Приложение 4

УТВЕРЖДЕНО
приказом директора
МБОУ СОШ № 7 г. Ставрополя
от_____ № _____

ПОЛОЖЕНИЕ

Об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах МБОУ СОШ № 7 г. Ставрополя

I. Общие положения

1. Настоящее Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах МБОУ СОШ № 7 г. Ставрополя (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Государственной технической комиссии при Президенте Российской Федерации от 30.08.2002 № 282, в целях реализации требований нормативных документов ФСБ России, ФСТЭК России.

2. Целями принятия настоящего Положения являются:

– обеспечение защиты прав и свобод физических лиц при обработке МБОУ СОШ № 7 г. Ставрополя их персональных данных;

– соблюдение требований законодательства Российской Федерации в области обеспечения безопасности персональных данных;

– предотвращение разглашения, утечки, неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении персональных данных, обрабатываемых в информационных системах МБОУ СОШ № 7 г. Ставрополя.

3. Настоящее Положение определяет порядок обеспечения безопасности персональных данных, обрабатываемых в информационных системах МБОУ СОШ № 7 г. Ставрополя, и устанавливает:

– цели и принципы построения системы защиты персональных данных;

– порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах МБОУ СОШ № 7 г. Ставрополя;

– методы и способы защиты информации в информационных системах МБОУ СОШ № 7 г. Ставрополя.

4. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, утечки персональных данных и специальных воздействий на них, результатом которых может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также путем исключения иных несанкционированных действий в отношении персональных данных.

5. Безопасность персональных данных должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования информационных систем.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию таких информационных систем.

6. Задача обеспечения безопасности персональных данных при их обработке в информационных системах должна решаться путем создания комплексной системы защиты персональных данных.

7. Настоящее Положение является основой для:

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

– выработки комплекса мер нормативно-правового, технического и организационного характера, направленных на выявление и предотвращение угроз безопасности персональных данных;

– координации деятельности структурных подразделений МБОУ СОШ № 7 г. Ставрополя при проведении работ по созданию, развитию и эксплуатации информационных систем с соблюдением требований по обеспечению безопасности персональных данных;

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

8. Действие настоящего Положения распространяется на всех работников МБОУ СОШ № 7 г. Ставрополя, которые в рамках своих должностных обязанностей осуществляют автоматизированную обработку персональных данных, а также на работников, осуществляющих сопровождение и

обслуживание информационных систем, и работников, обеспечивающих безопасность обрабатываемой в таких системах информации.

9. Планирование, координация и контроль проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах МБОУ СОШ № 7 г. Ставрополя осуществляется постоянно действующей комиссией по технической защите конфиденциальной информации в МБОУ СОШ № 7 г. Ставрополя (далее – Комиссия).

10. Контроль за соблюдением МБОУ СОШ № 7 г. Ставрополя и его работниками требований к защите персональных данных, установленных законодательством Российской Федерации, осуществляется ответственным за организацию обработки персональных данных в МБОУ СОШ № 7 г. Ставрополя.

11. Непосредственное проведение работ по обеспечению безопасности персональных данных, обрабатываемых в информационных системах МБОУ СОШ № 7 г. Ставрополя, по сопровождению средств защиты информации и контролю за работой пользователей информационных систем возлагается на администратора безопасности информации (далее – Администратор).

II. Основные термины и определения

Для целей настоящего Положения используются следующие термины и определения:

информационная система (далее – ИС) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

пользователь ИС – лицо, участвующее в функционировании ИС или использующее результаты ее функционирования. Пользователем ИС является любой работник МБОУ СОШ № 7 г. Ставрополя, имеющий доступ к ИС и ее ресурсам в соответствии с его функциональными обязанностями и установленным порядком;

безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в ИС;

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

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

уязвимость ИС – свойство ИС, обуславливающее возможность реализации угроз безопасности, обрабатываемых в ней персональных данных;

нарушитель – физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИС;

модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности;

модель угроз безопасности персональных данных – физическое, математическое, описательное представление свойств или характеристик угроз безопасности персональных данных;

несанкционированный доступ (несанкционированные действия) (далее – НСД) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств;

инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

система защиты информационных систем (далее – СЗИС) – совокупность правовых, организационных и технических мероприятий для защиты информационных систем от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними;

средство защиты информации (далее – СЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (персональных данных);

политика безопасности информации в организации – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

III. Цели и принципы построения системы защиты персональных данных

1. СЗИС является частью общей системы обеспечения информационной безопасности в МБОУ СОШ № 7 г. Ставрополя.

2. Основной целью создания СЗИС является организация непрерывного и защищенного процесса обработки персональных данных в МБОУ СОШ № 7 г.

Ставрополя и нейтрализация угроз безопасности персональных данных, возникающих посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИС или НСД к циркулирующей в ней информации и ее незаконного использования.

3. СЗИС должна обеспечивать:

– своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных;

– создание механизма оперативного реагирования на угрозы безопасности персональных данных;

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

4. Построение и функционирование СЗИС должно осуществляться в соответствии со следующими принципами:

1) законность. Предполагает осуществление защитных мероприятий и разработку СЗИС в соответствии с действующим законодательством в области персональных данных, стандартами и методическими документами по защите персональных данных;

2) системность. Системный подход к построению СЗИС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных;

3) комплексность. Комплексное использование методов и СЗИ предполагает согласованное применение разнородных средств при построении целостной СЗИС, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

4) непрерывность. Защита персональных данных должна обеспечиваться на всех технологических этапах обработки персональных данных и во всех режимах функционирования ИС, в том числе при проведении ремонтных и регламентных работ;

5) своевременность. Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на стадии разработки (модернизации) ИС в целом и ее системы защиты, в частности;

6) преемственность и совершенствование. Предполагают постоянное совершенствование мер и СЗИ на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее системы защиты с учетом изменений в методах и средствах перехвата

информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области;

7) разумная достаточность (экономическая целесообразность). Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от реализации угроз безопасности персональных данных;

8) персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого работника МБОУ СОШ № 7 г. Ставрополя в пределах его полномочий. В соответствии с этим принципом, распределение прав и обязанностей работников МБОУ СОШ № 7 г. Ставрополя строится таким образом, чтобы в случае любого нарушения круг виновных в нарушении лиц был четко известен или сведен к минимуму;

9) минимизация полномочий. Означает предоставление пользователям ИС прав доступа в соответствии с выполняемыми обязанностями, определенными должностными инструкциями;

10) гибкость системы защиты. Предполагает возможность варьирования уровнем защищенности;

11) простота применения средств защиты информации. Механизмы защиты должны быть интуитивно понятны и просты в использовании, без значительных дополнительных трудозатрат;

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

13) специализация и профессионализм. Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, имеющих опыт практической работы и лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация СЗИ должна осуществляться профессионально подготовленными работниками МБОУ СОШ № 7 г. Ставрополя;

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

IV. Проектирование системы защиты информационных систем

1. Проектирование СЗИС, выбор и реализация методов и способов защиты персональных данных при их обработке в ИС осуществляются на основании выявленных актуальных угроз безопасности персональных данных и в зависимости от класса ИС.

2. Выявление и оценка актуальности угроз безопасности персональных данных производится посредством разработки (актуализации) модели угроз безопасности персональных данных (далее – Модель угроз).

3. Методической базой для разработки Модели угроз являются следующие нормативные правовые акты:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах, утвержденная заместителем директора ФСТЭК России 15.02.2008;

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах, утвержденная заместителем директора ФСТЭК России 14.02.2008;

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144.

4. Модель угроз разрабатывается для каждой ИС МБОУ СОШ № 7 г. Ставрополя и должна содержать:

– описание структуры и состава ИС (состав обрабатываемых персональных данных, состав технических средств и программного обеспечения, существующие процессы обработки персональных данных, схему организации связи и т.п.), т.е. исходные данные по ИС;

– обоснование характеристик безопасности персональных данных (конфиденциальность, целостность, доступность и т.п.), нарушение которых ведет к ущербу для субъектов персональных данных;

– модель угроз (перечень угроз, оценку вероятностей угроз, показатели опасности угроз, оценки возможностей реализации угроз, выводы об актуальности угроз);

– модель нарушителя (объекты атак, возможные типы нарушителей, предположения о возможностях нарушителей, предположения об ограничениях на эти возможности, предположения о каналах атак и средствах атак, выводы о типе нарушителя).

5. Результатом разработки Модели угроз должен являться:

– перечень актуальных угроз;

– вывод о классе ИС;

– вывод о типе нарушителя, существующем в ИС, и требованиях к средствам криптографической защиты информации.

6. Классификация ИС проводится в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России

от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и является основой для определения методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

Классификация ИС проводится Комиссией на основании анализа исходных данных по ИС. Результаты классификации ИС оформляются соответствующим актом, утверждаемым директором МБОУ СОШ № 7 г. Ставрополя.

7. По результатам разработки Модели угроз, проведения классификации ИС и анализа исходных данных по ИС проектируется СЗИС: определяются конкретные методы и способы защиты персональных данных и осуществляется выбор СЗИ.

8. Выбранные и реализованные методы и способы защиты информации в ИС должны обеспечивать нейтрализацию предполагаемых актуальных угроз безопасности персональных данных при их обработке в ИС.

9. Оценка необходимости пересмотра класса ИС и Модели угроз должна осуществляться каждый раз, когда изменились характеристики, учитываемые при классификации ИС, характеристики, влияющие на актуальность угроз безопасности персональных данных и тип нарушителя.

10. При анализе исходных характеристик ИС, моделировании угроз, проектировании СЗИС и оценке уровня затрат на нее должна быть проведена оценка возможности оптимизации ИС.

Оценка возможности оптимизации ИС имеет своей целью такую реструктуризацию ИС, выполнение требований по защите персональных данных в которой может быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию СЗИС.

11. При проведении оптимизации ИС должна оцениваться возможность:

– снижения категории обрабатываемых персональных данных;

– обезличивания персональных данных;

– придания персональным данным статуса общедоступных;

– изменения структуры и состава технических и программных средств ИС, технологических процессов обработки персональных данных, в том числе, с целью:

1) уменьшения количества компонентов ИС, на которые потребуется установка СЗИ;

2) изменения вероятности и степени опасности угроз безопасности персональных данных и, соответственно, сокращения перечня актуальных угроз;

3) изменений требований к характеристикам СЗИ, в результате которых возможно использование более оптимальных по стоимости средств.

V. Состав системы защиты информационных систем

1. С позиций комплексного и системного подхода к построению СЗИС, такая система в общем случае должна включать в себя следующие функциональные подсистемы:

- управление доступом;
- регистрация и учет;
- обеспечение целостности;
- криптографическая защита;
- антивирусная защита;
- анализ защищенности;
- обеспечение безопасного межсетевого взаимодействия;
- обнаружение вторжений;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- обеспечение физической защиты.

2. Конкретный состав и функционал перечисленных подсистем (состав методов и способов защиты персональных данных) определяется в соответствии с разделом IV настоящего Положения на основании следующих нормативных правовых актов:

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

3. Порядок обеспечения безопасности персональных данных при их обработке в ИС в соответствии с функциональными подсистемами, определенными в пункте 28 настоящего Положения, детализируется в отдельных нормативных актах МБОУ СОШ № 7 г. Ставрополя, в том числе регламентирующих порядок предоставления доступа к ресурсам ИС и управления таким доступом, порядок антивирусной защиты, обеспечения безопасности эксплуатации используемых средств криптографической защиты информации.

VI. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и средств защиты информации информационных систем

1. В целях обеспечения непрерывной работы ИС и восстановления ее ресурсов вследствие сбоев в функционировании ИС применяются следующие технические средства и системы:

– системы жизнеобеспечения;
– системы обеспечения отказоустойчивости;
– системы резервного копирования и хранения данных.

2. Системы жизнеобеспечения ИС включают:

– пожарные сигнализации и системы пожаротушения;
– системы вентиляции и кондиционирования;
– системы резервного питания.

3. Все помещения МБОУ СОШ № 7 г. Ставрополя, в которых размещаются элементы ИС и СЗИ, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также автоматизированные рабочие места (далее – АРМ) пользователей ИС должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных АРМ;
– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
– резервные линии электропитания в пределах комплекса зданий;
– аварийные электрогенераторы.

6. Системы обеспечения отказоустойчивости:

– кластеризация;
– технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение персональных данных, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

7. С целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним, в ИС должны применяться системы резервного копирования и хранения данных.

8. Резервное копирование и хранение данных должно осуществляться на периодической основе:

– для обрабатываемых персональных данных – не реже раза в неделю;

– для технологической информации – не реже раза в месяц;

– для эталонных копий программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программное обеспечение СЗИ), с которых осуществляется их установка на элементы ИС – каждый раз при внесении изменений в такие копии (выход новых версий).

9. Порядок осуществления резервного копирования защищаемой информации ИС определяется Инструкцией по резервному копированию защищаемой информации в информационных системах МБОУ СОШ № 7 г. Ставрополя.

VII. Порядок обеспечения физической защиты элементов ИС

1. В целях исключения неконтролируемого пребывания посторонних лиц в помещениях МБОУ СОШ № 7 г. Ставрополя, в которых ведется работа с персональными данными и располагаются технические средства ИС и СЗИ, приказом директора МБОУ СОШ № 7 г. Ставрополя выделяется контролируемая зона.

2. Обеспечение физической защиты ИС, ее элементов, выделение и обеспечение пространства контролируемой зоны достигается посредством:

– организации разрешительной системы доступа на территорию МБОУ СОШ № 7 г. Ставрополя, в помещения с оборудованием ИС, к техническим средствам ИС;

– использования средств физической охраны;

– использования средств видеонаблюдения;

– конструктивных усилений окон, дверей, стен и установкой иных преград;

– виброакустическим, визуальным, электромагнитным экранированием помещений и средств обработки персональных данных.

3. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИС должны иметь прочные входные двери с надежными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода работников МБОУ СОШ № 7 г. Ставрополя.

4. Двери помещений, в которых размещаются АРМ пользователей ИС, должны быть оборудованы. Нахождение в таких помещениях лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал, иные работники МБОУ СОШ № 7 г. Ставрополя),

должно производиться только в присутствии работников, участвующих в соответствующих технологических процессах.

5. Расположение мониторов АРМ должно препятствовать несанкционированному просмотру выводимой на них информации.

6. При выносе устройств, используемых для хранения персональных данных, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

7. В отношении отдельных ИС возможны дополнительные либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз.

VIII. Контроль изменений в составе и структуре информационных систем

1. Все изменения в составе и структуре ИС должны контролироваться и регламентироваться. Контролю подлежат следующие изменения:

- внесение новых устройств в состав ИС (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);
- удаление устройств из состава ИС;
- изменение мест установки устройств из состава ИС;
- прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;
- существенное изменение состава и конфигурации системного и прикладного программного обеспечения, используемого для обработки персональных данных;
- создание новых и изменение существующих технологических процессов, связанных с обработкой персональных данных.

2. Каждое изменение состава ИС, типов технических средств, топологии ИС должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИС. При необходимости должна производиться модернизация СЗИС.

IX. Внутренний аудит безопасности персональных данных

1. Внутренний аудит безопасности персональных данных позволяет установить, что применяемые методы, способы и средства обеспечения безопасности персональных данных при их обработке в ИС:

соответствуют законодательству Российской Федерации и нормативным документам МБОУ СОШ № 7 г. Ставрополя, регламентирующим вопросы обеспечения безопасности персональных данных;

- своевременно и эффективно внедряются и поддерживаются;
- функционируют должным образом.

2. Процесс проведения внутреннего аудита безопасности предполагает получение объективных качественных и количественных оценок текущего

состояния СЗИС и проводится в рамках проведения общего контроля состояния и эффективности защиты информации конфиденциального характера в МБОУ СОШ № 7 г. Ставрополя.

3. В ходе проведения внутреннего аудита оценивается текущий уровень защищенности ИС, определяются уязвимости ИС, в том числе проверяется:

– наличие установленных СЗИ;

– корректность настроек СЗИ;

– выполнение пользователями ИС и Администраторами требований нормативных документов МБОУ СОШ № 7 г. Ставрополя, регламентирующих вопросы обеспечения безопасности персональных данных;

– исполнение требований к процедурам обработки персональных данных (уничтожению персональных данных, допуску работников МБОУ СОШ № 7 г. Ставрополя к персональным данным и т.п.);

– правильность организации работы с машинными носителями персональных данных.

4. Все события, происходящие в ИС и связанные с безопасностью (включая предоставление доступа, попытки аутентификации, изменение системных политик и пользовательских привилегий, системные сбои и т.п.), должны отслеживаться и протоколироваться в специальные электронные журналы аудита как СЗИ, так и встроенных средств, имеющихся в составе операционных систем, систем управления базами данных, прикладных приложений, с помощью которых осуществляется обработка персональных данных.

5. События, зафиксированные в указанных журналах аудита, анализируются Администратором в текущем порядке на постоянной основе, а также в ситуациях, требующих проведения расследования инцидента информационной безопасности.

6. В ИС должен проводиться анализ защищенности посредством использования средств анализа защищенности, предназначенных для решения следующих основных задач:

– анализ параметров конфигурации операционных систем и приложений по шаблонам с целью выявления уязвимостей ИС, в том числе связанных с некорректной настройкой таких систем и приложений, определения уровня защищенности контролируемых ИС и соответствия текущего состояния СЗИС принятой политике безопасности информации;

– коррекция конфигурационных параметров операционных систем и приложений;

– контроль изменения состояния операционных систем и приложений, осуществляемый на основе мгновенных снимков их параметров и атрибутов файлов.

7. Анализ защищенности проводится Администратором в плановом порядке с установленной периодичностью.

X. Заключительные положения

1. Работники МБОУ СОШ № 7 г. Ставрополя, осуществляющие автоматизированную обработку персональных данных, сопровождение и обслуживание информационных систем, а также обеспечивающие безопасность обрабатываемой в таких системах информации, должны иметь соответствующие навыки и знания.

2. Не реже одного раза в год должно проводиться обучение работников МБОУ СОШ № 7 г. Ставрополя, указанных в пункте 1 раздела XI настоящего Положения, по вопросам, связанным с обеспечением безопасности персональных данных. Обучение может проводиться в формате специализированных курсов, внешних и внутренних семинаров, конференций, инструктажей, методической помощи.

Внутренние семинары и инструктажи могут проводиться для работников МБОУ СОШ № 7 г. Ставрополя, осуществляющих автоматизированную обработку персональных данных, ответственным за организацию обработки персональных данных, приглашенными специалистами, другими подготовленными лицами, в том числе, по мере необходимости, Администратором БИ.

3. Работники МБОУ СОШ № 7 г. Ставрополя, виновные в нарушении норм, регламентирующих порядок обеспечения безопасности персональных данных при их обработке в ИС, установленных законодательством Российской Федерации, настоящим Положением и иными нормативными актами МБОУ СОШ № 7 г. Ставрополя, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.