ПРИНЯТО:
на Педагогическом совете
МКОУ СОШ с. Первомайское
Протокол № 1от 28.08.2026г.

УТВЕРЖДЕНО:
Директор
МКОУ СОШ с. Первомайское
_____ /И.Ю. Пьянкова/
Приказ №122-од от 28.08.2026г.

Положение
об обеспечении информационной безопасности
в МКОУ СОШ с. Первомайское

1. Общие положения

1.1. Данное Положение разработано в соответствии с Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» с изменениями от 4 августа 2026 года **[1]**, Трудовым кодексом Российской Федерации **[2]**, Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с изменениями от 29 декабря 2025 года **[3]**, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» с изменениями от 24 июня 2025 года **[4]**, Федеральным законом от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» с изменениями от 29 декабря 2025 года **[5]**, постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» **[6]**, приказом ФСТЭК РФ от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» с изменениями от 14 мая 2020 года **[7]**, а также Уставом общеобразовательной организации и другими нормативными правовыми актами Российской Федерации, регламентирующими деятельность организаций, осуществляющих образовательную деятельность.

1.2. Настоящее Положение определяет систему правовых, организационных и технических мер, направленных на обеспечение информационной безопасности обучающихся, работников и иных участников образовательных отношений в общеобразовательной организации, защиту информационных ресурсов, персональных данных, информационных систем, технических средств, а также ограничение доступа обучающихся к информации, причиняющей вред их здоровью и развитию.

1.3. Под информационной безопасностью общеобразовательной организации понимается состояние защищенности информации, информационных ресурсов, информационных систем, технологий их формирования и использования, при котором обеспечиваются конфиденциальность, целостность и доступность информации, а также защита прав субъектов персональных данных и иных участников образовательных отношений.

1.4. Использование сети Интернет в общеобразовательной организации подчинено следующим принципам:

- соответствие образовательным целям;
- способствование гармоничному формированию и развитию личности;
- уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;

- приобретение новых навыков и знаний;
- расширение применяемого спектра учебных и наглядных пособий;
- социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в общеобразовательной организации относятся:

- информационные ресурсы, содержащие сведения ограниченного доступа, включая персональные данные обучающихся, родителей (законных представителей), работников и иных лиц;
- информационные системы, базы данных, электронные журналы и дневники, системы электронного документооборота, официальный сайт, локальная сеть, средства доступа к сети Интернет;
- средства вычислительной и организационной техники, серверное оборудование, сетевое оборудование, средства связи и передачи данных, программное обеспечение;
- материальные и электронные носители информации;
- учетные записи пользователей, пароли, ключи доступа и иные средства идентификации и аутентификации.

1.6. Система информационной безопасности (далее – СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

- *правовая защита* – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- *организационная защита* – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- *инженерно-техническая защита* – это использование различных технических средств, препятствующих нанесению ущерба.

2. Основные термины и их определения

2.1. ***Аутентификация*** – действия по проверке подлинности субъекта доступа в информационной системе [ГОСТ р 58833-2020, пункт 3.4].

2.2. ***Безопасность информации*** – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [ГОСТ р 50922-2006, пункт 2.4.5].

2.3. ***Государственная информационная система*** – информационная система, создаваемая в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях [3, часть 1 статьи 14].

2.4. ***Доступ к информации*** – возможность получения информации и ее использования [3, пункт 6 статьи 2].

2.5. ***Доступность*** – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

2.6. ***Защита информации от несанкционированного доступа*** – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации [ГОСТ р 50922-2006, пункт 2.3.6].

2.7. ***Защищаемая информация*** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [ГОСТ р 50922-2006, пункт 2.5.2].
2.8. ***Идентификация*** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов [ГОСТ р 58833-2020, пункт 3.24].
2.9. ***Информационная система*** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [3, пункт 3 статьи 2].
2.10. ***Информационные ресурсы*** – отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов) [ГОСТ р 58833-2020, пункт 3.25].
2.11. ***Информационные технологии*** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [3, пункт 2 статьи 2].
2.12. ***Информация*** – сведения (сообщения, данные) независимо от формы их представления [3, пункт 1 статьи 2].
2.13. ***Контролируемая зона*** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
2.14. ***Конфиденциальность*** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [3, пункт 7 статьи 2].
2.15. ***Обработка персональных данных*** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [4, пункт 3 статьи 3].
2.16. ***Оператор*** – 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 [4, пункт 2 статьи 3].
2.17. ***Персональные данные*** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу [4, пункт 1 статьи 3].
2.18. ***Угроза безопасности информации*** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее [ГОСТ р 51624-2000, пункт 3.1.17].
2.19. ***Уязвимость*** – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации [ГОСТ р 58142-2018/ISO/IEC TR 20004:2015, пункт 3.8].
2.20. ***Целостность*** – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

3. Цели и задачи обеспечения безопасности информации

3.1. Главной целью обеспечения информационной безопасности в общеобразовательной организации является соблюдение требований законодательства Российской Федерации в сфере информации, защиты информации, персональных данных и защиты детей от информации, причиняющей вред их здоровью и развитию, а также предотвращение ущерба

вследствие неправомерного доступа, разглашения, утраты, уничтожения, блокирования, модификации, копирования, предоставления, распространения или иного неправомерного использования информации.

3.2. Основными целями обеспечения безопасности информации являются:

- предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в общеобразовательной организации;
- предотвращение нарушений прав личности обучающихся, работников школы на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по блокированию информации.

3.3. Основными задачами обеспечения безопасности информации являются:

- соответствие положениям законодательных актов и нормативным требованиям по защите информации;
- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам общеобразовательной организации, нарушению нормального функционирования и развития школы;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
- эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
- развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
- развитие и совершенствование защищенного юридически значимого электронного документооборота;
- создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности;
- создание механизмов управления системой информационной безопасности.

4. Основные принципы построения системы обеспечения информационной безопасности

Построение системы обеспечения информационной безопасности общеобразовательной организации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

4.1. ***Законность***. Предполагает осуществление защитных мероприятий и разработку системы защиты информации общеобразовательной организации в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по информационной безопасности, утвержденных органами государственной власти. Принятые меры информационной безопасности не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к ресурсам конкретных информационных систем. Все пользователи информационных систем школы должны иметь представление об ответственности за правонарушения в области информации.

4.2. ***Системность***. Системный подход к построению системы обеспечения информационной безопасности в общеобразовательной организации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности школы. При создании системы защиты учитываются все слабые и наиболее уязвимые места информационных систем общеобразовательной организации, а также характер, возможные объекты и направления атак на неё со стороны нарушителей, пути несанкционированного доступа к информации. Система защиты должна строиться с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.3. ***Комплексность***. Комплексное использование методов и средств защиты информационных систем предполагает согласованное применение программных и технических средств при построении целостной системы защиты, перекрывающей все значимые каналы реализации угроз. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.4. ***Непрерывность защиты***. Для обеспечения этого принципа необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий). Порядок получения доступа к информационным ресурсам регламентируется локальными нормативными актами и организационно-распорядительными документами общеобразовательной организации.

4.5. ***Своевременность***. Предполагается упреждающий характер мер обеспечения информационной безопасности, то есть постановка задач по комплексной защите информации и реализация мер обеспечения безопасности информации на ранних стадиях разработки информационных систем. Разработка системы защиты ведется параллельно с разработкой и развитием самой подлежащей защите информационной системы.

4.6. ***Преемственность и совершенствование***. Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем общеобразовательной организации и систем информационной защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.7. ***Персональная ответственность***. Предполагает возложение ответственности за обеспечение информационной безопасности на каждого работника общеобразовательной организации в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.8. ***Минимизация полномочий***. Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объёме, если это необходимо работнику для выполнения его должностных обязанностей.

4.9. ***Гибкость системы информационной безопасности***. Предполагает способность системы информационной безопасности реагировать на изменения внешней среды и условий осуществления общеобразовательной организацией своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры школы;
- изменение существующих или внедрение принципиально новых информационных систем;
- ввод в эксплуатацию новых технических средств.

4.10. ***Простота применения средств защиты***. Механизмы и методы системы защиты информации должны быть понятны и просты в использовании. Применение средств и методов защиты не связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не требует от пользователя выполнения малопонятных ему операций.

4.11. ***Обоснованность и техническая реализуемость***. Предполагает, что информационные технологии, технические и программные средства, средства и меры защиты информации реализуются на современном техническом уровне и обоснованы для достижения заданного уровня безопасности информации и экономической целесообразности, а также соответствуют установленным нормам и требованиям по безопасности информации.

4.12. ***Специализация и профессионализм***. Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности

информационных ресурсов, имеющих необходимые лицензии в случаях, когда наличие таких лицензий предусмотрено законодательством Российской Федерации. Реализация административных мер и эксплуатация средств защиты осуществляется профессионально подготовленными специалистами защиты информации общеобразовательной организации.

4.13. ***Обязательность контроля***. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает санкционированные и несанкционированные действия пользователей. Выявленные работниками общеобразовательной организации недостатки системы защиты информации доводятся до сведения непосредственного руководителя. О существенных недостатках сообщается директору школы.

5. Меры, методы и средства обеспечения информационной безопасности

Меры обеспечения информационной безопасности.

5.1. К *законодательным (правовым)* мерам обеспечения информационной безопасности относятся действующие в Российской Федерации законодательные и иные нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры обеспечения информационной безопасности носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем общеобразовательной организации.

5.2. К *технологическим* мерам обеспечения информационной безопасности относятся технологические решения и приемы, направленные на уменьшение возможности совершения работниками общеобразовательной организации ошибок и нарушений в рамках предоставленных им прав и полномочий.

5.3. *Организационные (административные)* меры обеспечения информационной безопасности – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Организационными (административными) мерами обеспечения информационной безопасности являются:

- регламентация доступа в здание общеобразовательной организации;
- регламентация допуска работников к использованию информационных ресурсов;
- анализ требований к элементам системы на основе заявок пользователей на обслуживание и модификацию аппаратных и программных ресурсов;
- обеспечение и контроль физической целостности (неизменности конфигурации) средств вычислительной техники;
- обучение пользователей;
- деятельность по обеспечению информационной безопасности;
- условия обработки информационных ресурсов конфиденциального характера, ответственность за нарушения установленного порядка пользования информационными ресурсами школы.

5.4. *Физические* меры обеспечения информационной безопасности основаны на применении механических, электронных или электронно-механических устройств, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к элементам информационных систем и защищаемой информации.

5.5. *Технические и программно-технические* меры обеспечения информационной безопасности основаны на использовании средств вычислительной техники, средств защиты

информации, программного обеспечения и иных технических решений, обеспечивающих идентификацию и аутентификацию пользователей, разграничение прав доступа, регистрацию событий безопасности, антивирусную защиту, резервное копирование, фильтрацию интернет-контента, защиту каналов связи и иные меры, необходимые для защиты информации.

6. Правовые нормы обеспечения информационной безопасности

6.1. Общеобразовательная организация в пределах своей компетенции определяет состав, объем и порядок защиты информации ограниченного доступа, включая персональные данные обучающихся, родителей (законных представителей), работников и иных лиц, а также принимает меры по защите такой информации от неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

6.2. Школа обязана обеспечить сохранность конфиденциальной информации.

6.3. Администрация общеобразовательной организации:

- назначает ответственного за обеспечение информационной безопасности;
- назначает ответственного за организацию обработки персональных данных, если такая обязанность возложена на отдельное должностное лицо;
- утверждает локальные нормативные акты и организационно-распорядительные документы по вопросам информационной безопасности и защиты персональных данных;
- утверждает перечень информационных систем, информационных ресурсов и баз данных, подлежащих защите;
- утверждает порядок доступа работников к информационным ресурсам и персональным данным;
- организует меры по ограничению доступа обучающихся к информации, причиняющей вред их здоровью и развитию;
- организует контроль соблюдения работниками требований информационной безопасности;
- принимает меры реагирования при выявлении нарушений информационной безопасности.

6.4. К организационным и функциональным документам по обеспечению информационной безопасности относятся:

- приказ о назначении ответственного за обеспечение информационной безопасности;
- приказ о назначении ответственного за организацию обработки персональных данных;
- перечень информационных систем, информационных ресурсов и баз данных;
- перечень лиц, имеющих доступ к информационным системам и персональным данным;
- инструкции пользователей информационных систем;
- порядок предоставления информации по запросам третьих лиц и уполномоченных органов;
- порядок учета, хранения, передачи и уничтожения носителей информации;
- порядок реагирования на инциденты информационной безопасности;
- иные локальные акты и организационно-распорядительные документы общеобразовательной организации.

6.5. Порядок допуска сотрудников общеобразовательной организации к информации предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства Российской Федерации и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

7. Использование сети Интернет

7.1. Использование сети Интернет в общеобразовательной организации осуществляется в целях реализации образовательных программ, воспитательной работы, методического обеспечения образовательной деятельности, выполнения работниками должностных обязанностей, а также обеспечения доступа обучающихся к образовательным и информационным ресурсам при соблюдении требований законодательства Российской Федерации.

7.2. Работники общеобразовательной организации вправе:

- размещать информацию в сети Интернет на интернет-ресурсах школы;
- иметь учетную запись электронной почты на интернет-ресурсах школы.

7.3. Работникам общеобразовательной организации запрещается размещать в сети Интернет, на официальном сайте, образовательных платформах, в социальных сетях и мессенджерах информацию:

- противоречащую законодательству Российской Федерации и локальным нормативным актам общеобразовательной организации;
- содержащую персональные данные обучающихся, родителей (законных представителей), работников и иных лиц без правового основания;
- нарушающую авторские, смежные и иные права третьих лиц;
- не относящуюся к образовательной деятельности и деятельности общеобразовательной организации;
- нарушающую требования профессиональной этики, честь, достоинство и деловую репутацию обучающихся, работников и иных лиц;
- содержащую сведения ограниченного доступа, если их размещение не предусмотрено законодательством Российской Федерации.

7.4. Обучающиеся вправе использовать ресурсы сети Интернет, информационные системы и электронные образовательные ресурсы школы в образовательных целях, в порядке и на условиях, установленных настоящим Положением, иными локальными нормативными актами общеобразовательной организации и указаниями педагогических работников.

7.5. Обучающимся запрещается:

- посещать интернет-ресурсы, содержащие информацию, причиняющую вред здоровью и развитию детей, а также информацию, распространение которой запрещено законодательством Российской Федерации;
- осуществлять действия, нарушающие права и законные интересы других лиц, включая распространение оскорбительной, недостоверной, порочащей информации, угроз, персональных данных иных лиц без правового основания;
- совершать сделки, регистрироваться на интернет-ресурсах, оформлять подписки, заказы, платежи и иные юридически значимые действия с использованием оборудования и сети общеобразовательной организации без разрешения педагогического работника или иного уполномоченного лица;
- загружать, устанавливать, копировать или запускать файлы и программы на оборудовании общеобразовательной организации без разрешения уполномоченного лица;
- предпринимать попытки обхода средств фильтрации, блокировки, антивирусной защиты, разграничения доступа и иных средств защиты информации;
- использовать сеть Интернет для целей, не связанных с образовательной деятельностью, если иное не разрешено педагогическим работником или уполномоченным лицом.

7.6. Доступ пользователей к сети Интернет, информационным системам и электронным образовательным ресурсам общеобразовательной организации предоставляется в порядке, установленном локальными нормативными актами школы. Ограничение, приостановление или восстановление доступа осуществляется уполномоченным лицом, назначенным приказом директора, при наличии оснований, связанных с обеспечением информационной

безопасности, защитой персональных данных, соблюдением законодательства Российской Федерации и настоящего Положения.

7.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательной деятельности, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

7.8. Уполномоченное лицо при получении информации об интернет-ресурсе, содержание которого не соответствует задачам образования и воспитания либо может нарушать законодательство Российской Федерации, обязано:

- принять сообщение пользователя;
- зафиксировать дату, время, адрес ресурса и обстоятельства выявления;
- принять меры по ограничению доступа к такому ресурсу с использованием технических средств фильтрации и блокирования;
- при наличии признаков распространения информации, запрещенной законодательством Российской Федерации, сообщить об этом директору школы и принять меры в порядке, установленном законодательством Российской Федерации и локальными актами общеобразовательной организации.

7.9. Общеобразовательная организация обеспечивает применение технических, программных и организационных мер, направленных на ограничение доступа обучающихся к информации, причиняющей вред их здоровью и развитию, в том числе с использованием средств контентной фильтрации, антивирусной защиты, разграничения прав доступа и контроля использования сети Интернет.

7.10. Педагогические работники осуществляют контроль использования обучающимися сети Интернет и электронных образовательных ресурсов во время учебных занятий, внеурочных занятий и иных мероприятий, организуемых общеобразовательной организацией, в пределах своих должностных обязанностей.

8. Мероприятия по обеспечению информационной безопасности

8.1. Для обеспечения информационной безопасности в общеобразовательной организации проводятся следующие мероприятия:

- определение перечня защищаемых информационных ресурсов, информационных систем и баз данных;
- назначение ответственных лиц за обеспечение информационной безопасности и организацию обработки персональных данных;
- разграничение прав доступа пользователей к информационным ресурсам;
- организация парольной защиты, идентификации и аутентификации пользователей;
- применение антивирусной защиты и средств контентной фильтрации;
- резервное копирование информации;
- учет, хранение и уничтожение материальных и электронных носителей информации;
- обучение и инструктаж работников по вопросам информационной безопасности и защиты персональных данных;
- контроль соблюдения требований информационной безопасности;
- реагирование на инциденты информационной безопасности и принятие мер по устранению их последствий.

9. Организация работы с информационными ресурсами и технологиями

9.1. Организация делопроизводства в общеобразовательной организации осуществляется в соответствии с инструкцией по делопроизводству, номенклатурой дел, требованиями законодательства Российской Федерации об архивном деле, законодательством о персональных данных и локальными нормативными актами общеобразовательной организации.

9.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

9.2.1. Документы, содержащие сведения ограниченного доступа, передаются исполнителям в порядке, установленном инструкцией по делопроизводству и локальными нормативными актами общеобразовательной организации.
9.2.2. Документы, дела и носители информации, содержащие сведения ограниченного доступа, хранятся в условиях, исключающих доступ к ним посторонних лиц, в специально отведенных помещениях, шкафах, сейфах или иных местах хранения, обеспечивающих их сохранность.
9.2.3. Выдача, возврат, копирование, передача и уничтожение документов и носителей информации, содержащих сведения ограниченного доступа, осуществляются в порядке, установленном локальными нормативными актами общеобразовательной организации.
9.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.
9.2.5. Вынос документов и носителей информации, содержащих сведения ограниченного доступа, за пределы общеобразовательной организации допускается только с разрешения директора или уполномоченного им лица при наличии служебной необходимости и с соблюдением мер защиты информации.
9.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется акт приема-передачи документов в произвольной форме.
9.3. Для организации делопроизводства приказом директора общеобразовательной организации назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной директором школы. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

10. О системном администрировании и обязанностях ответственного за информационную безопасность

10.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы системного администратора в общеобразовательной организации.
10.2. Для решения задач информационной безопасности системный администратор или иное уполномоченное лицо в пределах должностных обязанностей:

- обеспечивает учет пользователей информационных систем;
- обеспечивает настройку прав доступа пользователей;
- организует применение парольной защиты и ее изменение при наличии оснований;
- обеспечивает функционирование средств защиты информации, антивирусной защиты и контентной фильтрации;
- организует резервное копирование информации;
- принимает меры по восстановлению работоспособности информационных систем при сбоях;
- незамедлительно сообщает директору и ответственному за информационную безопасность о выявленных инцидентах, угрозах и нарушениях информационной безопасности.

11. Антивирусная защита

Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.).
11.1. Использование оборудования общеобразовательной организации без средств антивирусной защиты и иных предусмотренных мер защиты информации не допускается. Антивирусная защита организуется с применением лицензионного программного обеспечения, встроенных средств защиты операционных систем или иных средств защиты, использование которых не нарушает законодательство Российской Федерации и права правообладателей.
11.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически по мере выпуска обновлений производителем, а при невозможности – не реже одного раза в сутки.

11.3. За своевременное обновление антивирусного программного обеспечения отвечает системный администратор.
11.4. На компьютерах и иных устройствах, используемых обучающимися в образовательной деятельности, применяются средства ограничения доступа к информации, причиняющей вред здоровью и развитию детей, а также к информации, распространение которой запрещено законодательством Российской Федерации.
11.5. Доступ обучающихся к беспроводным сетям общеобразовательной организации предоставляется только в порядке, установленном локальными нормативными актами школы, с применением средств идентификации, аутентификации, разграничения доступа и контентной фильтрации. Использование обучающимися несанкционированного доступа к сети общеобразовательной организации запрещается.
11.6. Работа обучающихся с компьютерами, информационными системами, электронными образовательными ресурсами и сетью Интернет в рамках образовательной деятельности осуществляется под контролем педагогического работника или иного уполномоченного лица.

12. Обязанности и права должностных лиц общеобразовательной организации по обеспечению информационной безопасности

12.1. Директор общеобразовательной организации организует работу по построению системы обеспечения информационной безопасности в школе. В частности:

- назначает ответственного за организацию информационной безопасности из числа сотрудников общеобразовательной организации;
- утверждает круг лиц, имеющих доступ к защищаемой информации и порядок их работы;
- утверждает комплект документов, определяющих политику в отношении информационной безопасности и защиты информации в школе, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

12.2. Ответственный за организацию информационной безопасности:

- разрабатывает проекты организационно-распорядительных документов по вопросам информационной безопасности;
- организует контроль соблюдения требований информационной безопасности;
- проводит инструктаж работников по вопросам информационной безопасности;
- контролирует выполнение мер по защите информации, антивирусной защите, резервному копированию, разграничению доступа и контентной фильтрации;
- контролирует порядок учета, хранения и уничтожения носителей информации;
- участвует в рассмотрении инцидентов информационной безопасности;
- докладывает директору общеобразовательной организации о выявленных нарушениях, угрозах и недостатках системы защиты информации;
- организует подготовку предложений по совершенствованию системы информационной безопасности.

12.3. Лица, виновные в нарушении требований законодательства и локальных нормативных актов общеобразовательной организации в области информационной безопасности и защиты персональных данных, несут ответственность в случаях и порядке, предусмотренных законодательством Российской Федерации.

13. Реагирование на инциденты информационной безопасности

13.1. К инцидентам информационной безопасности относятся события, повлекшие или способные повлечь нарушение конфиденциальности, целостности или доступности информации, неправомерный доступ к информационным системам, утрату, уничтожение, изменение, блокирование, копирование, предоставление или распространение информации, включая персональные данные.
13.2. Работники общеобразовательной организации обязаны незамедлительно сообщать директору, ответственному за информационную безопасность и ответственному за

организацию обработки персональных данных о выявленных или предполагаемых инцидентах информационной безопасности.
13.3. При выявлении инцидента информационной безопасности общеобразовательная организация принимает меры по локализации инцидента, предотвращению дальнейшего нарушения, восстановлению работоспособности информационных систем, установлению причин и условий инцидента, а также привлечению виновных лиц к ответственности в порядке, установленном законодательством Российской Федерации.
13.4. В случае если инцидент связан с неправомерной или случайной передачей, предоставлением, распространением персональных данных, повлекшей нарушение прав субъектов персональных данных, общеобразовательная организация уведомляет уполномоченный орган по защите прав субъектов персональных данных в порядке и сроки, установленные Федеральным законом № 152-ФЗ «О персональных данных».

14 Заключительные положения
14.1. Настоящее Положение является локальным нормативным актом, принимается на Педагогическом совете школы и утверждается (либо вводится в действие) приказом директора общеобразовательной организации.
14.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии действующим законодательством Российской Федерации и утверждаются в порядке, установленном для принятия локальных нормативных актов общеобразовательной организации.
14.3. Настоящее Положение принимается на неопределенный срок и действует до принятия новой редакции либо признания его утратившим силу.
14.4. После утверждения настоящего Положения в новой редакции предыдущая редакция Положения утрачивает силу.