имеющий допуска к обработке 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	
6	ПО	046	Несанкционированная АБ установка (обновление) ПО
		047	ПО на дистрибутивных носителях не имеет лицензии.
		048	Хранение дистрибутивных носителей с устаревшим ПО
		049	Нет сведений о совместимости обновлений ПО с установленными СВТ
		050	

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по организации антивирусной защиты

1. Общие положения

1.1. Настоящая инструкция определяет порядок организации антивирусной защиты и порядок действий администратора информационной безопасности, и пользователей информационных систем персональных данных и государственных информационных систем (далее вместе – ИСПДн) РЦОИ при обнаружении вредоносного программного обеспечения.

1.2. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн.

1.3. Настоящая инструкция разработана в соответствии с:

- Приказом ФСТЭК России от 11.02.2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- Приказом ФСТЭК России от 15.02.2017 года № 27 "О внесении изменений в Требования о защите информации, на составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 года № 17»;
- Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Порядок организации антивирусной защиты

2.1. Программное обеспечение антивирусной защиты (далее – антивирусное ПО) устанавливают на все средства вычислительной техники, входящие в состав ИСПДн РЦОИ. Антивирусное ПО обеспечивает защиту от внедрения вредоносного программного обеспечения со съемных носителей, через электронные отправления, из информационно-вычислительной сети, из сетей связи общего пользования и международного информационного обмена (Интернет).

2.2. Антивирусная защита ИСПДн строится как единая система, которая обеспечивает:

2.2.1. управление конфигурацией и логической структурой всего программного обеспечения системы антивирусной защиты;

2.2.2. управление установкой и обновлением лицензионных ключей средств антивирусной защиты;

2.2.3. управление рассылкой и установкой обновлений баз средств антивирусной защиты;

2.2.4. ограничение доступа пользователей на рабочих местах к настройкам установленных средств антивирусной защиты;

2.2.5. настройку рассылки сообщений об обнаружении вирусов, о сбоях в работе средств антивирусной защиты и т.п.;

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

2.3. На все применяемые в ИСПДн средства антивирусной защиты должны быть документы, подтверждающие права АСОУ на их использование и действующие сертификаты ФСТЭК России.

2.4. При осуществлении антивирусной защиты ИСПДн выполняются следующие обязательные мероприятия:

2.4.1. контроль съемных носителей информации на предмет наличия на них вредоносного программного обеспечения до начала работы с ними;

2.4.2. проверка всех электронных отправлений на предмет наличия вредоносного программного обеспечения;

2.4.3. периодическая проверка на предмет наличия вредоносного программного обеспечения жестких магнитных дисков (не реже одного раза в неделю);

2.4.4. внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие вредоносного программного обеспечения;

2.4.5. восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

2.5. Обновления баз данных средств антивирусной защиты в ИСПДн РЦОИ осуществляется в автоматическом режиме (не реже одного раза в сутки).

2.6. При загрузке автоматизированного рабочего места в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

2.7. Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

2.8. Установку и настройку антивирусного ПО осуществляет администратор информационной безопасности в соответствии с эксплуатационной документацией на данное ПО.

3. Порядок действий при обнаружении вредоносного ПО

3.1. При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

3.2. При обнаружении вредоносного программного обеспечения на съемных носителях, в электронных отправлениях пользователь обязан:

3.2.1. приостановить работу с источником угрозы (съемным носителем, электронным отправлением), иные работы на автоматизированном рабочем месте не запрещаются;

3.2.2. сообщить администратору информационной безопасности (или администратору ИСПДн) об обнаружении вредоносного программного обеспечения;

3.2.3. принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором информационной безопасности (администратором ИСПДн).

3.3. При обнаружении вредоносного программного обеспечения в процессе обработки информации, за исключением п. 3.1, пользователь обязан:

3.3.1. приостановить все работы на автоматизированном рабочем месте;

3.3.2. сообщить администратору информационной безопасности (или администратору ИСПДн) об обнаружении вредоносного программного обеспечения;

3.3.3. принять меры по локализации и удалению вредоносного программного обеспечения, рекомендованные администратором информационной безопасности (администратором ИСПДн).

3.4. Администратор информационной безопасности (администратор ИСПДн) по факту событий по п.3.1 и п.3.2 должен зарегистрировать вирусную атаку в журнале событий безопасности в соответствии с Инструкцией по управлению событиями информационной безопасности.

3.5. При обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании, администратор информационной безопасности (администратор ИСПДн) обязан принять меры по локализации и удалению вредоносного программного обеспечения, а также по выявлению источника и способа проникновения вредоносного программного обеспечения.

3.6. В случае невозможности удаления вредоносного программного обеспечения, администратору информационной безопасности (администратору ИСПДн) 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 в ИСПДн РЦОИ информации.

4. Заключительные положения

4.1. Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей инструкции.

4.2. Пользователи должны быть ознакомлены с настоящей Инструкцией до начала работы с ИСПДн РЦОИ под подпись. Обязанность ознакомления

сотрудников с настоящей инструкцией лежит на администраторе информационной безопасности (администраторе ИСПДн).

4.3. Работники РЦОИ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ, а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно администратором информационной безопасности:

– Длина пароля должна быть не менее 8 символов;

– В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, даты рождения, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

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

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

– При смене пароля новое значение должно отличаться от предыдущих;

– Не использовать ранее использованные пароли;

– Пользователь не имеет права сообщать личный пароль другим лицам.

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 6 месяцев.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности.

В случае компрометации (утеря, передача другому лицу) личного пароля, пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по управлению программным обеспечением

1. Общие положения

1.1. Настоящая инструкция определяет порядок действий администратора информационной безопасности при установке и обновлении программного обеспечения (далее – ПО) в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ, в том числе ПО средств защиты информации (далее – СЗИ).

2. Порядок установки и обновления

2.1. Установку (обновление) ПО в ИСПДн, в том числе ПО СЗИ осуществляет администратор информационной безопасности, имеющий необходимые полномочия в соответствии с матрицей доступа.

2.2. Установка ПО производится с рабочих копий оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных законным порядком. Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию и руководство пользователя.

2.3. Устанавливаемое в ИСПДн ПО должно быть предварительно проверено (протестировано) администратором информационной безопасности на работоспособность, отсутствие опасных функций, а также на совместимость с установленными в ИСПДн программными и техническими средствами, в том числе ПО СЗИ.

2.4. После установки (обновления) программного обеспечения в ИСПДн администратор информационной безопасности и администратор информационных систем персональных данных, каждый в своей части, выполняют необходимые настройки, выполняют тестирование работоспособности и вносят необходимые изменения в эксплуатационную документацию на ИСПДн и систему защиты информации.

2.5. Администратор информационной безопасности и администратор информационных систем персональных данных, каждый в своей части, проводят оценку изменений в ПО на условия отклонения технологического процесса обработки информации в ИСПДн от ранее принятого. На основании полученной информации администратор информационных систем персональных данных принимает решение о действиях, связанных с изменением конфигурации ГИС.

2.6. После обновления ПО администратор информационной безопасности заменяет носители с дистрибутивом неактуального программного обеспечения на носители с дистрибутивом обновленного ПО.

3. Заключительные положения

3.1. Администратор информационной безопасности и администратор информационных систем персональных данных должны быть предупреждены об ответственности за действия с ПО, нарушающие требования настоящей Инструкции.

3.2. Администратор информационной безопасности и администратор информационных систем персональных данных должны быть ознакомлены с настоящей Инструкцией до начала работы в ИСПДн под подпись.

3.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по управлению конфигурацией в ИСПДн

1. Общие положения

1.1. Настоящая инструкция предназначена для управления конфигурацией в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ, в том числе конфигурацией их системы защиты информации.

1.2. Изменением базовой конфигурации является:

1.2.1. изменение места расположения оборудования, входящего в ИСПДн, обрабатывающие защищаемую информацию, не содержащую сведения, составляющие государственную тайну, а также в систему защиты информации;

1.2.2. установка и ввод в эксплуатацию нового оборудования ИСПДн, системы защиты информации.

1.3. Настоящая инструкция определяет порядок действий администратора информационных систем персональных данных.

2. Порядок управления конфигурацией

2.1. Базовая конфигурация ИСПДн и системы защиты отражена в проектной, эксплуатационной и организационно-распорядительной документации на систему защиты информации.

2.2. Администратор информационных систем персональных данных не реже, чем один раз в год после очередной проверки организует проверку текущей конфигурации ИСПДн и ее системы защиты на соответствие базовой конфигурации. Результат проверки оформляется Актом контроля текущей конфигурации по форме Приложения 1 к настоящей Инструкции.

2.3. При обнаружении отклонений текущей конфигурации от базовой администратор информационных систем персональных данных организует и контролирует восстановление базовой конфигурации ИСПДн и ее системы защиты информации. Срок восстановления и мероприятия по восстановлению определяет администратор информационных систем персональных данных.

2.4. Администратору информационных систем персональных данных разрешены решения, направленные на внесение изменений в базовую конфигурацию ИСПДн и (или) систему ее защиты в случае такой необходимости.

2.5. Необходимость внесения изменений в базовую конфигурацию ИСПДн и (или) ее систему защиты определяет администратор информационных систем персональных данных:

2.5.1. по результату контроля защищенности информации;

2.5.2. по техническому состоянию технических средств ИСПДн и средств защиты информации;

2.5.3. по актуальности используемых технических средств ИСПДн и средств защиты информации;

2.5.4. по изменениям в технологических процессах обработки информации;

2.5.5. по иным причинам.

2.6. При принятии решения о необходимости внесения изменений в базовую конфигурацию ИСПДн и (или) ее системы защиты администратор информационных систем персональных данных проводит анализ новых структурно – функциональных характеристик ИСПДн и системы ее защиты при внесении изменений в базовую конфигурацию.

2.7. На основании:

2.7.1. анализа результатов изменений в конфигурации;

2.7.2. анализа действующей модели угроз информационной безопасности;

администратор информационных систем персональных данных) принимает решения:

– либо о внесении изменений в конфигурацию без повторной аттестации ИСПДн и (или) системы ее защиты (при сохранении структурно – функциональных характеристик и состава модели угроз);

– либо об утверждении мероприятий ректором АСОУ по изменению конфигурации ИСПДн и ее системы защиты (при изменении структурно – функциональных характеристик и (или) изменении состава модели угроз с необходимостью повторной аттестации ИСПДн и (или) ее системы защиты на требования безопасности информации).

2.8 При принятии решения о внесении изменений в базовую конфигурацию ИСПДн и (или) системы ее защиты изменения в конфигурацию администратор информационных систем персональных данных вносит и контролирует результаты изменений.

2.9 Данные о новой конфигурации ИСПДн и (или) ее системы защиты администратор информационных систем персональных данных вносит в соответствующую эксплуатационную документацию с указанием даты внесения изменений.

2.10 Решение о проведении повторной аттестации, либо об отказе от повторной аттестации принимает ректор АСОУ по представлению администратора информационных систем персональных данных.

3. Заключительные положения

3.1. Администратор информационных систем персональных данных, пользователи ИСПДн должны быть предупреждены об ответственности за действия, нарушающие требования настоящей Инструкции.

3.2. Администратор информационных систем персональных данных, пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы в ИСПДн, под подпись.

3.3. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1

АКТ № _____
контроля текущей конфигурации в ИСПДн_____ и ее средств защиты информации

1. Отклонения в составе ИСПДн:

_____

_____

2. Отклонения в составе системы защиты информации:

_____

_____

3. Отклонения в подключениях технических средств ИСПДн и системы защиты информации:

_____

_____

4. Отклонения в составе программного обеспечения:

_____

_____

5. Отклонения в технологии обработки информации:

_____

_____

6. Выводы:

_____

_____

Администратор информационных систем персональных данных:

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

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по контролю защищенности информации

1. Общие положения

1.1. Настоящая инструкция определяет порядок выявления, анализа и устранения уязвимостей, недостатков программного обеспечения, аппаратных средств, организационно-технических недостатков и порядок действий администратора информационной безопасности при контроле защищенности информации, обрабатываемой в информационных системах персональных данных и государственных информационных системах (далее вместе – ИСПДн) РЦОИ.

2. Выявление, анализ и устранение уязвимостей

2.1. Уязвимость – это недостаток ИСПДн или системы защиты информации, который может привести к реализации угрозы безопасности информации.

2.2. Периодичность плановых процедур выявления, анализа и устранения уязвимостей составляет один год. Внеплановые процедуры выявления, анализа и устранения уязвимостей проводят в случае необходимости. Необходимость внеплановой процедуры выявления и устранения уязвимостей определяет администратор информационной безопасности на основе анализа журналов событий информационной безопасности.

2.3. В ИСПДн РЦОИ должно осуществляться выявление и устранение следующих типов уязвимостей:

2.3.1. недостатки и (или) ошибки программного обеспечения ИСПДн и ее системы защиты информации;

2.3.2. недостатки аппаратных средств ИСПДн, в том числе аппаратных средств защиты информации;

2.3.3. организационно-технические недостатки.

2.4. Мероприятия по выявлению, анализу и устранению уязвимостей выполняет администратор информационной безопасности.

3. Мероприятия по выявлению, анализу и устранению недостатков программного обеспечения

3.1. Проверка конфигурации и настроек программно–технических средств ИСПДн и ее системы защиты информации на соответствие требованиям эксплуатационной документации и требований к защите информации.

3.2. Проверка наличия и сроков действия лицензий на установленное программное обеспечение.

3.3. Проверка наличия последних обновлений используемого программного обеспечения:

3.3.1. проверка соответствия обновлений версиям программного обеспечения, установленного в ИСПДн и системе защиты информации;

3.3.2. проверка обновлений вирусных баз.

3.4. Анализ сообщений об уязвимостях из специальных источников.

3.5. Устранение обнаруженных недостатков на основании своих полномочий осуществляют администратор информационной безопасности и администратор информационных систем персональных данных, каждый в своей части касающейся.

3.6. При наличии в ИСПДн сканеров безопасности, администратор информационной безопасности осуществляет процесс сканирования и анализ отчетов об обнаруженных уязвимостях.

3.7. Результаты сканирования должны быть отсортированы администратором информационной безопасности по степени критичности (опасности реализации известных угроз безопасности) обнаруженных уязвимостей.

4. Недостатки аппаратных средств

4.1. К недостаткам аппаратных средств, используемых в ИСПДн, относят низкую надежность функционирования (частые аппаратные сбои, отключения), нарушения аппаратной конфигурации, низкое качество контактных соединений.

4.2. При выявлении недостатков аппаратных средств проверяют:

4.2.1. техническое состояние аппаратных средств, журналы планово-профилактического обслуживания аппаратных средств за период контроля защищенности;

4.2.2. наличие сертификатов соответствия на примененные в ИСПДн и ее системе защиты информации аппаратные средства;

4.2.3. наличие у поставщиков обновленных версий аппаратных средств, примененных в ИСПДн и ее системе защиты информации;

4.2.4. перечень событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств;

4.2.5. конфигурацию соединений и установки аппаратных средств, условия их эксплуатации.

4.3. Проверку осуществляет администратор информационной безопасности.

4.4. При обнаружении аппаратных средств с низкой надежностью, частыми выходами из строя администратор информационной безопасности принимает меры по ремонту или замене этих аппаратных средств.

4.5. Координирует работы и устраняет обнаруженные в ходе проверки отклонения от конфигурации администратор информационных систем персональных данных.

5. Мероприятия по выявлению, анализу и устранению организационно – технических недостатков

5.1. Проверка состояния и актуальности организационно-распорядительной документации (далее – ОРД) по защите информации, обрабатываемой в ИСПДн РЦОИ.

5.2. Проверка заполнения рабочих документов ОРД (записи в журналах, перечнях, актах и других формах по требованиям ОРД).

5.3. Проверка соответствия выполнения правил генерации и смены паролей пользователей принятым требованиям.

5.4. Проверка соответствия выполнения правил заведения и удаления учетных записей пользователей принятым требованиям.

5.5. Проверка соответствия выполнения правил разграничения доступа к информации и ресурсам ИСПДн принятым требованиям.

5.6. Проверка соответствия полномочий пользователей принятым требованиям.

5.7. Проверка наличия документов, подтверждающих правомерность изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей.

5.8. Проверка состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемых зонах).

5.9. Проверка знания и соблюдения пользователями ИСПДн основных нормативно-правовых актов в области защиты информации и требований ОРД.

5.10. Проверки организует ответственный за защиту информации ограниченного доступа совместно с администратором информационных систем персональных данных, администратором информационной безопасности и ответственным за организацию обработки персональных данных.

6. Заключительные положения

6.1. Работники РЦОИ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Порядок
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется по форме Приложения 4 к Правилам обработки персональных данных).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

После уничтожения информации, содержащей персональные данные ответственный за организацию обработки персональных данных, подписывает Акт в двух экземплярах.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
ответственного за эксплуатацию средств криптографической защиты информации в информационных системах РЦОИ

1. Общие положения

1.1. Настоящая инструкция определяет основные права и обязанности ответственного за эксплуатацию средств криптографической защиты информации (далее – СКЗИ) в информационных системах РЦОИ (далее – ИС).

1.2. Ответственный за эксплуатацию СКЗИ назначается приказом ректора АСОУ из числа работников РЦОИ.

2. Обязанности ответственного за эксплуатацию СКЗИ

2.1. Вести учет используемых криптосредств, эксплуатационной и технической документации.

2.2. Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации в ИС РЦОИ (пользователи криптосредств).

2.3. Осуществлять контроль за соблюдением условий использования криптосредств, установленных в эксплуатационной и технической документации на СКЗИ.

2.4. Контролировать организацию и обеспечение функционирования криптосредств в пределах своих служебных полномочий.

2.5. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.6. Соблюдать требования к обеспечению безопасности информации в ИС, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.7. Сообщать руководителю РЦОИ о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

2.8. Немедленно уведомлять руководителя РЦОИ о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ и о других фактах, которые могут привести к разглашению информации ограниченного доступа.

2.9. Осуществлять ведение журнала учёта СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, журнала учёта лиц, допущенных к работе с СКЗИ и журнала учёта хранилищ с ключевыми документами по форме Приложения 1 (при наличии).

2.10. Немедленно принимать меры по предупреждению разглашения

защищаемой информации, а также возможной ее утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.11. Проводить уничтожение и контролировать результаты уничтожения СКЗИ при необходимости.

3. Права ответственного за эксплуатацию СКЗИ

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий использования криптосредств, которые могут привести к нарушению безопасности информации или другим нарушениям, приводящим к снижению уровня защищенности ИС РЦОИ.

3.2. Инициировать разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4. Ответственность

4.1. Ответственный за эксплуатацию СКЗИ несет ответственность за действия с СКЗИ, нарушающие требования настоящей инструкции и других организационных и правовых документов, определяющих меры по защите информации, в том числе персональных данных, с помощью криптосредств.

4.2. Ответственный за эксплуатацию криптосредств обязан ознакомиться с требованиями настоящей инструкции под подпись.

Приложение 1

Уч. № _____
20_____ г.

ЖУРНАЛ (форма)
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
1	2	3	4	5	6	7	8
пример	*Инв. Номер 410100000*	*шкаф*	*10.10.2010*	*Йцукен Г.Ш.*	*Каб 206*	*-*	*-*

Лист _____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
пользователя средств криптографической защиты информации

1. Общие положения

1.1. Настоящая инструкция регламентирует обязанности и действия пользователя средств криптографической защиты информации (далее – СКЗИ) при их использовании для защиты информации, обрабатываемой в информационных системах РЦОИ (далее – ИС).

1.2. Настоящая инструкция дополняет комплект организационно – распорядительной документации для ИС РЦОИ, эксплуатируемой в РЦОИ.

2. Обязанности пользователя СКЗИ

2.1. Пользователи криптосредств допускаются к работе с ними по указанию руководителя РЦОИ.

2.2. При наличии двух и более пользователей криптосредств обязанности между ними распределяются с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.3. В ходе своей деятельности пользователи криптосредств обязаны выполнять требования технической, эксплуатационной и организационно-распорядительной документации по защите информации, обрабатываемой в ИС РЦОИ на использование СКЗИ. При выполнении своих обязанностей по криптографической защите информации пользователи криптосредств выполняют все требования и указания ответственного за эксплуатацию криптосредств.

2.4. Пользователи криптосредств обязаны:

2.4.1. не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых носителях к ним и других мерах защиты;

2.4.2. не допускать снятие копий с ключевых носителей;

2.4.3. не допускать вывод ключевых документов на дисплей (монитор) автоматизированного рабочего места (далее – АРМ) или принтер при наличии возможности компрометации выводимой информации

2.4.4. не допускать записи на ключевой носитель посторонней информации;

2.4.5. соблюдать требования к обеспечению безопасности информации, требования к обеспечению безопасности криптосредств и ключевых носителей к ним;

2.4.6. не допускать установки ключевых носителей на другие АРМ;

2.4.7. сдавать ключевые носители к криптосредствам при увольнении или отстранении от исполнения обязанностей;

2.4.8. сообщать ответственному за эксплуатацию криптосредств о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах, ключевых носителях или документации к ним;

2.4.9. немедленно уведомлять ответственного за эксплуатацию криптосредств о фактах утраты или недостачи криптосредств, ключевых носителей к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации (в том числе персональных данных).

3. Заключительные положения

3.1. Все пользователи криптосредств несут ответственность за действия с СКЗИ, нарушающие требования настоящей Инструкции и других организационных и правовых документов, определяющих меры по защите информации, с помощью криптосредств.

3.2. Пользователи криптосредств обязаны ознакомиться с требованиями настоящей Инструкции под подпись.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Правила
по работе с средствами криптографической защиты информации

1. Сокращения

1.1. ИС РЦОИ–информационные системы РЦОИ.

1.2. ОРД – организационно – распорядительная документация по управлению обработкой информации в ИС РЦОИ и управлению системой защиты ИС РЦОИ.

1.3. ПДн – персональные данные.

1.4. СКЗИ – средства криптографической защиты информации.

1.5. СЗИ – средства защиты информации.

1.6. ТС – технические средства.

2. Общие сведения

2.1. Настоящие Правила по работе с СКЗИ в ИС РЦОИ разработаны в соответствии со следующими нормативными правовыми актами и документацией на ИС РЦОИ и их систему защиты информации:

2.1.1. Приказом ФСБ 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 информационной системе 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».

2.1.2. Приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (в ред. Приказа ФСБ РФ от 12.04.2010 № 173).

2.1.3. Федеральным законом от 27.07.2006 № 149 – ФЗ «Об информации, информационных технологиях и защите информации».

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

2.1.5. Приказом ФСТЭК России от 15.02.2017 № 27 «О внесении изменений в Требования о защите информации, на составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17».

2.2. Настоящие Правила предназначены для организации защиты информации в ИС РЦОИ, в том числе ПДн, с помощью СКЗИ.

2.3. Настоящие Правила при использовании в ИС РЦОИ СКЗИ и на основании приказа ФСБ Российской Федерации № 378, часть 1, п. 4 используются в РЦОИ совместно с организационно - распорядительными документами по управлению обработкой и защитой информации в ИС РЦОИ.

2.4. При использовании СКЗИ требования настоящих Правил имеют преимущество перед требованиями организационно – распорядительной документации по управлению обработкой и защитой информации в ИС в отношении аналогичных объектов или процессов защиты.

2.5. Настоящие Правила вступают в силу после их утверждения ректором АСОУ и действуют бессрочно, до момента их замены новыми.

2.6. Для обеспечения функционирования и безопасности СКЗИ ректор АСОУ приказом назначает из числа работников РЦОИ ответственного за эксплуатацию криптосредств.

2.7. Обязанности ответственного за эксплуатацию криптосредств изложены в Инструкции ответственного за эксплуатацию средств криптографической защиты информации в информационных системах РЦОИ.

2.8. Все пользователи СКЗИ участвуют в защите информации, обрабатываемой в ИС РЦОИ, и обязаны знать и выполнять требования:

2.8.1. нормативно – правовых документов по защите информации;

2.8.2. организационно – распорядительных документов по управлению системой защиты информации.

2.8.3. настоящих Правил и перечисленных в них инструкций, в части их касающейся;

2.8.4. Инструкцию пользователя средств криптографической защиты информации.

3. Управление СКЗИ

3.1. Управление СКЗИ осуществляется РЦОИ с целью обеспечения безопасности приема и передачи информации, с использованием криптосредств (Приказ ФСБ Российской Федерации № 378, часть 1, п. 3).

3.2. Настоящие Правила регламентируют порядок управления СКЗИ на стадии эксплуатации СКЗИ в составе системы защиты информации ИС РЦОИ.

3.3. К управлению СКЗИ на этапе эксплуатации отнесены процедуры:

– учет СКЗИ;
– учет пользователей СКЗИ;
– контроль соблюдения условий использования СКЗИ;
– хранение, выдача, замена и уничтожение СКЗИ;
– действия при утере и компрометации СКЗИ;
– защита СКЗИ.

3.4. Учет СКЗИ.

3.4.1. Учет СКЗИ осуществляет ответственный за эксплуатацию криптосредств в журнале учета СКЗИ, эксплуатационной и технической документации к ним.

3.5. Учет пользователей СКЗИ.

3.5.1. Учет пользователей СКЗИ осуществляет ответственный за эксплуатацию криптосредств в журнале учета лиц, допущенных к работе с СКЗИ по форме Приложения 1.

3.6. Контроль соблюдения условий использования СКЗИ.

3.6.1. Условия использования СКЗИ в ИС РЦОИ должны периодически, не реже 1 раза в год, проверяться на соответствие требованиям эксплуатации СКЗИ.

3.6.2. Результаты проверок оформляются Актом результатов проверки условий использования СКЗИ по форме Приложения 2 к настоящим Правилам.

3.6.3. В Акте результатов проверки условий использования СКЗИ должны быть отражены результаты проверки по следующим пунктам:

– состояние и актуальность журнала учета СКЗИ;

– состояние и актуальность учетных листов пользователей СКЗИ;

– соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС РЦОИ и систему защиты информации;

– знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ.

– знание и выполнение пользователями правил защиты СКЗИ.

3.6.4. Если произошла потеря или компрометация СКЗИ, то администратор информационной безопасности совместно с ответственным за эксплуатацию криптосредств назначает внеплановую проверку условий использования СКЗИ.

3.7. Действия при утере и компроментации СКЗИ.

3.7.1. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи ответственный за эксплуатацию криптосредств должен немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

3.7.2. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного за эксплуатацию криптосредств, согласованного с администратором информационной безопасности (администратором информационных систем персональных данных), использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.7.3. При обнаружении недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения ответственный за эксплуатацию криптосредств организует срочные меры к их розыску.

3.7.4. РЦОИ при утере и (или) компрометации СКЗИ проводит мероприятия по устранению причин и последствий инцидента информационной безопасности в

отношении СКЗИ. Порядок действий в этом случае регламентирован в организационно-распорядительной документации.

4. Правила учета СКЗИ

4.1. СКЗИ, используемые для обеспечения безопасности информации при ее обработке в ИС РЦОИ, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

4.2. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале учета СКЗИ по форме Приложения 3. Заполнение, хранение и ведение журнала учета СКЗИ осуществляет ответственный за эксплуатацию криптосредств. В Приложении 4 приведена инструкция по ведению журнала учета СКЗИ.

4.3. Программные криптосредства учитываются в журнале учета СКЗИ совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

4.4. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств ИС РЦОИ, то такие криптосредства учитываются совместно с соответствующими аппаратными средствами, о чем вносится соответствующая запись в журнале учета СКЗИ.

5. Правила хранения СКЗИ

5.1. Пользователи криптосредств должны хранить инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.2. Пользователи криптосредств должны обеспечить раздельное безопасное хранение действующих и резервных ключевых носителей, предназначенных для применения в случае компрометации действующих ключевых документов.

5.3. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. Отключение и уборку криптосредств в опечатываемые хранилища производит ответственный за эксплуатацию криптосредств.

6. Правила выдачи СКЗИ

6.1. Все экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых носителей ответственный за эксплуатацию

криптосредств выдает пользователям криптосредств под подпись в журнале учета СКЗИ.

6.2. Ответственный за эксплуатацию криптосредств заводит и ведет на каждого пользователя криптосредств учетный лист по форме Приложения 5, в котором регистрирует числящиеся за ним криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

6.3. Передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов пользователю криптосредств может производить только ответственный за эксплуатацию криптосредств под подпись в журнале учета СКЗИ. Передача криптосредств между пользователями криптосредств запрещена.

7. Правила уничтожения СКЗИ

7.1. Уничтожение криптоключей (исходной ключевой информации) 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. 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 криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

7.3. Ключевые носители уничтожают 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 криптосредствам, 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 криптосредствам уничтожают путем сжигания или с помощью любых бумагорезательных машин.

7.5. Криптосредства уничтожают (утилизируют) по приказу руководителя РЦОИ.

7.6. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств, и они полностью отсоединены от 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 криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

7.8. . Ключевые носители должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. 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 в журнал учета СКЗИ заносит ответственный за эксплуатацию криптосредств.

7.9. Ключевые документы уничтожаются ответственным за эксплуатацию криптосредств**.**

7.10. Уничтожение большого объема ключевых документов может быть оформлено актом по установленной форме, согласно Приложению 6. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. В акте указывается что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих криптосредства носителей, эксплуатационной и технической документации.

8. Установка и хранение СКЗИ

8.1. Размер помещений для установки и хранения СКЗИ должен быть выбран с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией на СКЗИ.

8.2. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

8.3. Окна помещений, расположенных на первых и последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, необходимо оборудовать охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в помещения.

8.4. Размещение и специальное оборудование в помещениях должны исключить возможность неконтролируемого просмотра посторонними лицами ведущихся там работ.

8.5. Для предотвращения просмотра извне помещений, в которых установлены или хранятся СКЗИ, их окна должны быть защищены.

8.6. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по АСОУ.

8.7. Охрана и организация режима в помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц.

8.8. Режим охраны помещений, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливается приказом ректора АСОУ.

9. Размещение и монтаж СКЗИ

9.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с криптосредствами, в соответствующих помещениях должны сводить к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

9.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

10. Заключительные положения

10.1. Все пользователи криптосредств должны быть предупреждены об ответственности за действия с СКЗИ, нарушающие требования настоящих Правил и других организационных и правовых документов, определяющих меры по защите информации с помощью криптосредств.

10.2. Пользователи криптосредств, в том числе ответственный за эксплуатацию криптосредств должны быть ознакомлены в части их касающейся, с настоящими Правилами до начала работы с криптосредствами под подпись.

Приложение 1

Уч. № _____
20_____ г.

ЖУРНАЛ
учета лиц, допущенных к работе с СКЗИ

№ п/п	Ф.И.О. и должность допущенного к работе с СКЗИ	Наименование СКЗИ	Серийный номер СКЗИ
1.	2	3	4
2.	*Иванов И.И.*	*Vipnet Client 4.2*	*000-111-222-444*
3.			
4.			
5.			
6.			
7.			
8.			

Лист _____

Приложение 2

АКТ № _____

проверки соблюдений условий использования средств криптографической защиты информации

Дата составления: «____» _____ 20__ г.

Место проведения проверки: _____

Комиссия, назначенная приказом ректора АСОУ от «___» __20__ №__в составе:

Председатель: _____

Члены комиссии: _____

Проведена проверка соблюдений условий использования средств криптографической защиты информации в _____.

(наименование информационной системы РЦОИ)

В ходе проведения проверки определялись:

- состояние и актуальность журнала учета СКЗИ;
- состояние и актуальность журнала учета пользователей СКЗИ;
- соответствие технического состояния СКЗИ и сопрягаемых с СКЗИ ТС требованиям эксплуатационной документации на СКЗИ, ИС и систему защиты информации;
- знание и выполнение пользователями правил хранения, выдачи и уничтожения СКЗИ;
- знание и выполнение пользователями правил защиты СКЗИ;
- случаи компрометации СКЗИ и действия по устранению причин и последствий компрометации СКЗИ;
- состояние помещений с установленными или хранящимися в них СКЗИ и состояние режима доступа в эти помещения;
- наличие и состояние хранилищ СКЗИ и режим доступа к ним.

Выявленные нарушения:

_____

ЗАКЛЮЧЕНИЕ комиссии:

Соблюдений условий использования средств криптографической защиты информации соответствует / не соответствует *(нужное подчеркнуть)* требованиям к условиям использования СКЗИ в организации «Государственное бюджетное образовательное учреждение высшего образования Московской области «Академия социального управления».

Председатель комиссии _____

Члены комиссии: _____

_____

Приложение 3

ЖУРНАЛ
учета СКЗИ

учетный № _____
_____2_____ год.

№	Наименование СКЗИ	Регистрационные номера СКЗИ	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и подпись о получении
1	2	3	4	5	6	7	8
1	*VipNet Client 3.2*	*16162-8507*	*1*	*ЗАО «Калуга Астрал»*	*12.12.2017 Договор №1234562*	*Иванов И.И.*	*(подпись Иванова И.И.)*

Отметка о подключении (установке) СКЗИ	Отметка об изъятии СКЗИ из аппаратных средств, уничтожении	Примечание

			ключевых документов			
Ф.И.О. пользователя СКЗИ, производившего 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. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15
«ГБОУ ВО МО «Академия социального управления»	*1.01.2018г*	*Инв.№ 00023*				*Пример заполнения*

Приложение 4

Правила
по формированию и ведению журнала учета СКЗИ (поэкземплярного)

Настоящая инструкция определяет порядок ведения журнала учета СКЗИ.

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается из листов плотностью 100-120 г/м^2.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – наименование СКЗИ.
         2.2.2.1. Возможные варианты:
         2.2.2.2. ViPNet CSP, версия 3.2.
         2.2.2.3. ViPNet Клиент КС2, версия 3.1.
         2.2.2.4. ViPNet Координатор КС2, версия 3.1.
         2.2.2.5. ViPNet Координатор КС2 Linux.
         2.2.2.6. Домен-КС2 [ViPNet КриптоСервис].
      2.2.3. Графа 3 – серийный (регистрационный) номер СКЗИ.
      2.2.4. Графа 4 – 1 (если лицензия на одну установку) или по порядку.
      2.2.5. Графа 5 – наименование организации, передавшей СКЗИ.
      2.2.6. Графа 6 – указывается дата установки.
      2.2.7. Графа 7 – ФИО лица, на чьем компьютере произведена установка.
      2.2.8. Графа 8 – подпись лица по п. 7.
      2.2.9. Графа 9 – ФИО лица, производившего установку СКЗИ при передаче через агента, или наименование организации, установившей СКЗИ.
      2.2.10. Графа 10 – дата установки.
      2.2.11. Графа 11 – серийный или инвентарный номер компьютера.
      2.2.12. Графа 12 – не заполняется.
      2.2.13. Графа 13 – не заполняется.
      2.2.14. Графа 14 – не заполняется.
   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 5

Учетный лист
пользователя СКЗИ

Пользователь _____

№п.п.	Наименование СКЗИ	Регистрационные номера СКЗИ	Номера экземпляров ключевых документов	Дата получения	Примечание

Приложение 6

АКТ № _____ от «__» _____ 20__г.

об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

Комиссия в составе:

Председатель комиссии: _____
(ФИО, должность)

Члены комиссии _____
(ФИО, должность)

_____
(ФИО, должность)

произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов подтверждаю:

Председатель комиссии: _____/_____

Члены комиссии _____/_____
_____/_____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах РЦОИ, и криптоключами к ним

1. Общие положения

1.1 Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации (далее – СКЗИ), предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – Информация), обрабатываемой в информационных системах РЦОИ (далее – ИС РЦОИ), и криптоключами к ним регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты Информации.

1.2 Под криптосредством в настоящей Инструкции понимается шифровальное (криптографическое) средство, предназначенное для защиты информации.

1.3 К криптосредствам (шифровальным, криптографическим средствам) относятся:

Средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

Ключевые носители (независимо от вида носителя ключевой информации).

1.4 В настоящей Инструкции используются следующие понятия и определения:

Доступ к информации – возможность получения информации и ее использования.

Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

Ключевой носитель – физический носитель определенной структуры, содержащий криптоключи.

Компрометация криптоключа – утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз – перечень возможных угроз.

Пользователь криптосредства – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

1.5 Для обеспечения безопасности информации при её обработке в ИС РЦОИ должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства (имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

1.6 Класс криптосредства определяется в соответствии с Приказом Федеральной службы безопасности Российской Федерации (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 требований к защите персональных данных для каждого из уровней защищенности».

2. Организационная структура

Безопасность обработки информации в ИС РЦОИ с использованием криптосредств организует и обеспечивает ответственный за эксплуатацию СКЗИ в ИС РЦОИ.

3. Учет ключевых носителей

3.1 Ключевые носители подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых носителей считается ключевой носитель информации.

3.2 Все экземпляры ключевых носителей выдаются пользователям криптосредств под подпись в соответствующем журнале учета СКЗИ.

3.3 Передача ключевых носителей допускается только между пользователями криптосредств и ответственным за эксплуатацию СКЗИ под подпись в соответствующем журнале учета СКЗИ. Аналогичная передача между пользователями криптосредств осуществляется с письменного разрешения ответственного за эксплуатацию СКЗИ.

3.4 Для исключения компрометации ключевых носителей на период отсутствия пользователя и в нерабочее время, ключевые носители убираются в защищенные хранилища (ящики, шкафы) индивидуального пользования, которые, в свою очередь, закрываются на ключ и опечатываются.

3.5 Учет эксплуатационной и технической документации к криптосредствам:

3.5.1 Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

3.5.2 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под подпись.

3.5.3 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и ответственным пользователем за эксплуатацию СКЗИ под подпись. Аналогичная передача между пользователями криптосредств осуществляется с санкции ответственного за эксплуатацию СКЗИ.

3.6 Плановая смена ключевых носителей:

3.6.1 Заказ на изготовление очередных ключевых носителей, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

3.7 Внеплановая смена ключевых носителей:

3.7.1 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.

3.8 Уничтожение ключевых носителей:

3.8.1 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются ответственному за эксплуатацию СКЗИ или уничтожаются на месте.

3.8.2 Уничтожение ключевых носителей производится путем стирания (разрушения) криптоключей без повреждения ключевого носителя.

3.8.3 Бумажные и прочие сгораемые ключевые носители уничтожаются путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

3.8.4 Ключевые носители уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые носители уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия).

3.9 Уничтожение эксплуатационной и технической документации к криптосредствам:

3.9.1 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

4. Техническое обслуживание криптосредств

4.1 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

4.2 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

5. Порядок доступа к хранилищам

5.1 Эксплуатация хранилищ:

5.1.1 Пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

5.1.2 Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

5.2 При необходимости доступа к содержимому хранилища работник,

ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

5.3 По окончании работы работник закрывает и опечатывает хранилище, за которое он ответственен.

5.4 Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за данные хранилища.

6. Контроль безопасности криптосредств

Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на ответственного за эксплуатацию СКЗИ в пределах его полномочий.

7. Ответственность за нарушение требований

7.1 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

7.2 Ответственный за эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки Информации с использованием криптосредств лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Порядок
доступа работников РЦОИ в помещения, в которых ведется обработка информации ограниченного доступа и расположены средства криптографической защиты информации

1. Общие положения

1.1. Настоящий Порядок доступа работников в помещения РЦОИ, в которых ведется обработка информации ограниченного доступа, в том числе персональных данных, (далее – Информации) не содержащей сведения, составляющие государственную тайну, и расположены средства криптографической информации разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом 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» и другими нормативными правовыми актами.

1.2. Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается, в том числе, установлением правил доступа в помещения, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

1.3. Размещение информационных систем (далее – ИС), в которых обрабатывается Информация, должно осуществляться в пределах контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации. Для помещений, в которых обрабатывается Информация (далее – Помещения) и расположены средства криптографической защиты информации (далее – СКЗИ), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, криптосредств и ключевых носителей к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

2. Допуск в помещения, в которых ведётся обработка информации ограниченного доступа

2.1. В помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только работники, уполномоченные на обработку Информации, а

также только лица, имеющие право доступа в помещения РЦОИ, где осуществляется обработка Информации.

2.2. При оборудовании Помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

2.3. Нахождение в помещениях с ИС лиц, не включенных в перечни, указанные в пункте 2.1. настоящего Порядка, возможно только в присутствии работника, уполномоченного на обработку Информации в данном помещении. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

2.4. Работники, допущенные к обработке Информации, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители Информации без присмотра в незапертом помещении.

2.5. Помещения, в которых ведется обработка Информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками и/ или системой контроля и управления доступом (далее – СКУД). Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

2.6. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

2.7. После окончания рабочего дня дверь каждого помещения, в котором ведется обработка Информации закрывается на ключ или с помощью СКУД здания.

2.8. В нерабочее время помещения, в которых осуществляется функционирование СКЗИ, должны ставиться на охрану, при этом все окна и двери должны быть надежно закрыты, ключевые документы убраны в запираемые шкафы.

3. Допуск лиц в помещения

3.1. Для предотвращения просмотра извне окна Помещений должны быть защищены шторами или жалюзи.

3.2. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, оборудуются охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

3.3. При утрате ключа от хранилища (запираемого шкафа) или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей. Факт изготовления новых ключей должен быть документально оформлен в виде акта в произвольной форме. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

3.4. Контроль и управление физическим доступом к информационным системам и средствам криптографической защиты должны предусматривать:

поддерживание в актуальном состоянии перечня лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах;

санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;

учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений под подпись в соответствующем журнале.

3.5. В обычных условиях помещения и находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями СКЗИ или ответственным за эксплуатацию СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за эксплуатацию СКЗИ. Прибывший ответственный за эксплуатацию СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

3.6. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка Информации и расположены средства криптографической информации, возлагается на сотрудников структурных подразделений, уполномоченных на обработку Информации в РЦОИ, а также руководителей структурных подразделений РЦОИ.

3.7. В случае нарушения настоящего Порядка работники могут быть привлечены к дисциплинарной ответственности.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Инструкция
по восстановлению конфиденциальной связи в случае компрометации действующих ключей к криптосредствам в информационных системах РЦОИ

1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

1). утрата (хищение) носителей ключевой информации (далее – НКИ), в том числе с последующим их обнаружением;

2). увольнение (переназначение) работников, имевших доступ к ключевой информации;

3). нарушение правил хранения криптоключей;

4). вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

5). отрицательный результат при проверке наложенной электронной подписи;

6). несанкционированное или безучётное копирование ключевой информации;

7). все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

2. События 1-4 п.1 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

3. При наступлении любого из перечисленных выше событий владелец ключа (пользователь) должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию криптографических средств защиты информации лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа (пользователь) обязан убедиться, что его сообщение получено и прочтено адресатом – ответственным за эксплуатацию криптографических средств защиты информации.

4. При подтверждении факта компрометации действующих ключей владелец (пользователь) обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей в течение трёх рабочих дней.

5. Для восстановления конфиденциальной связи после компрометации действующих ключей владелец (пользователь) получает новые ключи в течение рабочего дня на основании предоставленного заявления.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Уч. № _____
20_____ г.

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание
1	2	3	4	5	6	7
пример	*Dallas Lock 8-K*	*000-111-222-444*	*X0-0001223*	*ГБУ НСО «ЦЗИ НСО»*	*Каб. 206*	
пример	*Kaspersky endpoint Protection 11*	*000-111-222-444*	*X0-0001223*	*ГБУ НСО «ЦЗИ НСО»*	*Каб. 206*	
пример	*Vipnet Client 4.2*	*000-111-222-444*	*X0-0001223*	*ГБУ НСО «ЦЗИ НСО»*	*Каб. 206*	

Лист _____

Приложение

Правила
по формированию и ведению журнала учета средств защиты информации

Настоящая инструкция определяет порядок ведения журнала учета средств защиты информации.

1. ФОРМИРОВАНИЕ ЖУРНАЛА.
   1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации:
   1.2. Обложка журнала изготавливается из листов плотностью 100-120 г/м^2.
   1.3. Все листы журнала, за исключением листов обложки, нумеруются.
   1.4. Все листы журнала, вместе с обложкой сшиваются.

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:
      2.2.1. Графа 1 – номер записи по порядку.
      2.2.2. Графа 2 – наименование средства защиты информации.
      2.2.3. Графа 3 – серийный (заводской) номер.
      2.2.4. Графа 4 – номер специального защитного знака.
      2.2.5. Графа 5 – наименование организации, установившей СЗИ.
      2.2.6. Графа 6 – место установки.
      2.2.7. Графа 7 – примечание.
   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.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

ЖУРНАЛ
учета паролей пользователей государственной информационной системы
«АИС РЦОИ РИС МО»

Уч. № _____
20_____ г.

ФИО пользователя (АРМ № ___ГИС «АИС РЦОИ РИС МО») _____

№ п.п.	Значение пароля	Дата	Подпись в получении	Подпись администратора ИСПДн
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Лист _____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

ЖУРНАЛ
учета паролей пользователей информационной системы персональных данных
«АИС ГИА»

Уч. № _____
20_____ г.

ФИО пользователя (АРМ № ___ ИСПДн «АИС ГИА») _____

№ п.п.	Значение пароля	Дата	Подпись в получении	Подпись администратора ИСПДн
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Лист _____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

ЖУРНАЛ
учета печати конфиденциальной информации

Кабинет № _____ (Листов __ _____)

Действует с «_____» _____ 20 __ ___ г.

№ п/п	Наименование принтера для печати конфиденциальной информации	Учетный номер	Место нахождения принтера	Примечание
1	2	3	4	5

Ответственный за печать конфиденциальной информации*: _____
Лист _____

№ п/п	Дата и время	Принтер, на котором распечатан документ (учетный номер)	Название документа	Количество листов в документе	Ф.И.О. и подпись лица, которым был распечатан документ
1	2	3	4	5	6

Ответственный за печать конфиденциальной информации*: _____
Лист _____

*Ответственный за печать конфиденциальной информации расписывается по завершении заполнения листа журнала.

Правила
регистрации печати конфиденциальной информации

Формирование журнала.
1.1. Журнал формируется из стандартных листов формата А4 в альбомной ориентации.
1.2. Обложка журнала изготавливается на отдельном листе.
1.3. Все листы журнала, за исключением листов обложки, нумеруются.
1.4. Все листы журнала, вместе с обложкой сшиваются.

Ведение журнала.
Перед началом использования журнала на лицевой стороне обложки указывается номер кабинета с установленными принтерами, количество листов и дата начала ведения журнала.

Первый лист предназначен для перечня принтеров, на которых может быть распечатана конфиденциальная информация.
Графы перечня заполняются следующим образом:
2.1. Графа 1 – номер записи по порядку.
2.2. Графа 2 – наименование принтера для печати конфиденциальной информации.
2.3. Графа 3 – учетный номер принтера.
2.4. Графа 4 – место установки принтера.
2.5. Графа 5 – любая информация касательно внесенного в список принтера.

Второй лист и далее предназначен для регистрации печати конфиденциальной информации.
2.6. Графа 1 – номер записи по порядку.
2.7. Графа 2 – дата и время печати.
2.8. Графа 3 – учетный номер принтера, на котором распечатан документ.
2.9. Графа 4 – название документа.
2.10. Графа 5 – количество листов документа.
2.11. Графа 6 – ФИО пользователя, напечатавшего документ.
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.

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

ЖУРНАЛ
учета выдачи аппаратных лицензионных электронных ключей ABBYY

Журнал начат «___» _____202__ г.

_____ /Должность/

_____/ ФИО должностного лица/

Журнал завершен «___» _____202__ г.

_____ /Должность/

_____/ ФИО должностного лица/

На ___ листах

Номер электронного ключа ABBYY _____

№ п/п	Дата получения ключа	Время получения ключа	ФИО пользователя	Подпись пользователя	Дата сдачи ключа	Время сдачи ключа	Подпись пользователя
1	2	3	4	5	6	7	8
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Лист _____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

Уч. № _____
20_____ г.

ЖУРНАЛ
активации электронных ключей

№ п/п	Номер электронного ключа	Дата активации ключа	Место активации	Срок действия лицензии	ФИО производившего активацию	Подпись производившего активацию	Примечание
1	2	3	4	5	6	7	8

Лист _____

УТВЕРЖДЕНО
приказом АСОУ
от 21.02.2022 № 235-04

ЖУРНАЛ
проведения инструктажей по информационной безопасности

Начат: _____

Окончен: _____

№ п/п	Наименование ИСПДн	Дата проведения инструктажа	ФИО инструктируемого сотрудника	Краткое содержание инструктажа	Должность, ФИО, проводившего инструктаж	Подпись инструктирующего	Подпись инструктируемого

Лист _____