УТВЕРЖДАЮ
Президент Общероссийской
общественной организации
«Общество врачей
Российской Федерации»

_____ Янушевич О.О.
«__» _____20__г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах Общероссийской общественной организации «Общество врачей Российской Федерации» (далее – Общество).

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 Общества «Общество врачей Российской Федерации» (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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 февраля 2013 г. № 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 февраля 2013 г. № 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), в информационных системах (далее – ИС) (далее – Общество на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

1.3. Руководитель Общества «Общество врачей Российской Федерации») несет персональную ответственность за обеспечение информационной безопасности.

1.4. К защищаемой информации, обрабатываемой в ИС Общества, относится следующая информация:

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

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

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), 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 защищенности государственной информационной системы (далее – ГИС) и информационных технологий, используемых в ИС.

3.3. Безопасность защищаемой информации при ее обработке в ИС обеспечивает или лицо, осуществляющее обработку защищаемой информации по поручению, Общество на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Обществом 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 Обществом требований к организации защиты информации, содержащейся в ИС, и требований к мерам защиты информации, содержащейся в ИС.

3.5. Обществом назначается лицо, ответственное за организацию обработки персональных данных при их обработке в «Общество врачей Российской Федерации».

3.6. Для обеспечения безопасности защищаемой информации, содержащейся в ИС, Обществом назначается структурное подразделение или должностное лицо (работники), ответственное за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах (Общества «Общество врачей Российской Федерации (далее – Ответственный).

3.7. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации ИС Обществом 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 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.8. При необходимости к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты могут привлекаться специализированные организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (за исключением случая, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»).

3.9. 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 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

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

3.11. 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).

3.12. 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.

3.13. В целях осуществления мониторинга, предусмотренного подпунктом «в» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», должностным лицам органов федеральной службы безопасности разрешается беспрепятственный доступ (в том числе удаленный) к принадлежащим используемым Обществом информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

3.14. Ответственный за обеспечение информационной безопасности осуществляет организацию и контроль исполнения:

– указаний, данных органами федеральной службы безопасности по результатам мониторинга;

– организационных и технических мер, решение о необходимости осуществления которых принято Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направлению в адрес Ассоциации.

4. ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

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

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) 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. В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

4.8. 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 ее отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности ее функционирования.

4.9. По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

4.10. 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.

4.11. 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.

4.12. При определении требований к СЗИ учитываются положения политики Ассоциация в отношении обработки персональных данных.

5. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Разработка СЗИ организуется Обществом.

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 требования к параметрам 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.

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 Обществом.

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 Обществом 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:

– планирования мероприятий по защите информации в ИС;

– 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 за обеспечением уровня защищенности информации, содержащейся в ИС;

– информирования и обучения персонала 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. По результатам анализа уязвимостей должно быть подтверждено, что в ИС отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

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 проводится на этапе ее создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний), в результате которых подтверждается соответствие ИС требованиям по защите информации в условиях ее эксплуатации. Допускается проведение аттестации ИС на этапе ее эксплуатации в случае, если Обществом принято решение об обработке защищаемой информации после ввода в эксплуатацию ИС.

7.2. Для проведения аттестационных испытаний Общество привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным

постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (далее – орган по аттестации).

7.3. Срок проведения работ по аттестации ИС устанавливается Ассоциацией по согласованию с органом по аттестации, но не может превышать четырех месяцев.

7.4. Проведение аттестационных испытаний ИС должностными лицами, осуществляющими проектирование и (или) внедрение СЗИ ИС, не допускается.

7.5. Для проведения работ по аттестации Учреждение представляет в орган по аттестации следующие документы или их копии (по решению Ассоциация документы (их копии) могут быть представлены в орган по аттестации в виде электронных документов):

– технический паспорт на ИС по форме согласно приложению № 1 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29 апреля 2021 г. № 77;

– акт классификации ИС по форме согласно приложению № 3 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29 апреля 2021 г. № 77;

– акт категорирования объекта критической информационной инфраструктуры (если аттестуемая ИС является объектом критической информационной инфраструктуры);

– акт определения уровня защищенности ПДн при их обработке в ИС (при обработке в аттестуемой ИС ПДн);

– модель угроз безопасности информации;

– техническое задание на создание (развитие, модернизацию) ИС и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации ИС;

– проектная документация на систему защиты информации ИС (в случае ее разработки в ходе создания ИС);

– эксплуатационная документация на систему защиты информации ИС и применяемые средства защиты информации;

– организационно-распорядительные документы по защите информации Общества, регламентирующие защиту информации в ходе эксплуатации ИС, в том числе план мероприятий по защите информации на ИС, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией ИС, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации (далее – документы по защите информации);

– документы, содержащие результаты анализа уязвимостей ИС и приемочных испытаний системы защиты информации ИС (в случае проведения анализа и испытаний в ходе создания ИС).

7.6. Общество ИС проводится в соответствии с программой и методиками аттестационных испытаний. Программа и методики аттестационных испытаний разрабатывается органом по аттестации в соответствии с Порядком организации и

проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77, и согласовывается с Обществом. В ходе аттестационных испытаний орган по аттестации может вносить изменения в программу и методики аттестационных испытаний по согласованию с Обществом.

7.7. В программу и методики испытаний должны быть включены следующие методы проверок (испытаний):

– экспертно-документальный метод, предусматривающий проверку соответствия СЗИ ИС установленным требованиям по защите информации на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования ИС;

– анализ уязвимостей ИС, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

– испытания СЗИ путем осуществления попыток несанкционированного доступа (воздействия) к ИС в обход ее СЗИ.

7.8. 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, Обществом обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно-распорядительных документов по защите информации.

7.9. Особенности аттестации ИС на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты ИС должны быть определены органом по аттестации в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

7.10. В ходе аттестационных испытаний Общество может вносить изменения в ИС, в том числе в архитектуру ее системы защиты информации, в целях приведения ИС в соответствие с требованиями по защите информации.

7.11. По результатам аттестационных испытаний Общество получает от органа по аттестации следующие документы:

– заключение по результатам аттестационных испытаний ИС;

– протокол по результатам аттестационных испытаний ИС.

7.12. В случае наличия в полученных Обществом от органа по аттестации заключении и протоколе сведений о наличии недостатков (несоответствий системы защиты информации ИС требованиям по защите информации) Ассоциация оценивает возможность их устранения в процессе аттестации ИС и, при возможности, обеспечивает их устранение. По результатам устранения всех обозначенных в заключении и протоколе недостатков

Общества оформляет и направляет в адрес органа по аттестации уведомление об устранении недостатков для оценки качества их устранения.

7.13. По результатам оценки качества устранения недостатков орган по аттестации повторно оформляет и направляет в адрес Общества заключение, в которое включаются сведения об устранении Обществом всех выявленных недостатков, а также делается вывод о возможности выдачи аттестата соответствия требованиям по защите информации (далее – аттестат соответствия) на ИС.

7.14. Учреждение в случае несогласия с выявленными органом по аттестации недостатками и выводами, содержащимися в заключении и протоколах, направляет в течение 5 рабочих дней с момента получения заключения и протоколов письменное обращение с обоснованием такого несогласия во ФСТЭК России.

К обращению прилагаются в электронном виде копии следующих документов:

– технический паспорт на ИС;

– акт классификации ИС по форме согласно приложению № 3 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29 апреля 2021 г. № 77;

– акт категорирования объекта критической информационной инфраструктуры (если аттестуемая ИС является объектом КИИ);

– акт определения уровня защищенности ПДн при их обработке в ИС (при обработке в аттестуемой ИС ПДн);

– программы и методики аттестационных испытаний ИС;

– заключения и протоколы.

7.15. ФСТЭК России проводит оценку представленных документов на предмет соответствия проведенных органом по аттестации аттестационных испытаний и выводов, содержащихся в заключении, требованиям по защите информации и положениям Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77 в течение 10 календарных дней с момента получения обращения. По согласованию с Обществом работники ФСТЭК России (территориального органа ФСТЭК России) могут провести контрольные испытания на ИС в соответствии с пунктами 15 и 16 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77. По результатам оценки ФСТЭК России (территориальный орган ФСТЭК России) направляет:

– в орган по аттестации уведомление о необходимости устранения выявленных недостатков в указанный в уведомлении срок. Копия уведомления направляется Учреждению. Орган по аттестации обязан устранить недостатки, выявленные ФСТЭК России по результатам оценки документов, в указанный в уведомлении срок и оформить аттестат соответствия (если установлено несоответствие аттестационных испытаний и (или) выводов, содержащихся в заключении или протоколах, требованиям по защите информации

или Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77).

– результаты проведенной оценки Обществом для устранения недостатков, выявленных органом по аттестации (если по результатам оценки подтвержден вывод органа по аттестации о невозможности выдачи аттестата соответствия, аттестат соответствия на ИС органом по аттестации не оформляется).

7.16. После получения аттестата соответствия на ИС от органа по аттестации Учреждение может получить от ФСТЭК России (территориального органа ФСТЭК России) заключение, содержащее описание выявленных по результатам экспертно-документальной оценки материалов, представленных органом по аттестации, недостатков и рекомендации по их устранению. В случае получения от ФСТЭК России (территориального органа ФСТЭК России) такого заключения Обществом обеспечивает устранение выявленных недостатков в соответствии с выданными рекомендациями в указанный в заключении срок. Об устранении недостатков Ассоциация информирует ФСТЭК России (территориальный орган ФСТЭК России). Неустранение недостатков, выявленных ФСТЭК России (территориальным органом ФСТЭК России), в указанный в заключении срок является основанием для приостановления действия аттестата соответствия на ИС.

7.17. Аттестат соответствия выдается на весь срок эксплуатации ИС. Общество в ходе эксплуатации ИС обеспечивает поддержку соответствия СЗИ аттестату соответствия в рамках реализации мероприятий, предусмотренных пунктом 18 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

7.18. Действие аттестата соответствия может быть приостановлено ФСТЭК России (территориальным органом ФСТЭК России) в случаях, предусмотренных пунктом 34 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77. Учреждение прекращает эксплуатацию ИС со дня получения уведомления о приостановлении действия аттестата соответствия.

7.19. Действие аттестата соответствия может быть возобновлено ФСТЭК России (территориальным органом ФСТЭК России) в случаях, предусмотренных пунктом 38 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77. Общество может возобновить эксплуатацию ИС со дня получения уведомления о возобновлении действия аттестата соответствия.

7.20. Действие аттестата соответствия может быть прекращено ФСТЭК России (территориальным органом ФСТЭК России) в случаях, предусмотренных пунктом 40 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей

государственную тайну, утвержденного приказом ФСТЭК России от 29 апреля 2021 г. № 77. Общество прекращает эксплуатацию ИС со дня получения уведомления о прекращении действия аттестата соответствия, если действие аттестата соответствия ранее не было приостановлено.

7.21. В случае утраты аттестата соответствия Обществом вправе обратиться в орган по аттестации с заявлением о выдаче дубликата аттестата соответствия. Дубликат аттестата соответствия выдается органом по аттестации с пометкой «Дубликат, оригинал аттестата соответствия признается недействующим».

8. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

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

– планирование и контроль мероприятий по защите информации в ИС;

– планирование мероприятий по проведению внутренних проверок режима обработки и защиты ПДн в Обществе;

– анализ угроз безопасности информации в ИС;

– управление (администрирование) СЗИ;

– выявление инцидентов и реагирование на них;

– управление конфигурацией ИС и ее СЗИ;

– информирование и обучение персонала ИС;

– контроль за обеспечением уровня защищенности информации, содержащейся в ИС.

8.2. В ходе планирования мероприятий по защите информации в ИС осуществляется:

– определение лиц, ответственных за планирование и контроль мероприятий по защите информации в ИС;

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

– разработка, утверждение и актуализация плана мероприятий по защите информации в ИС;

– определение порядка контроля выполнения мероприятий по защите информации в ИС, предусмотренных утвержденным планом.

Планирование мероприятий по защите информации в ИС и контроль выполнения мероприятий должны осуществляться в соответствии с порядком планирования мероприятий по защите информации в ИС (Общество «Общество врачей Российской Федерации») и контроля их выполнения, разработанным в рамках внедрения СЗИ ИС.

8.3. В ходе планирования мероприятий по проведению внутренних проверок режима обработки и защиты ПДн осуществляется:

– определение лиц, ответственных за осуществление внутреннего контроля соответствия обработки ПДн в Обществе «Общество врачей Российской Федерации» требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

– утверждение правил осуществления внутреннего контроля соответствия обработки ПДн требованиям, установленным Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами;

– утверждение на год приказом президента Общества «Общество врачей Российской Федерации» плана проведения внутренних проверок режима обработки и защиты ПДн.

8.4. В ходе анализа угроз безопасности информации в ИС осуществляется:

– выявление, анализ и устранение уязвимостей ИС;

– анализ изменения угроз безопасности информации в ИС;

– оценка возможных последствий реализации угроз безопасности информации в ИС.

Периодичность проведения указанных мероприятий на планируемый период (год) определяется ежегодным планом мероприятий по защите информации.

8.5. В ходе управления (администрирования) СЗИ осуществляются:

– определение лиц, ответственных за управление (администрирование) СЗИ ИС;

– управление учетными записями пользователей ИС и поддержание в актуальном состоянии правил разграничения доступа в ИС;

– управление средствами защиты информации в ИС;

– управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС;

– централизованное управление СЗИ ИС (при необходимости);

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

– обеспечение функционирования СЗИ ИС в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

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

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

– 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.

8.7. В ходе управления конфигурацией ИС и ее СЗИ осуществляются:

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

– определение компонентов ИС и ее СЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

– управление изменениями ИС и ее СЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на защиту информации, санкционирование внесения изменений в ИС и ее СЗИ, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации ИС;

– контроль действий по внесению изменений в ИС и ее СЗИ.

8.8. В ходе информирования и обучения персонала ИС осуществляется:

– информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС;

– доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

– обучение персонала ИС правилам эксплуатации отдельных средств защиты информации;

– проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты;

– контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала ИС по вопросам обеспечения защиты информации.

Периодичность проведения указанных мероприятий на планируемый период (год) определяется ежегодным планом мероприятий по защите информации.

8.9. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

– контроль (анализ) защищенности информации с учетом особенностей функционирования ИС;

– анализ и оценка функционирования ИС и ее СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ ИС;

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

– принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки (модернизации) ее СЗИ.

Мероприятия по контролю за обеспечением уровня защищенности информации на аттестованной ИС включаются в ежегодный план мероприятий по защите информации.

Контроль за обеспечением уровня защищенности информации на аттестованной ИС проводится Обществом самостоятельно или с привлечением организации, имеющей

лицензию на осуществление деятельности по технической защите конфиденциальной информации, выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

По результатам контроля за обеспечением уровня защищенности информации на аттестованной ИС оформляется протокол и вносится отметка в технический паспорт на ИС. Протоколы контроля защиты информации на аттестованном объекте информатизации не реже одного раза в два года представляются Обществом во ФСТЭК России (территориальный орган ФСТЭК России).

Непредставление протоколов контроля защиты информации во ФСТЭК России (территориальный орган ФСТЭК России) является основанием для приостановления действия аттестата соответствия на ИС.

8.10. В случае развития (модернизации) ИС, в ходе которого изменена конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключены программные, программно-технические средства и средства защиты информации, дополнительно включены аналогичные средства или заменены на аналогичные средства, проводятся дополнительные аттестационные испытания органом по аттестации в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77. Сведения об изменениях аттестованной ИС и проведенных при этом аттестационных испытаниях включаются Обществом в технический паспорт. Действие аттестата соответствия не прекращается.

8.11. В случае развития (модернизации) ИС, приводящего к повышению класса защищенности (уровня защищенности, категории значимости) ИС и (или) к изменению архитектуры СЗИ ИС в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры СЗИ, состава и мест расположения объекта информации и его компонентов, проводится повторная аттестация в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77.

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 Обществом 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 Общества.

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.