УТВЕРЖДЕНО
Приказом ГОАУСОН «Кировский ПНИ»
от 12.03.2021 №135

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах государственного областного автономного учреждения социального обслуживания населения «Кировский психоневрологический интернат»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах государственного областного автономного учреждения социального обслуживания населения «Кировский психоневрологический интернат» (далее –Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», 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», постановления Правительства Российской Федерации 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», приказом 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», приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее –защищаемая информация, информация), в информационных системах (далее – ИС) государственного областного автономного учреждения социального обслуживания населения «Кировский психоневрологический

интернат» (далее – Учреждение, Оператор, ГОАУСОН «Кировский ПНИ») на всех стадиях (этапах) создания ИС и в ходе их эксплуатации.

1.3. К защищаемой информации, обрабатываемой в ИС Учреждения, относится следующая информация:

– персональные данные, содержащиеся в информационных системах персональных данных Учреждения;

– информация, не содержащая сведения, составляющие государственную тайну, содержащаяся в государственных информационных системах Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

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

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

Обработка информации –действия (операции) с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Оператор – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. В случае обработки персональных данных под оператором понимается 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.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (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.

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

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

Средства вычислительной техники – совокупность программных и технических элементов

систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

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

Уровень защищенности персональных данных –комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

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

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Под организацией обеспечения безопасности защищаемой информации при ее обработке в ИС понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее –СЗИ).

3.2. СЗИ включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации, уровня защищенности персональных данных (далее –ПДн), который необходимо обеспечить, класса государственная информационная система (далее –ГИС) и информационных технологий, используемых в ИС.

3.3. Безопасность защищаемой информации при ее обработке в ИС обеспечивает оператор или лицо, осуществляющее обработку защищаемой информации по поручению оператора на основании заключаемого с этим лицом договора (далее –уполномоченное лицо). Договор между оператором и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность защищаемой информации при ее обработке в ИС.

3.4. Защита информации, содержащейся в ИС, обеспечивается путем выполнения Оператором требований к организации защиты информации, содержащейся в ИС, и требований к мерам защиты информации, содержащейся в ИС.

3.5. Для обеспечения безопасности защищаемой информации, содержащейся в ИС, Оператором назначается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности информации.

3.6. Оператором назначается лицо, ответственное за организацию обработки защищаемой информации.

3.7. Для проведения работ по защите информации в ходе создания и эксплуатации ИС Оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.8. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании».

3.9. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках СЗИ.

3.10.Организационные и технические меры защиты информации, реализуемые в рамках СЗИ, должны быть направлены на исключение:

– неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

– неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

– неправомерного блокирования информации (обеспечение доступности информации).

3.11.Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в ИС;

– разработка СЗИ;

– внедрение СЗИ;

– аттестация ИС по требованиям защиты информации (далее - аттестация ИС);

– обеспечение защиты информации в ходе эксплуатации аттестованной ИС;

– обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации.

4. ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется Оператором.

4.2. Формирование требований к защите информации, содержащейся в ИС, включает:

– принятие решения о необходимости защиты информации, содержащейся в ИС;

– классификацию ИС по требованиям защиты информации, определение уровня защищенности ПДн, при их обработке в ИС;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработку на их основе модели угроз безопасности информации;

– определение требований к СЗИ.

4.3. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

– анализ целей создания ИС и задач, решаемых этой ИС;

– определение информации, подлежащей обработке в ИС;

– анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИС;

– принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в ИС, основных этапов создания СЗИ и функций по обеспечению защиты информации, содержащейся в ИС.

4.4. Результаты классификации ИС оформляются актом классификации.

4.5. Результаты определения уровня защищенности ПДн при их обработке в ИС оформляются актом определения уровня защищенности.

4.6. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

4.7. При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИС, включающие структуру и состав ИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС, с иными ИС и информационно-телекоммуникационными сетями, режимы обработки информации в ИС и в их отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности их функционирования.

4.8. По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке

структурно-функциональных характеристик ИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

4.9. Модель угроз безопасности информации должна содержать описание ИС и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

4.10.Требования к СЗИ определяются в зависимости от класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

4.11.При определении требований к СЗИ учитываются положения политики Оператора в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну.

5. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Разработка СЗИ организуется Оператором.

5.2. Разработка СЗИ осуществляется в соответствии с техническим заданием на создание СЗИ, и в том числе, включает:

– проектирование СЗИ;
– разработку эксплуатационной документации на СЗИ;
– макетирование и тестирование СЗИ (при необходимости).

5.3. СЗИ не должна препятствовать достижению целей создания ИС и ее функционированию.

5.4. При разработке СЗИ учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

5.5. При проектировании СЗИ осуществляются следующие мероприятия:

– определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);
– определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ИС;
– выбираются меры защиты информации, подлежащие реализации в СЗИ;
– определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определяется структура СЗИ, включая состав (количество) и места размещения ее элементов;

– осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС;

– определяются параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации;

– определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

5.6. Результаты проектирования СЗИ отражаются в проектной документации на ИС.

5.7. При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по ИС и (или) ее СЗИ с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

5.8. Разработка эксплуатационной документации на СЗИ осуществляется в соответствии с техническим заданием на создание СЗИ.

5.9. При макетировании и тестировании СЗИ, в том числе, осуществляются:

– проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

– проверка выполнения выбранными средствами защиты информации требований к СЗИ;

– корректировка проектных решений, разработанных при создании СЗИ;

– корректировка проектной и эксплуатационной документации на СЗИ.

5.10. Макетирование СЗИ и ее тестирование может проводиться, в том числе, с использованием средств и методов моделирования ИС и технологий виртуализации.

6. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Внедрение СЗИ организуется Оператором.

6.2. Внедрение СЗИ осуществляется в соответствии с проектной и эксплуатационной документацией на СЗИ и, в том числе, включает:

– установку и настройку средств защиты информации в ИС;

– разработку документов, определяющих правила и процедуры, реализуемые Оператором для обеспечения защиты информации в ИС в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации;

– предварительные испытания СЗИ (при необходимости);

– опытную эксплуатацию СЗИ (при необходимости);

– анализ уязвимостей ИС и принятие мер защиты информации по их устранению;

– приемочные испытания СЗИ (при необходимости).

6.3. Установка и настройка средств защиты информации в ИС должна проводиться в соответствии с эксплуатационной документацией на СЗИ и документацией на средства защиты информации.

6.4. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

– управления (администрирования) СЗИ;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

– управления конфигурацией аттестованной ИС и СЗИ;

– контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

– защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

6.5. При внедрении организационных мер защиты информации осуществляются:

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации;

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

6.6. Предварительные испытания СЗИ включают проверку работоспособности СЗИ, а также принятие решения о возможности опытной эксплуатации СЗИ.

6.7. Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации СЗИ.

6.8. Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации угроз безопасности информации. Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ИС. При анализе уязвимостей ИС проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением. В случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

6.9. Приемочные испытания СЗИ включают проверку выполнения требований к СЗИ в соответствии с техническим заданием на создание СЗИ.

7. АТТЕСТАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

7.1. Аттестация ИС организуется Оператором и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СЗИ требованиям по безопасности информации.

7.2. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, акт определения уровня защищенности ПДн при их обработке в ИС, техническое задание на создание СЗИ, проектная и эксплуатационная документация на СЗИ, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний СЗИ (при наличии).

7.3. Аттестация ИС проводится в соответствии с программой и методиками аттестационных испытаний. Для проведения аттестации ИС применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии (не соответствии)ИС требованиям по защите информации и

аттестат соответствия в случае положительных результатов аттестационных испытаний.

7.4. Допускается аттестация ИС на основе результатов аттестационных испытаний выделенного набора сегментов ИС, реализующих полную технологию обработки информации. В этом случае распространение аттестата соответствия на другие сегменты ИС осуществляется при условии их соответствия сегментам ИС, прошедшим аттестационные испытания. Сегмент считается соответствующим сегменту ИС, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, уровни защищенности, уровни важности, угрозы безопасности информации, реализованы одинаковые проектные решения по ИС и ее СЗИ. В сегментах ИС, на которые распространяется аттестат соответствия, Оператором обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно-распорядительных документов по защите информации.

7.5. Особенности аттестации ИС на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты ИС определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

7.6. Повторная аттестация ИС осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании СЗИ, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

8. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

8.1. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется Оператором в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и, в том числе, включает:

– управление (администрирование) СЗИ;
– выявление инцидентов и реагирование на них;
– управление конфигурацией аттестованной ИС и СЗИ;
– контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС.

8.2. В ходе управления (администрирования) СЗИ осуществляются:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;

– управление средствами защиты информации в ИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

– установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

– централизованное управление СЗИ (при необходимости);

– регистрация и анализ событий в ИС, связанных с защитой информации (далее - события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ и отдельных средств защиты информации, а также их обучение;

– сопровождение функционирования СЗИ в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

8.3. В ходе выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

8.4. В ходе управления конфигурацией аттестованной ИС и ее СЗИ осуществляются:

– поддержание конфигурации ИС и ее СЗИ (структуры СЗИ, состава, мест установки и параметров настройки средств защиты информации,

программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СЗИ (поддержание базовой конфигурации ИС и ее СЗИ);

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и СЗИ;

– управление изменениями базовой конфигурации ИС и СЗИ, в том числе определение типов возможных изменений базовой конфигурации ИС и СЗИ, санкционирование внесения изменений в базовую конфигурацию ИС и СЗИ, документирование действий по внесению изменений в базовую конфигурацию ИС и СЗИ, сохранение данных об изменениях базовой конфигурации ИС и СЗИ, контроль действий по внесению изменений в базовую конфигурацию ИС и ее СЗИ;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и СЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и СЗИ;

– внесение информации (данных) об изменениях в базовой конфигурации ИС и СЗИ в эксплуатационную документацию на СЗИ;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

8.5. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

– контроль за событиями безопасности и действиями пользователей в ИС;

– контроль (анализ) защищенности информации, содержащейся в ИС;

– анализ и оценка функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;

– периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

8.6. Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с Планом мероприятий по защите информации (Приложение № 1). Внутренние проверки режима

защиты информации проводятся в соответствии с Планом внутренних проверок режима защиты информации (Приложение № 2). По результатам проведения внутренней проверки составляется Отчет о результатах внутренней проверки режима защиты информации в ГОАУСОН «Кировский ПНИ» (Приложение № 3).

9. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИЗ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ ИНФОРМАЦИИ

9.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации осуществляется Оператором в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и, в том числе, включает:

– архивирование информации, содержащейся в ИС;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

9.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности Оператора.

9.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

Приложение № 1
к Положению по организации и проведению
работ по обеспечению безопасности
защищаемой информации, не содержащей
сведения, составляющие государственную
тайну, при ее обработке в информационных
системах ГОАУСОН «Кировский ПНИ»

План
мероприятий по обеспечению безопасности защищаемой информации
в ГОАУСОН «Кировский ПНИ»

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с информацией	При необходимости	Разработка и (или) актуализация организационно-распорядительных документов по защите информации
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области защиты информации». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к защищаемой информации	При необходимости	В случае создания ИС, а также приведения имеющихся ИС в соответствие с требованиями по безопасности информации необходимо разграничить доступ сотрудников Оператора к защищаемой информации
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи ПДн, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
6.	Ведение журналов учета отчуждаемых машинных носителей защищаемой информации, средств защиты информации	Постоянно	-
7.	Повышение квалификации сотрудников в области защиты информации	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности информации)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия защищаемой информации
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Оператором устанавливаются сроки обработки, которые документально подтверждаются в нормативных документах Оператора. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области защиты информации»
11.	Определение класса защищенности ИС	При необходимости	Определение класса защищенности ИС осуществляется при создании ИС, при изменении состава ИС, масштаба ИС, степеней ущерба для характеристик ИС (конфиденциальности, целостности, доступности)
12.	Определение уровня защищенности ПДн при их обработке в ИС	При необходимости	Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
13.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании СЗИ
14.	Аттестация ИС на соответствие требованиям по обеспечению безопасности информации	При необходимости	-
15.	Эксплуатация ИС и контроль безопасности защищаемой информации	Постоянно	

Приложение № 2
к Положению по организации и проведению
работ по обеспечению безопасности
защищаемой информации, не содержащей
сведения, составляющие государственную
тайну, при ее обработке в информационных
системах ГОАУСОН «Кировский ПНИ»

План
внутренних проверок режима защиты информации
в ГОАУСОН «Кировский ПНИ»

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн Федеральному Закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в год	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в год	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Разово при устройстве на работу	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - Уведомления о факте обработки ПДн без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПДн; - Формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами ГОАУСОН «Кировский ПНИ» по вопросам обработки ПДн; - Типового обязательства о прекращении обработки ПДн в случае расторжения служебного контракта (трудового договора); - Разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	Разово при устройстве на работу	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	

8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	
9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	Разово при устройстве на работу	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику ГОАУСОН «Кировский ПНИ» в отношении обработки ПДн	Ежегодно	
11.	Организация анализа и пересмотра имеющихся угроз безопасности информации, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального Закона от 27.07.2006 № 152-ФЗ «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности информации средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИС	При необходимости	
15.	Контроль учета машинных носителей информации	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности информации, класса защищенности ИС и уровня защищенности ПДн в ИС	Раз в полгода	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИС	При необходимости	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	

Приложение № 3
к Положению по организации и
проведению работ по обеспечению
безопасности защищаемой информации,
не содержащей сведения, составляющие
государственную тайну, при ее
обработке в информационных системах
ГОАУСОН «Кировский ПНИ»

Отчет
о результатах внутренней проверки системы защиты информации в ГОАУСОН «Кировский ПНИ»

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах ГОАУСОН «Кировский ПНИ».

1.2 Проверка проводилась «___»_____20__ г. по адресу:_____

1.3 В ходе проверки были проведены следующие мероприятия:

1) _____
2) _____
3) _____
4) _____
5) _____

1.4 Результаты проведения проверки:

6) _____
7) _____
8) _____
9) _____
10) _____

1.5 Необходимые мероприятия.

На основании проведения внутренней проверки системы защиты информации рекомендуется осуществить следующие мероприятия:

11) _____
12) _____
13) _____
14) _____
15) _____

Подписи ответственных лиц, проводивших внутреннюю проверку системы защиты информации:

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