



ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности
защищаемой информации при её обработке в информационных системах
ГБПОУ Республики Марий Эл «УОР»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности защищаемой информации при её обработке в информационных системах ГБПОУ Республики Марий Эл «УОР» (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», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Положения – установление порядка организации и проведения работ по обеспечению безопасности защищаемой информации (далее – защищаемая информация, информация), в информационных системах (далее – ИС) ГБПОУ Республики Марий Эл «УОР» (далее – Учреждение) на всех стадиях (этапах) создания ИС, в ходе её эксплуатации и вывода из эксплуатации.

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

– персональные данные, содержащиеся в информационных системах персональных данных 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 её 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 её 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 её 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, приёма 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 её 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 её 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 защищённости 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 её 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 учётом актуальных угроз безопасности защищаемой информации, уровня защищённости персональных данных (далее – ПДн), который необходимо обеспечить, класса защищённости государственной информационной системы (далее – ГИС) и информационных технологий, используемых в ИС.

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

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

3.5. Учреждением назначается лицо, ответственное за организацию обработки персональных данных при их обработке в ГБПОУ Республики Марий Эл «УОР».

3.6. Для обеспечения безопасности защищаемой информации, содержащейся в ИС, Учреждением назначается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности персональных данных и за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах ГБПОУ Республики Марий Эл «УОР» (далее – Ответственный).

3.7. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации ИС Учреждением 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. 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 статьёй 5 Федерального закона от 27 декабря 2002 г. № 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) её создания, в ходе эксплуатации и вывода из эксплуатации путём принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в ИС, 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. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ УЧРЕЖДЕНИЯ

4.1. Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в ИС Учреждения.

4.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

4.3. Резервному копированию подлежит информация, обрабатываемая в ИС Учреждения.

4.4. В Учреждении должна быть реализована централизованная система резервного копирования.

4.5. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

4.6. Перед выполнением процедур резервного копирования или восстановления информации и программного обеспечения средств защиты необходимо провести проверку:

- доступности резервного носителя, достаточности свободного места в хранилище для записи или восстановления данных;
- работоспособности средств резервного копирования и восстановления;
- готовности информационных ресурсов к осуществлению их резервного копирования или восстановления;
- завершения работы ПО и процессов, способных повлиять на процесс создания или восстановления копий.

4.7. Расписание проведения резервного копирования определяется Ответственным.

4.8. Резервное копирование проводится Ответственным и регистрируется в Журнале резервного копирования и восстановления информации (ПРИЛОЖЕНИЕ № 1).

4.9. Перечень информационных ресурсов, подлежащих резервному копированию, время и дата создания копии, пометки об успешном/неуспешном завершении, а также, при необходимости, комментарии Ответственного заносятся в Журнал резервного копирования и восстановления информации.

4.10. В случае выявления нарушений Ответственному необходимо в кратчайшие сроки устранить неисправности в системе резервного копирования и восстановить работоспособность подсистем в штатный режим работы.

4.11. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, Ответственный сообщает руководству Учреждения немедленно.

4.12. Ответственный должен контролировать проведение резервного копирования в целях выполнения требований по защите информации.

4.13. В случае обнаружения ошибки резервного копирования Ответственный выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями Учреждения, в Журнал резервного копирования и восстановления информации заносятся соответствующие отметки.

4.14. Хранение резервных копий данных осуществляется на сменных носителях информации (CD/DVD, внешние жёсткие диски и т.п.), промаркированных Ответственным в соответствии с расписанием резервного копирования. Маркировка должна содержать номер копии, дату её создания, наименование ИС.

4.15. Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

4.16. Срок хранения резервных копий определяется Ответственным.

4.17. Очистка устаревших резервных копий из хранилища должна производиться Ответственным регулярно по мере заполнения выделенной области памяти или по истечении предусмотренного срока хранения.

4.18. Удаление резервных копий для повторного использования носителя информации либо окончательное удаление производится Ответственным.

4.19. Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоя оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится Ответственным.

4.20. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

4.21. В зависимости от характера и уровня повреждения информационных ресурсов, Ответственный восстанавливает либо весь

архив копии данных, либо отдельные потерянные части или технические средства из соответствующих хранилищ.

4.22. После завершения процесса восстановления Ответственным проверяется целостность информационных ресурсов и корректная работа технических средств ИС, также заполняются соответствующие поля в Журнале резервного копирования и восстановления информации.

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

5.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется Учреждением.

5.2. 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 защищённости 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.

5.3. 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.

5.4. Результаты классификации ИС оформляются актом классификации.

5.5. Результаты определения уровня защищённости ПДн при их обработке в ИС оформляются актом определения уровня защищённости.

5.6. 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).

5.7. В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности

информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

5.8. 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 её отдельных сегментах, а также иные характеристики ИС, применяемые информационные технологии и особенности её функционирования.

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

5.10. Модель угроз безопасности информации должна содержать описание ИС и её 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.

5.11. Требования к СЗИ определяются в зависимости от класса защищённости ИС, уровня защищённости ПДн при их обработке в ИС и угроз безопасности информации, включённых в модель угроз безопасности информации.

5.12. При определении требований к СЗИ учитываются положения политики Учреждения в отношении обработки защищаемой информации.

6. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Разработка СЗИ организуется Учреждением.

6.2. 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).

6.3. СЗИ не должна препятствовать достижению целей создания ИС и её функционированию.

6.4. При разработке СЗИ учитывается её информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

6.5. 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 её элементов;

- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учётом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищённости ИС, уровня защищённости 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.

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

6.7. 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) её СЗИ с учётом функциональных возможностей имеющихся сертифицированных средств защиты информации.

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

6.9. 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.

6.10.Макетирование СЗИ и её тестирование может проводиться в том числе с использованием средств и методов моделирования ИС и технологий виртуализации.

7. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Внедрение СЗИ организуется Учреждением.

7.2. 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 Учреждением для обеспечения защиты информации в ИС в ходе её 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;

- приёмочные испытания СЗИ (при необходимости).

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

7.4. 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 защищённости информации, содержащейся в ИС;

- информирования и обучения персонала ИС;
- защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации.

7.5. 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.

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

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

7.8. 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 учётом 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.

7.9. Приёмочные испытания СЗИ включают проверку выполнения требований к СЗИ в соответствии с техническим заданием на создание СЗИ.

8. АТТЕСТАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

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

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

8.3. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, акт определения уровня защищённости 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 приёмочных испытаний СЗИ (при наличии).

8.4. Аттестация ИС проводится в соответствии с программой и методиками аттестационных испытаний. Для проведения аттестации ИС применяются национальные стандарты, а также методические документы, разработанные и утверждённые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утверждённого Указом Президента Российской Федерации от 16 августа 2004 г. № 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.

8.5. При проведении аттестационных испытаний должны применяться 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 путём осуществления попыток несанкционированного доступа (воздействия) к ИС в обход её СЗИ.

8.6. 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 защищённости, уровни защищённости, уровни важности, угрозы безопасности информации, реализованы одинаковые проектные решения по ИС и её СЗИ. В сегментах ИС, на которые распространяется аттестат соответствия, Учреждением обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно-распорядительных документов по защите информации.

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

8.8. Повторная аттестация ИС осуществляется по окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищённости ИС. При увеличении состава угроз безопасности информации или изменении проектных решений, реализованных при создании СЗИ, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

9. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

9.1. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется Учреждением 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;
- анализ угроз безопасности информации в ИС;
- управление (администрирование) СЗИ;
- выявление инцидентов и реагирование на них;
- управление конфигурацией ИС и её СЗИ;
- информирование и обучение персонала ИС;
- контроль за обеспечением уровня защищённости информации, содержащейся в ИС.

9.2. 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 утверждённым 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 и контроля их выполнения, разработанным в рамках внедрения СЗИ ИС.

9.3. 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 работ определена в Плате мероприятий по защите информации (ПРИЛОЖЕНИЕ № 2) и в Плате внутренних проверок режима защиты информации (ПРИЛОЖЕНИЕ № 3).

9.4. В ходе управления (администрирования) СЗИ осуществляются:

- определение лиц, ответственных за управление (администрирование) СЗИ ИС;
- управление учётными 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 учётом 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 её эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

9.5. 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 её 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.

9.6. В ходе управления конфигурацией ИС и её СЗИ осуществляются:

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

- определение компонентов ИС и её 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 её СЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на защиту информации, санкционирование внесения изменений в ИС и её СЗИ, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации ИС;

- контроль действий по внесению изменений в ИС и её СЗИ.

9.7. 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 учётом внесённых 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 осведомлённости персонала ИС об угрозах

безопасности информации и уровня знаний персонала ИС по вопросам обеспечения защиты информации.

Периодичность проведения указанных работ определена в Плане мероприятий по защите информации и в Плане внутренних проверок режима защиты информации.

9.8. В ходе контроля за обеспечением уровня защищённости информации, содержащейся в ИС, осуществляются:

- контроль (анализ) защищённости информации с учётом особенностей функционирования ИС;
- анализ и оценка функционирования ИС и её СЗИ, включая анализ и устранение уязвимостей и иных недостатков в функционировании СЗИ ИС;
- документирование процедур и результатов контроля за обеспечением уровня защищённости информации, содержащейся в ИС;
- принятие решения по результатам контроля за обеспечением уровня защищённости информации, содержащейся в ИС, о необходимости доработки (модернизации) её СЗИ.

9.9. Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с Планом мероприятий по защите информации. Внутренние проверки режима защиты информации проводятся в соответствии с Планом внутренних проверок режима защиты информации. По результатам проведения внутренней проверки составляется Отчёт о результатах внутренней проверки режима защиты информации в ГБПОУ Республики Марий Эл «УОР» (ПРИЛОЖЕНИЕ № 4).

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

10.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации осуществляется Учреждением 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.

10.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности Учреждения.

10.3. 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.

к Положению по организации и
проведению работ по
обеспечению безопасности
защищаемой информации при её
обработке в информационных
системах ГБПОУ Республики
Марий Эл «УОР»
от «26» августа 2024 г.

ОТ «ДБ» августа 2004 г.

[illegible]

ПРИЛОЖЕНИЕ № 2

к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации при её обработке в информационных системах ГБПОУ Республики Марий Эл «УОР»
от «16» августа 2021 г.

ПЛАН мероприятий по обеспечению безопасности защищаемой информации в ГБПОУ Республики Марий Эл «УОР»

№ 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 «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 содержанием собственноручную подпись субъекта ПДн согласно 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

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
			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 Учреждения к защищаемой информации
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учёта передачи ПДн, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6.	Ведение журналов учёта 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 одного раза в три года, повышение осведомлённости сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности персональных данных и за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Учреждения)
8.	Инвентаризация информационных ресурсов	Один 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 Учреждением устанавливаются сроки обработки, которые документально подтверждаются в локальных актах Учреждения. При пересмотре сроков необходимых изменений вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных)	При	Уничтожение электронных (бумажных) носителей информации

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
	носителей информации при достижении целей обработки защищаемой информации	необходимости	при достижении целей обработки защищаемой информации производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению защищаемой информации, не содержащей сведения, составляющие государственную тайну»
11.	Определение класса защищённости ИС	При необходимости	Определение класса защищённости ИС осуществляется при создании ИС, при изменении состава ИС, масштаба ИС, степеней ущерба для характеристик ИС (конфиденциальности, целостности, доступности)
12.	Определение уровня защищённости ПДн при их обработке в ИС	При необходимости	Определение уровня защищённости ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объёма 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	
16.	Анализ угроз безопасности в информационной системе	При необходимости	В рамках данного мероприятия проводится: – выявление, анализ и устранение уязвимостей или принятие мер по предотвращению возможности эксплуатации выявленных уязвимостей; – анализ изменения угроз безопасности информации в информационных системах; – оценка возможных последствий реализации угроз безопасности информации.

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
			По результатам разрабатывается/корректируется модель нарушителей и угроз безопасности информации. При проведении работ необходимо руководствоваться действующими нормативно-методическими документами в области защиты информации
17.	Обновление программного обеспечения (в том числе средств защиты информации)	При необходимости	Получение обновлений производится из доверенных источников
18.	Информирование персонала информационных систем о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационных систем	Постоянно	-
19.	Доведение до персонала информационных систем требований по защите информации, а также положений организационно-распорядительных документов по защите информации	При необходимости	-
20.	Обучение персонала информационных систем правилам эксплуатации отдельных средств защиты информации	Постоянно	Мероприятие проводится при: – вводе средств защиты информации в эксплуатацию; – изменении правил эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией; – изменении пользователей средств защиты информации; – по запросу пользователей, но не реже одного раза в два года
21.	Проведение практических занятий и тренировок с персоналом информационных систем по блокированию угроз безопасности информации и реагированию	Постоянно	Мероприятие проводится не реже одного раза в два года

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
22.	на инциденты Контроль за обеспечением уровня защищённости информации, содержащейся в информационных системах	Постоянно	Проводится ГБПОУ Республики Марий Эл «УОР» самостоятельно или с привлечением организации, имеющей лицензию на деятельность по технической защите информации, для: – информационных систем с установленным 2 или 3 классом защищённости не реже одного раза в два года; – для информационных систем с установленным 1 классом защищённости не реже одного раза в год. Процедура контроля и результаты должны быть задокументированы

ПРИЛОЖЕНИЕ № 3

к Положению по организации и проведению работ по обеспечению безопасности защищаемой информации при её обработке в информационных системах ГБПОУ Республики Марий Эл «УОР»
от «ав» августа 20ав г.

План внутренних проверок режима защиты информации в ГБПОУ Республики Марий Эл «УОР»

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в полгода	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
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 ГБПОУ Республики Марий Эл «УОР» по вопросам обработки ПДн;	Раз в полгода	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
	- Разъяснения субъекту ПДн юридических последствий отказа предоставить свой ПДн		
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учёту обращений субъектов ПДн и учёту 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	Раз в полгода	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику ГБПОУ Республики Марий Эл «УОР» в отношении обработки ПДн	Раз в полгода	
11.	Организация анализа и пересмотра имеющихся угроз безопасности информации, а также предсказание появления новых, ещё неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинён субъектам ПДн в случае нарушения ФЗ-152 «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 учёта машинных носителей информации	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности информации, класса защищённости ИС и уровня защищённости ПДн в ИС	Раз в полгода	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИС	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты информации	Раз в полгода	
22.	Контроль выполнения мероприятий, предусмотренных планом(ами) мероприятий по защите информации	Ежемесячно	
23.	Контроль осведомлённости персонала информационной системы об угрозах безопасности информации	Раз в полгода	
24.	Контроль уровня знаний персонала по вопросам обеспечения защиты информации	Ежегодно	

ПРИЛОЖЕНИЕ № 4
к Положению по организации и
проведению работ по обеспечению
безопасности защищаемой
информации при её обработке в
информационных системах
ГБПОУ Республики Марий Эл
«УОР»
от «26» августа 2021 г.

ОТЧЁТ
о результатах внутренней проверки режима защиты информации в
ГБПОУ Республики Марий Эл «УОР»

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 её обработке в информационных системах ГБПОУ Республики Марий Эл «УОР»
от «__» _____ 20__ г.

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:

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

1.5 Необходимые мероприятия.

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

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

Подписи ответственных лиц, проводивших внутреннюю проверку режима защиты информации:

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