Приложение 2
к приказу управления финансов Липецкой области «О назначении ответственного за защиту информации, утверждении инструкции по защите информации, положения по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в государственной информационной системе «Электронный бюджет Липецкой области»»
от «___» _____20__г. № ____

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в государственной информационной системе «Электронный бюджет Липецкой области»

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 государственной информационной системе «Электронный бюджет Липецкой области» (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, информация), в государственной информационной системе «Электронный бюджет Липецкой области» (далее – ГИС) управления финансов Липецкой области (далее – управление финансов области) на всех стадиях (этапах) создания ГИС, в ходе ее эксплуатации и вывода из эксплуатации.

1.3. К защищаемой информации, обрабатываемой в ГИС управления финансов области, относится следующая информация:

– персональные данные, содержащиеся в информационной системе персональных данных управления финансов области;

– информация, не содержащая сведения, составляющие государственную тайну, содержащаяся в государственной информационной системе «Электронный бюджет Липецкой области».

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 ГИС 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 ГИС и информационных технологий, используемых в ГИС.

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

3.4. Защита информации, содержащейся в ГИС, обеспечивается путем выполнения управлением финансов области требований к организации защиты информации, содержащейся в ГИС, и требований к мерам защиты информации, содержащейся в ГИС.

3.5. Управлением финансов области назначается лицо, ответственное за организацию обработки персональных данных при их обработке в управлении финансов Липецкой области.

3.6. Для обеспечения безопасности защищаемой информации, содержащейся в ГИС, управлением финансов области назначается структурное подразделение или должностное лицо (работник), ответственное за защиту информации, не содержащей сведения, составляющие государственную тайну, в государственной информационной системе «Электронный бюджет Липецкой области» (далее – Ответственный).

3.7. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации ГИС управлением финансов области 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 ГИС, 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».

3.9. Защита информации, содержащейся в ГИС, является составной частью работ по созданию и эксплуатации ГИС 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 ГИС, 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 ГИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в ГИС;

– разработка СЗИ;

– внедрение СЗИ;

– аттестация ГИС по требованиям защиты информации (далее – аттестация ГИС);

– обеспечение защиты информации в ходе эксплуатации аттестованной ГИС;

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

4. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЭЛЕКТРОННЫЙ БЮДЖЕТ ЛИПЕЦКОЙ ОБЛАСТИ»

4.1. Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в ГИС управления финансов области.

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 ГИС управления финансов области.

4.4. В управлении финансов области 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 управления финансов области 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 управления финансов области, в Журнал резервного копирования и восстановления информации заносятся соответствующие отметки.

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

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 сбоев

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 ГИС, также заполняются соответствующие поля в Журнале резервного копирования и восстановления информации.

5. ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЭЛЕКТРОННЫЙ БЮДЖЕТ ЛИПЕЦКОЙ ОБЛАСТИ»

5.1. Формирование требований к защите информации, содержащейся в ГИС, осуществляется управлением финансов области.

5.2. Формирование требований к защите информации, содержащейся в ГИС, включает:

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

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

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

– определение требований к СЗИ.

5.3. При принятии решения о необходимости защиты информации, содержащейся в ГИС, осуществляется:

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

– определение информации, подлежащей обработке в ГИС;

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

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

5.4. Результаты классификации ГИС оформляются актом классификации.

5.5. Результаты определения уровня защищенности ПДн при их обработке в ГИС оформляются актом определения уровня защищенности.

5.6. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ГИС, 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 ГИС, включающие структуру и состав ГИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ГИС, с иными ГИС и информационно-телекоммуникационными сетями, режимы обработки информации в ГИС и в ее отдельных сегментах, а также иные характеристики ГИС, применяемые информационные технологии и особенности ее функционирования.

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

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

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

5.12.При определении требований к СЗИ учитываются положения политики управления финансов области в отношении обработки персональных данных.

6. РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Разработка СЗИ организуется управлением финансов области.

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 ГИС и ее функционированию.

6.4. При разработке СЗИ учитывается ее информационное взаимодействие с иными ГИС 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 ГИС;

– 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 ГИС, уровня защищенности ПДн при их обработке в ГИС;

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

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

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

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 ГИС и (или) ее СЗИ с учетом 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 ее тестирование может проводиться в том числе с использованием средств и методов моделирования ГИС и технологий виртуализации.

7. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Внедрение СЗИ организуется управлением финансов области.

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 ГИС;

– разработку документов, определяющих правила и процедуры, реализуемые управлением финансов области для обеспечения защиты информации в ГИС 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 ГИС и принятие мер защиты информации по их устранению;

– приемочные испытания СЗИ (при необходимости).

7.3. Установка и настройка средств защиты информации в ГИС 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 ГИС;

– управления (администрирования) СЗИ;

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

– управления конфигурацией аттестованной ГИС и СЗИ;

– контроля за обеспечением уровня защищенности информации, содержащейся в ГИС;

– информирования и обучения персонала ГИС;

– защиты информации при выводе из эксплуатации ГИС 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 ГИС 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 ГИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации угроз безопасности информации. Анализ уязвимостей ГИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ГИС. При анализе уязвимостей ГИС 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 ГИС, 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 ГИС отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

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

8. АТТЕСТАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

8.1. Аттестация ГИС организуется управлением финансов области 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 ГИС должностными лицами, осуществляющими проектирование и (или) внедрение СЗИ ГИС, не допускается.

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

8.4. Аттестация ГИС проводится в соответствии с программой и методиками аттестационных испытаний. Для проведения аттестации ГИС применяются национальные стандарты, а также методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии (не соответствии) ГИС 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 ГИС установленным требованиям по защите информации на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования ГИС;

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

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

8.6. Допускается аттестация ГИС на основе результатов аттестационных испытаний выделенного набора сегментов ГИС, реализующих полную технологию обработки информации. В этом случае распространение аттестата соответствия на другие сегменты ГИС осуществляется при условии их соответствия сегментам ГИС, прошедшим аттестационные испытания. Сегмент считается соответствующим сегменту ГИС, 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 ГИС и ее СЗИ. В сегментах ГИС, на которые распространяется аттестат соответствия, управлением финансов области обеспечивается соблюдение эксплуатационной документации на СЗИ и организационно-распорядительных документов по защите информации.

8.7. Особенности аттестации ГИС на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также

условия и порядок распространения аттестата соответствия на другие сегменты ГИС определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

8.8. Повторная аттестация ГИС осуществляется по окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищенности ГИС. 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 ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «ЭЛЕКТРОННЫЙ БЮДЖЕТ ЛИПЕЦКОЙ ОБЛАСТИ»

9.1. Обеспечение защиты информации в ходе эксплуатации аттестованной ГИС осуществляется управлением финансов области 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 ГИС;

– анализ угроз безопасности информации в ГИС;

– управление (администрирование) СЗИ;

– выявление инцидентов и реагирование на них;

– управление конфигурацией ГИС и ее СЗИ;

– информирование и обучение персонала ГИС;

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

9.2. В ходе планирования мероприятий по защите информации в ГИС осуществляется:

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

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

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

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

Планирование мероприятий по защите информации в ГИС и контроль выполнения мероприятий должны осуществляться в соответствии с порядком планирования мероприятий по защите информации в ГИС и контроля их выполнения, разработанным в рамках внедрения СЗИ ГИС.

9.3. В ходе анализа угроз безопасности информации в ГИС осуществляется:

– выявление, анализ и устранение уязвимостей ГИС;

– анализ изменения угроз безопасности информации в ГИС;

– оценка возможных последствий реализации угроз безопасности информации в ГИС.

Периодичность проведения указанных работ определена в Плане мероприятий по защите информации (Приложение 2) и в Плане внутренних проверок режима защиты информации (Приложение 3).

9.4. В ходе управления (администрирования) СЗИ осуществляются:

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

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

– управление средствами защиты информации в ГИС;

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

– централизованное управление СЗИ ГИС (при необходимости);

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

– обеспечение функционирования СЗИ ГИС в ходе ее 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 ГИС и администраторами ГИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ГИС;

– 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 ГИС 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.

9.6. В ходе управления конфигурацией ГИС и ее СЗИ осуществляются:

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

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

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

9.7. В ходе информирования и обучения персонала ГИС осуществляется:

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

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

– обучение персонала ГИС правилам эксплуатации отдельных средств защиты информации;

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

– контроль осведомленности персонала ГИС об угрозах безопасности информации и уровня знаний персонала ГИС 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 защищенности информации, содержащейся в ГИС, осуществляются:

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

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

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

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

Отчет о результатах внутренней проверки режима защиты информации в управлении финансов Липецкой области (Приложение 4).

10. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИЗ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЭЛЕКТРОННЫЙ БЮДЖЕТ ЛИПЕЦКОЙ ОБЛАСТИ» ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ ИНФОРМАЦИИ

10.1.Обеспечение защиты информации при выводе из эксплуатации аттестованной ГИС или после принятия решения об окончании обработки информации осуществляется управлением финансов области в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и в том числе включает:

– архивирование информации, содержащейся в ГИС;

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

10.2.Архивирование информации, содержащейся в ГИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности управления финансов области.

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

Приложение 1
к Положению по организации и
проведению работ по обеспечению
безопасности защищаемой информации, не
содержащей сведения, составляющие
государственную тайну, при ее обработке в
государственной информационной системе
«Электронный бюджет Липецкой области»
от «__» _____20__г.

Журнал резервного копирования/восстановления данных

№ п/п	Схема резервного копирования/восстановления данных	Копируемые/восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/восстановления	Фамилия ответственного	Подпись ответственного	Результат резервного копирования/восстановления данных	Комментарий
1	2	3	4	5	6	7	8	9

Приложение 2
к Положению по организации и проведению
работ по обеспечению безопасности
защищаемой информации, не содержащей
сведения, составляющие государственную
тайну, при ее обработке в государственной
информационной системе «Электронный
бюджет Липецкой области»
от «__» _____20__г.

План мероприятий по обеспечению безопасности защищаемой информации в управлении финансов Липецкой области

№ 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 содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
			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 управления финансов области к защищаемой информации
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи ПДн, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
6.	Ведение журналов учета машинных носителей защищаемой информации, средств защиты информации	Постоянно	-
7.	Повышение квалификации сотрудников в области защиты информации	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах управления финансов области)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия защищаемой информации
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн управлением финансов области устанавливаются сроки обработки, которые документально

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
			подтверждаются в локальных актах управления финансов области. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению защищаемой информации, не содержащей сведения, составляющие государственную тайну»
11.	Определение класса защищенности ИС	При необходимости	Определение класса защищенности ИС осуществляется при создании ИС, при изменении состава ИС, масштаба ИС, степеней ущерба для характеристик ИС (конфиденциальности, целостности, доступности)
12.	Определение уровня защищенности ПДн при их обработке в ИС	При необходимости	Определение уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
13.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании СЗИ
14.	Аттестация ИС на соответствие требованиям по обеспечению безопасности информации	При необходимости	-
15.	Эксплуатация ИС и контроль безопасности защищаемой информации	Постоянно	

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
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. 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	-

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
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 на инциденты	Постоянно	Мероприятие проводится не реже одного раза в два года

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
22.	Контроль за обеспечением уровня защищенности информации, содержащейся в информационных системах	Постоянно	Проводится управлением финансов Липецкой области самостоятельно или с привлечением организации, имеющей лицензию на деятельность по технической защите информации, для: – информационных систем с установленным 2 или 3 классом защищенности не реже одного раза в два года; – для информационных систем с установленным 1 классом защищенности 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, не содержащей
сведения, составляющие государственную
тайну, при ее обработке в государственной
информационной системе «Электронный
бюджет Липецкой области»
от «__» _____20__г.

План внутренних проверок режима защиты информации в управлении финансов Липецкой области

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Организация анализа и пересмотра имеющихся угроз безопасности информации, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
2.	Проверка применения для обеспечения безопасности информации средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
3.	Контроль учета машинных носителей информации	Раз в полгода	
4.	Контроль за принимаемыми мерами по обеспечению безопасности информации, класса защищенности ИС и уровня защищенности ПДн в ИС	Раз в полгода	
5.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС	Ежеквартально	
6.	Контроль внесения изменений в структурно-функциональные характеристики ИС	Ежеквартально	
7.	Контроль корректности настроек средств защиты информации	Раз в полгода	
8.	Контроль за обеспечением резервного копирования	Ежеквартально	
9.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты информации	Раз в полгода	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
10.	Контроль выполнения мероприятий, предусмотренных планом(ами) мероприятий по защите информации	Ежемесячно	
11.	Контроль осведомленности персонала информационной системы об угрозах безопасности информации	Раз в полгода	
12.	Контроль уровня знаний персонала по вопросам обеспечения защиты информации	Ежегодно	

Приложение 4
к Положению по организации и проведению
работ по обеспечению безопасности
защищаемой информации, не содержащей
сведения, составляющие государственную
тайну, при ее обработке в государственной
информационной системе «Электронный
бюджет Липецкой области»
от «__» _____20__г.

Отчет о результатах внутренней проверки режима защиты информации в управлении финансов Липецкой области

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах управления финансов Липецкой области 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)