ЧАСТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ОБЩЕОБРАЗОВАТЕЛЬНАЯ ГИМНАЗИЯ «АЛЬБЕРТИНА»
236003 г.Калининград, ул.Ялтинская,126; тел./факс 8 (4012) 355-400
электронная почта: albertina_a@mail.ru

П Р И К А З

« 30 » августа 2019 г. № 69/1

О мерах по защите информации ограниченного доступа и защите персональных данных при их обработке в информационных системах

В соответствии с Федеральными законами 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», Постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21.03.2012 № 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» и иными нормативно-правовыми актами, действующими на территории Российской Федерации,

ПРИКАЗЫВАЮ:

1. Утвердить следующие документы по организации информации ограниченного доступа и защиты персональных данных в гимназии «Альбертина» (далее –гимназия):

- Концепцию информационной безопасности информационных систем персональных данных в гимназии «Альбертина» (приложение № 1);
- Политику в гимназии «Альбертина» в отношении обработки персональных данных (приложение № 2);
- Перечень информации конфиденциального характера и персональных данных, обрабатываемых в гимназии «Альбертина» (приложение № 3);
- Положение по обработке и защите персональных данных (приложение №4);
- Положение о порядке учета, хранения и обращения со съемными носителями персональных данных (приложение № 5);
- Положение о разграничении прав доступа к обрабатываемым персональным

данным (приложение № 6);

- Правила рассмотрения запросов субъектов персональных данных или их представителей (приложение № 7);
- Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение № 8);
- Правила работы с обезличенными персональными данными (приложение №9);
- Инструкцию реагирования на инциденты информационной безопасности (приложение № 10);
- Инструкцию по организации антивирусной защиты при работе в информационной системе (приложение № 11);
- Инструкцию по организации парольной защиты при работе в информационной системе (приложение № 12);
- Инструкцию по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных (приложение № 13);
- Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (приложение № 14);
- Инструкцию по обращению с криптографическими средствами защиты информации (приложение № 15);
- Инструкцию по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн гимназии «Альбертина» (приложение № 16);
- Инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (приложение № 17).

2. Признать утратившими силу локальные акты прошлых лет в гимназии «Альбертина» в отношении информационной безопасности и защиты персональных данных.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор _____ Е.В. Ольшанская

Приложение № 1
Утверждено приказом
директора гимназии
«Альбертина»
Ольшанская Е.В.
от 30.08.2019 г. №69/1

Концепция информационной безопасности информационных систем персональных данных и информации ограниченного доступа
ЧАСТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ОБЩЕОБРАЗОВАТЕЛЬНАЯ ГИМНАЗИЯ «АЛЬБЕРТИНА»

Определения

В настоящем документе используются следующие термины и их определения.
Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.
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 информационных системах персональных данных.
Биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.
Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.
Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.
Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.
Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.
Доступ к информации - возможность получения информации и ее использования.
Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).
Защищаемая информация - информация, являющаяся предметом собственности и под- лежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие

физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации. **Контролируемая зона** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности - функциональные возможности средств вычисли- тельной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. **Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или

физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных - средства вычислительной

техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (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, применяемые в информационных системах.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических эле- ментов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных - 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 информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение - учреждения образования, здравоохранения, социальной сферы, труда и занятости.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

АВС - антивирусные средства
АРМ - автоматизированное рабочее место
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
ИОД –информация ограниченного доступа
КЗ - контролируемая зона
ЛВС - локальная вычислительная сеть
МЭ - межсетевой экран
НСД - несанкционированный доступ
ОС - операционная система
ПДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПЭМИН - побочные электромагнитные излучения и наводки
САЗ - система анализа защищенности
СЗИ - средства защиты информации
СЗИОД-системы защиты информации ограниченного доступа
СЗПДн - система (подсистема) защиты персональных данных
СОВ - система обнаружения вторжений
ТКУИ - технические каналы утечки информации
УБПДн - угрозы безопасности персональных данных

Введение

Настоящая Концепция информационной безопасности гимназии «Альбертина», разработана в соответствии с действующими нормативно-методическими документами и является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности в гимназии.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в гимназии при обработке информации в гимназии.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты информации ограниченного доступа (ИОД) и персональных данных гимназии «Альбертина».

Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.
Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ИОД и ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.
Под информационной безопасностью ИОД и ПДн понимается защищенность информации ограниченного доступа и персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ИОД и ПДн, а также к прогнозированию и предотвращению таких воздействий.
Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности школы, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.
Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности ИОД и ПДн в школе;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности ИОД и ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ИОД и ПДн;
- координации деятельности структурных подразделений школы при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ИОД и ПДн в ИСПДн школы.

Область применения Концепции распространяется на все подразделения школы, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.
Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности ИОД и ПДн.

Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) и системы защиты информации ограниченного доступа (СЗИОД) гимназии в соответствии с Перечнем ИСПДн. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.
СЗПДн и СЗИОД представляет собой совокупность организационных и технических мероприятий для защиты ИОД и ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.
Безопасность персональных данных и ИОД достигается путем исключения несанкционированного, в том числе случайного, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.
Структура, состав и основные функции СЗПДн и СЗИОД определяются исходя из класса. СЗПДн и СЗИОД включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно- технических воздействий на технические средства обработки ИОД и ПДн), а также используемые в информационной системе информационные технологии.
Эти меры призваны обеспечить:

- **конфиденциальность** информации (защита от несанкционированного ознакомления);
- **целостность** информации (актуальность и непротиворечивость информации, ее

защищенность разрушения и несанкционированного изменения);

- **доступность** информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание;
- стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемосдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности ИОД и ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно-распорядительных документов:

- План мероприятий по обеспечению защиты ИОД и ПДн при их обработке;
- План мероприятий по контролю обеспечения защиты ИОД и ПДн;
- Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;
- Должностная инструкция администратора ИСПДн в части обеспечения безопасности ИОД и ПДн при их обработке;
- Должностная инструкция администратора безопасности ИСПДн;
- Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ИОД и ПДн при их обработке в ИСПДн;
- Инструкция на случай возникновения внештатной ситуации;
- Рекомендации по использованию программных и аппаратных средств защиты информации.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн.

1. Задачи СЗПДн и СЗИОД

Основной целью СЗПДн и СЗИОД является минимизация ущерба от возможной реализации угроз безопасности ИОД и ПДн.

Для достижения основной цели система безопасности ИОД и ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИОД и ИСПДн;

б) средствам вычислительной техники ИОД и ИСПДн;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту ИОД и ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту ИОД и ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от

несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;
- своевременное выявление источников угроз безопасности ИОД и ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

2. Объекты защиты

2.1. Перечень информационных систем

В гимназии производится обработка персональных данных в информационных система обработки персональных данных (ИСПДн).

Перечень ИСПДн определяется на основании Отчета по результатам внутренней проверки гимназии

2.2. Перечень объектов защиты

Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПДн.

Объекты защиты включают:

1) Обрабатываемая информация.
2) Технологическая информация.
3) Программно-технические средства обработки.
4) Средства защиты ПДн.
5) Каналы информационного обмена и телекоммуникации.
6) Объекты и помещения, в которых размещены компоненты ИСПДн.

3. Классификация пользователей ИСПДн

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник школы, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

1) Администратор ИСПДн. Сотрудник школы, который занимается настройкой, внедрением и сопровождением системы. Администратор ИСПДн обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн;
- обладает информацией об алгоритмах и программах обработки информации на ИСПДн.

2) Администратор безопасности ИСПДн. Сотрудник школы, который занимается проведением работ по организационно-технической и антивирусной защите ИСПДн и поддержанию достигнутого уровня защиты ИС и ее ресурсов.

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- имеет право доступа к конфигурированию технических средств сети исключительно в контрольных (инспекционных) целях;
- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.

3) Пользователь (оператор) ИСПДн. Сотрудники школы, участвующие в процессе эксплуатации ИСПДн. Оператор ИСПДн обладает следующим уровнем доступа:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности школы.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки школы. На основании Отчета определяются права доступа к элементам ИСПДн для всех групп пользователей и отражаются в Положении о разграничении прав доступа к обрабатываемым персональным данным школы.

4. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности ИОД и ПДн ИСПДн и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку СЗИОД и СЗПДн в соответствии с действующим законодательством в области защиты ИОД и ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной и муниципальной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ИОД и ПДн ИСПДн должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ИОД и ПДн.

5.2. Системность

Системный подход к построению СЗПДн и СЗИОД предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ИОД и ПДн ИСПДн школы. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ИОД и ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрываю- щей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее

компонентов.
Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.
Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

5.4. Непрерывность защиты ИОД и ПДн

Защита ИОД и ПДн - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.
ИСПДн и ИОД должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.
Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ИОД и ПДн, то есть постановку задач по комплексной защите ИСПДни ИОД и реализацию мер обеспечения безопасности ИОД и ПДн на ранних стадиях разработки СЗИОД и ИСПДн в целом и ее системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

5.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИОД и ИСПДн и их системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ИО Д и ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.8. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ИОД и ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн и ИОД, для снижения вероятности возникновения негативных действий

связанных с человеческим фактором.
В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

5.10. Гибкость системы защиты ИОД и ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

5.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

5.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).
Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

5.13. 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 ИОД и ПДн.
СЗПДн и СЗИОД должны быть ориентированы на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

5.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ИОД и ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Учреждения.

5.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ИОД И ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.
Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

6. Меры, методы и средства обеспечения требуемого уровня защищенности Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИОД и ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных и информации ограниченного доступа.

6.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ИОД и ПДн, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ИОД и ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.
Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

6.3. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн и ИОД, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИОД и ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.
Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ИОД и ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Реализация Политики информационной безопасности ИОД и ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.
К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

— принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ИОД и ПДн, определение ответственных за ее реализацию;

—формулирование целей, постановка задач, определение направлений деятельности в области безопасности ИОД и ПДн;

—принятие решений по вопросам реализации программы безопасности, которые

рассматриваются на уровне Учреждения в целом;

— обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ИОД и ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ИОД и ПДн. Эти правила определяют:

— какова область применения политики безопасности ИОД и ПДн;

— каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ИОД и ПДн, а так же их установить ответственность;

— кто имеет права доступа к ИОД и ПДн;

— какими мерами и средствами обеспечивается защита ИОД и ПДн;

— какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

— предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

— определять коалиционные и иерархические принципы и методы разграничения доступа к ИОД и ПДн;

— определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

— организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

В организационные меры должны состоять из:

—регламента доступа в помещения с ИОД и ИСПДн;

— порядок допуска сотрудников к использованию ресурсов школы;

— регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

— регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

— инструкций пользователей ИСПДн (администратора ИСПДн, администратора без опасности, оператора ИСПДн);

— инструкция пользователя при возникновении внештатных ситуаций.

6.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита здания, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

6.5. Аппаратно-программные средства защиты ПДн

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

— средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

— средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн школы;

— средства обеспечения и контроля целостности программных и информационных ресурсов;

— средства оперативного контроля и регистрации событий безопасности;

— криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 5) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

— обеспечена физическая целостность всех компонент ИСПДн;

— каждый сотрудник (пользователь ИСПДн) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

— в ИСПДн школы разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;

— все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства школы;

— сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

— сотрудниками школы осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Контроль эффективности системы защиты ИОД и ИСПДн

Контроль эффективности СЗИОД и СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗИОД и СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так прогнозирование и превентивное реагирование на новые угрозы безопасности ИОД и ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ИОД и ПДн, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты ИОД и ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

8. Сферы ответственности за безопасность ИОД и ПДн

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель школы. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

Сфера ответственности руководителя включает следующие направления обеспечения безопасности ИОД и ПДн:

— планирование и реализация мер по обеспечению безопасности ИОД и ПДн;

— анализ угроз безопасности ИОД и ПДн;

— разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

— контроль защищенности ИТ инфраструктуры школы от угроз ИБ путем;

— обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

— предотвращение, выявление, реагирование и расследование нарушений безопасности ИОД и ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 3), с этими организациями должно быть заключено

«Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

9. Модель нарушителя безопасности

Под нарушителем в школе понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты (раздел 3).

Нарушители подразделяются по признаку принадлежности к ИОД и ИСПДн. Все нарушители делятся на две группы:

— внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

— внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10. Модель угроз безопасности

Для ИСПДн и ИОД школы выделяются следующие основные категории угроз безопасности персональных данных:

- Угрозы утечки информации по техническим каналам.
- Угрозы несанкционированного доступа к информации:
- Угрозы уничтожения, хищения аппаратных средств ИСПДн и ИОД носителей информации путем физического доступа к элементам ИСПДн и ИОД.
- Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).
- Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования СЗИОД и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
- Угрозы преднамеренных действий внутренних нарушителей.
- Угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности ИОД И персональных данных каждой ИСПДн.

11. Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИОД и ИСПДн в средствах обеспечения безопасности информации.

Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности ИОД и ПДн в ИСПДн позволит:

- оценить состояние безопасности информации ИОД и ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;
- разработать распорядительные и нормативно-методические документы применительно к ИОД и ИСПДн;
- провести классификацию и сертификацию ИОД и ИСПДн;
- провести организационно-режимные и технические мероприятия по обеспечению безопасности ИОД и ПДн в ИСПДн;
- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИОД и ИСПДн и создаст условия для ее дальнейшего совершенствования.

Приложение № 2
Утверждено приказом
директора гимназии
«Альбертина»
Ольшанская Е.В.
от 30.08.2019 г. №69/1

Политика гимназии «Альбертина» в отношении обработки персональных данных

1. Термины и определения

Термин/Сокращение	**Определение**
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
Доступ к персональным данным	Возможность получения персональных данных и их использования
Информационная система персональных данных	Совокупность содержащихся н базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Конфиденциальность персональных данных	Обязательное для выполнения Операторам и иными лицами, получившим доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федералы ним законом
Обезличивание персональных данных	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
Обработка персональных данных	Любое действие (операция) пли совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, храпение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
Персональные данные	Любая информация, относящийся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	Действия, направленные на получение персональных данных определенным кругом лиц или передачу персональных данных определенному кругу лиц
Распространение персональных данных	Действия, направленные па раскрытие персональных данных неопределенному кругу лиц

Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

2. Назначение и область применения

Настоящая Политика в отношении обработки персональных данных (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяет принципы обработки и обеспечения безопасности персональных данных в гимназии «Альбертина».

Действие настоящей Политики распространяется на все процессы обработки персональных данных в гимназии, как с использованием средств автоматизации, так и без использования таких средств, на всех работников гимназии, участвующих в таких процессах, а также на информационные системы гимназии, используемые в процессах обработки персональных данных.

3. Принципы обработки персональных данных

Обработка персональных данных в гимназии осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. В гимназии не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

При обработке персональных данных в гимназии обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. В гимназии принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

При определении состава обрабатываемых персональных данных субъектов персональных данных гимназии «Альбертина» руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

4. Условия обработки персональных данных

Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями гимназии определенными действующим законодательством Российской Федерации и договорными отношениями с гимназией.

Получение и обработка персональных данных в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», осуществляется только с письменного согласия субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается

согласие в форме электронного документа, подписанного электронной подписью.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются гимназией.

Гимназия «Альбертина» вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, не осуществляется.

Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.
Персональные данные субъекта могут быть получены от лица, не являющегося субъектом персональных данных, при условии предоставления в гимназию подтверждения наличия оснований, указанных в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных» или иных оснований, предусмотренных федеральным законодательством.

Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют сотрудники гимназии «Альбертина»» в соответствии с их должностными обязанностями.

Гимназия «Альбертина» не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные исключительно на автоматизированной обработке персональных данных субъекта.

5. Цели обработки персональных данных

В соответствии с принципами и условиями обработки персональных данных, в гимназии определены следующие цели обработки персональных данных:

- организация учебного процесса и контроль качества образования;
- учет и анализ успеваемости учащихся, организация информирования родителей (законных представителей) об успеваемости детей;
- выполнение обязательств, предусмотренных Трудовым договором;
- выполнение требований Трудового кодекса РФ и других нормативных актов РФ (в том числе предоставление персональных данных в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования);
- принятие решений и выполнение обязательств по обращениям граждан Российской Федерации в соответствии с законодательством РФ;
- оказание государственных услуг гражданам.

6. Особенности обработки персональных данных и их передачи третьим лицам

Обработка персональных данных в гимназии «Альбертина» осуществляется как с использованием средств автоматизации, так и без использования таких средств.

При обработке персональных данных гимназия осуществляет следующие действия с персональными данными: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Передача персональных данных субъектов персональных данных третьим лицам осуществляется в соответствии с требованиями действующего законодательства.

Гимназия «Альбертина» вправе поручить обработку персональных данных третьей стороне с

согласия субъекта персональных данных и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной договора, (далее - поручение). Третья сторона, осуществляющая обработку персональных данных по поручению гимназии, обязана соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», обеспечивая конфиденциальность и безопасность персональных данных при их обработке.

7. Права субъектов персональных данных

Субъект персональных данных вправе требовать от гимназии уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных ;
- правовые основания и цели обработки персональных данных;
- цели и применяемые способы обработки персональных данных;
- наименование и место нахождения гимназии «Альбертина» , сведения о лицах (за исключением работников гимназии, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с гимназией или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению гимназии, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

8. Реализованные меры обеспечения безопасности персональных данных

Гимназия «Альбертина» при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

К таким мерам, в частности, относятся:

- назначение лица, ответственного за организацию обработки персональных данных;
- осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- ознакомление работников гимназии с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных;
- издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства РФ;
- определение угроз безопасности персональных данных и необходимого уровня защищённости персональных данных, при их обработке в информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;
- осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

Приложение № 3
Утверждено
приказом директора гимназии
«Альбертина»
Ольшанская Е.В.
от 30.08.2019 г.
№69/1

Перечень
информации конфиденциального характера и персональных данных, обрабатываемых в гимназии «Альбертина»

№ п/п	Содержание сведений	Основание для включения в Перечень
1.	Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника и руководителя муниципальной образовательной организации (персональные данные).	Статья 85 Трудового кодекса Российской Федерации, утвержденного Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.
2.	Сведения, содержащиеся в записях актов о рождении, о смерти, о заключении брака, о расторжении брака, об установлении отцовства, о перемене имени, а также сведения о тайне усыновления (удочерения), за исключением сведений, разглашение которых осуществлено по воле усыновителя.	Статья 12 Федерального закона от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния».
3.	Персональные данные, внесенные в личные дела и документы учета муниципальных служащих. Сведения о доходах, имуществе и обязательствах имущественного характера гражданского служащего и руководителя муниципальной образовательной организации.	Статьи 14, 20 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

4.	Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц: страховой номер; фамилия, имя и отчество; фамилия, которая была у застрахованного лица при рождении; дата рождения; место рождения; пол; адрес постоянного места жительства; серия и номер паспорта или удостоверения личности, дата выдачи указанных документов; наименование выдавшего их органа; гражданство; номер телефона; периоды трудовой и иной общественно полезной деятельности, включаемые в общий стаж для назначения государственной трудовой пенсии, а также специальный стаж, связанный с особыми условиями труда, работой в районах Крайнего Севера и приравненных к ним местностях, выслугой лет, работой на территориях, подвергшихся радиоактивному	Статья 17 Федерального закона от 31 декабря 2002 г. № 198-ФЗ «Об индивидуальном (персонифицированном) учете в системе государственного пенсионного страхования».
	загрязнению; заработная плата или доход (за каждый месяц страхового стажа), на которые начислены страховые взносы в Пенсионный фонд Российской Федерации в соответствиис законодательством Российской Федерации; сумма заработка (за каждый месяц страхового стажа), который учитывается при назначении трудовой пенсии; сумма начисленных данному застрахованному лицу страховых взносов (за каждый месяц страхового стажа), включая страховые взносы за счет работодателя и страховые взносы самого застрахованного лица; периоды выплаты пособия по безработице; периоды военной службы и другой приравненной к ней службы, включаемые в общий трудовой стаж; сведения о назначении (перерасчете), индексации и начислении пенсии.	
5.	Материалы, полученные при рассмотрении жалоб, до вынесения окончательного решения по ней, сведения о частной жизни заявителя и других лиц без их письменного согласия.	Статья 28 Федерального конституционного закона от 26 февраля 1997 г. № 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации».
6.	Сведения, имеющие потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которым нет доступа на законном основании, обладатель которых принимает меры к охране их конфиденциальности.	Статья 139 Федерального закона от 30 ноября 1994 г. № 52-ФЗ «О введении части первой Гражданского кодекса Российской Федерации».
7.	Государственная статистическая отчетность по конкретному хозяйствующему субъекту.	Перечень служебной информации ограниченного распространения, Утвержденный Председателем Госкомстата России от 14 февраля 2002 г.

8.	Анкета ребенка и анкета гражданина относятся в соответствии с законодательством Российской Федерации в области информации, информатизации и защиты информации к конфиденциальной информации. Порядок доступа к конфиденциальной информации о детях, оставшихся без попечения родителей, и гражданах, желающихпринять детей на воспитание в свои семьи, определяется статьей 11 настоящего закона. Конфиденциальная информация о детях, оставшихся без попечения родителей, может быть использована региональными операторами и Федеральным оператором для создания производной информации о	Статья 8 Федерального закона от 16 апреля 2001 г. № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей».
	детях, оставшихся без попечения родителей, и распространения указанной информации посредством опубликования в средствах массовой информации или иным способом в целях информирования населения Российской Федерации о детях, оставшихся без попечения родителей и подлежащих устройству на воспитание в семьи. Использование производной информации о детях, оставшихся без попечения родителей, в коммерческих целях не допускается. При создании и распространении указанной информации должна быть исключена возможность идентификации личности ребенка, оставшегося без попечения родителей, его родителей и других его родственников.	
9.	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, за исключением информации, которая возникает при: - обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных; - организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.	Статья 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Приложение № 4
Утверждено
приказом директора гимназии
«Альбертина»
Ольшанская Е.В.
от 30.08.2019 г. №69/1

Положение
по обработке и защите персональных данных

1. Общие положения

1.1. Настоящее Положение по обработке и защите персональных данных (далее - Положение) разработано на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлений 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» и от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСТЭК России 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» и нормативно-методическими документами по вопросам безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. В Положении используются следующие термины:

персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и /или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

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

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет порядок и условия обработки ПДн в гимназии «Альбертина» (далее по тексту -краткое наименование), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиты ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения директором гимназии и действует бессрочно до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом директора гимназии.

2. Цели и задачи обработки ПДн

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с заявленными целями.

2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в различных целях.

2.3. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.4. Обработка ПДн сотрудников гимназии может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества гимназии.

2.5. Основными целями обработки ПДн является:

- обеспечение прав граждан, организаций, органов государственной власти и органов местного самоуправления на поиск, получение, передачу, производство и распространение информации;
- внедрение информационно-телекоммуникационных технологий в процедуры предоставления государственных услуг населению и организациям;
- исполнение муниципальных функций и муниципальных услуг;
- контроль за предоставлением государственных и муниципальных услуг в подведомственных учреждениях;
- заключение трудовых отношений с физическими лицами;
- выполнение договорных обязательств гимназии;
- выполнение функций удостоверяющего центра;
- соблюдение действующего законодательства Российской Федерации.

2.6. ИСПДн обеспечивают решение следующих задач:

- защита персональных данных;
- контроль использования персональных данных;
- воспрепятствование неправомерному доступу к персональным данным сотрудников гимназии;
- упрощение процедуры обработки персональных данных, сокращение времени на их обработку;
- объединение в едином хранилище данных, предоставленных субъектами;
- возможности обмена персональными данными с использованием информационных систем связи.

3. Персональные данные, обрабатываемые в ИСПДн

3.1. В ИСПДн обрабатываются ПДн следующих субъектов ПДн:

- сотрудников гимназии
- лиц, связанных с сотрудниками (дети, в отношении которых выплачиваются алименты, жены, и т.д.);
- руководителей муниципальных образовательных организаций;
- клиентов (потребители услуг гимназии «Альбертина»;
- клиентов организаций, контрагентов гимназии «Альбертина»;
- Выше указанный перечень может пересматриваться по мере необходимости.

3.2. Персональные данные субъектов ПДн включают:

- специальные категории персональных данных, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- биометрические персональные данные, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность;
- общедоступные персональные данные, которые получены только из общедоступных источников персональных данных;
- иные категории персональных данных.

3.3. Полные списки обрабатываемых ПДн формируются в перечне ПДн, подлежащих защите в ИСПДн гимназии (приложение № 3 к приказу «О мерах по защите персональных данных при их обработке в информационных системах гимназии «Альбертина»;

4. Доступ к ПДн

4.1. Сотрудники гимназии «Альбертина, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к необходимым категориям ПДн на срок выполнения ими соответствующих должностных обязанностей в соответствии с утвержденным директором гимназии перечнем лиц, допущенных к работе с ПДн.

4.2. Список лиц, имеющих доступ к ПДн для информационной системы, должен поддерживаться в актуальном состоянии.

4.3. гимназия «Альбертина» установлен разрешительный порядок доступа к ПДн. Сотрудникам предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании приказа директора гимназии.

4.4. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником гимназии «Альбертина» по согласованию с директором гимназии.

4.5. Доступ к ПДн третьих лиц, не являющихся сотрудниками гимназии без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства. Предоставление информации по запросу или требованию органа исполнительной власти осуществляется с ведома директора гимназии.

4.6. В случае если сотруднику сторонней организации необходим доступ к ПДн гимназии необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ПДн и обязанность сторонней организации и ее сотрудников по соблюдению требований действующего законодательства Российской Федерации в области защиты ПДн. Кроме того, в случае доступа к ПДн лиц, не являющихся сотрудниками гимназии, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного гимназии с субъектом ПДн.

4.7. Доступ сотрудника гимназии «Альбертина» к ПДн прекращается с даты завершения трудовых отношений либо с даты изменения должностных обязанностей сотрудника и (или) исключения его из списка лиц, имеющих право доступа к ПДн. В случае увольнения все находившиеся в распоряжении сотрудника в соответствии с его должностными обязанностями носители, содержащие ПДн, передаются руководителям структурных подразделений.

5. Основные требования по защите ПДн

5.1. При обработке ПДн в информационных системах гимназии «Альбертина» должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и(или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа;
- постоянный контроль обеспечения уровня защищенности ПДн.

5.2. гимназии «Альбертина» обязана принимать необходимые правовые, организационные и технические меры для обеспечения безопасности ПДн.

5.3. На основании нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» для установления требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн в Комитете разрабатывается комплект организационно распорядительной документации и модель угроз безопасности ПДн при их обработке в ИСПДн.

5.4. В соответствии с 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» членами комиссии по обследованию режимных помещений, категорированию и классификации объектов информатизации гимназии «Альбертина» проводится классификация ИСПДн.

5.5. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн, должны быть под роспись ознакомлены с требованиями настоящего Положения, а также должны подписать обязательство о неразглашении конфиденциальной информации (приложения 1 и 2 к Положению по обработке и защите персональных данных).

5.6. Сотрудники гимназии «Альбертина» обязаны незамедлительно сообщать руководителям структурных подразделений об утрате или недостаче носителей информации, содержащих ПДн; о причинах и условиях возможной утечки ПДн; о попытках посторонних лиц получить от сотрудника ПДн, обрабатываемые в гимназии.

6. Согласие на обработку ПДн

6.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, по своей воле и в своих интересах. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством Российской Федерации.

6.2. Получение письменного согласия на обработку ПДн осуществляется сотрудником при получении ПДн от субъекта ПДн путем оформления письменного согласия по форме (приложении 3 и 4 к Положению по обработке и защите персональных данных).

7. Права субъекта в отношении ПДн, обрабатываемых в гимназии «Альбертина»

7.1. Субъект ПДн имеет право:

- получать информацию, касающуюся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Перечень сведений и порядок получения сведений предусмотрен действующим законодательством Российской Федерации. Факты обращения субъектов ПДн о выполнении их законных прав фиксируются в журнале (приложение 5 к Положению по обработке и защите персональных данных);
- требовать от гимназии уточнения его ПДн, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав;
- давать предварительное письменное согласие при обработке ПДн в целях продвижения

товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

- давать предварительное письменное согласие при принятии гимназией исключительно в процессе автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;
- заявлять возражения на решения гимназии в процессе исключительно автоматизированной обработки ПДн и на возможные юридические последствия таких решений;
- обжаловать действия или бездействие гимназии в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

8. Права и обязанности гимназии «Альбертина»

8.1. Гимназия «Альбертина» вправе:

8.1.1. Поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта.

8.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве Российской Федерации.

8.1.3. Отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством Российской Федерации. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на гимназии.

8.1.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей гимназии, предусмотренных законодательством Российской Федерации.

8.2. Гимназия «Альбертина» обязана:

8.2.1. До начала обработки ПДн уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.2.2. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», гимназия «Альбертина» обязана обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление,изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.2.3. При получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено Федеральным законом.

8.2.4. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований обработки ПДн без согласия субъекта ПДн.

8.2.5. До начала осуществления трансграничной передачи ПДн убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн.

8.2.6. Прекратить по требованию субъекта ПДн обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации.

8.2.7. Разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

8.2.8. При сборе ПДн предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством Российской Федерации.

8.3. Если предоставление ПДн является обязательным в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», оно обязано разъяснить субъекту ПДн юридические последствия его отказа предоставить ПДн.

8.2.9. Если ПДн получены не от субъекта ПДн, гимназия, за исключением случаев,

предусмотренных законодательством Российской Федерации, до начала обработки таких ПДн должна предоставить субъекту ПДн следующую информацию:

- наименование и адрес гимназии «Альбертина»;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные права субъекта персональных данных;
- источник получения ПДн.

8.2.10. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей гимназии «Альбертина», предусмотренных законодательством Российской Федерации.

8.2.11. Представить документы и локальные акты, предусмотренные законодательством Российской Федерации, и (или) иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей гимназии «Альбертина по запросу уполномоченного органа по защите прав субъектов ПДн.

8.2.12. При обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

8.2.13. Назначить лицо, ответственное за организацию обработки ПДн.

9. Порядок обработки и защиты ПДн

9.1. Обеспечение конфиденциальности ПДн, обрабатывающихся в гимназии , является обязательным требованием для всех лиц, которым ПДн стали известны.

9.2. Сотрудники гимназии «Альбертина», осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

9.3. В случае нарушения установленного порядка обработки ПДн сотрудники гимназии «Альбертина» несут ответственность в соответствии с разделом 11 настоящего Положения.

9.4. ПДн субъектов на бумажных носителях, обрабатываемые гимназией, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн. Право допуска сотрудников к неавтоматизированным ИСПДн определяется распоряжением директора. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места сотрудники, осуществляющие обработку ПДн, должны убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется их восстановление (по возможности).

9.5. Места хранения документов, содержащих ПДн:

9.5.1. ПДн клиентов гимназии «Альбертина» (договоры, акты, соглашения, анкеты, копии паспортов и подобные документы, содержащие ПДн клиентов, носители информации (флэш-карты, CD-диски, и т.п.) хранятся в сейфах, размещаются на полках и запираются на ключ. Ответственное лицо, осуществляющее контроль, определяется распоряжением руководителя.

9.5.2. ПДн сотрудников гимназии «Альбертина»: документы, носители информации (флэш-карты, CD-диски и т.п.) - хранятся в сейфах и запираются на ключ.

9.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок не более одного рабочего дня.

9.7. При работе с программными средствами информационной системы гимназии «Альбертина , реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

9.8. При получении ПДн сотрудником гимназии, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника, иного лица, в обязательном порядке проводится проверка достоверности ПДн. Ввод ПДн, полученных в информационную систему осуществляется сотрудниками, имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

9.9. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствии с постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9.10. При неавтоматизированной обработке различных категорий ПДн должен использоваться

отдельный материальный носитель для каждой категории ПДн.

9.11. При неавтоматизированной обработке ПДн на бумажных носителях:

9.11.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых различны;

9.11.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

9.12. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы), должны соблюдаться следующие условия:

9.12.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес гимназии «Альбертина», фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПДн;

9.12.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, при необходимости получения письменного согласия на обработку ПДн;

9.12.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн;

9.12.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых различны.

9.13. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

9.14. Случаи уничтожения, блокирования и уточнения ПДн:

9.15. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

9.16. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, если это не допускается техническими особенностями материального носителя — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

9.17. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

9.17.1. ПДн на бумажных носителях уничтожаются путем использования шредера (уничтожители документов), установленного в помещениях гимназии «Альбертина».

9.17.2. ПДн, размещенные в памяти ПЭВМ удаляются с использованием программного обеспечения гарантированного удаления данных, прошедших сертификацию в установленном порядке ФСТЭК России.

9.17.3. ПДн, размещенные на флэш-карте, CD-диске, ином носителе информации, уничтожаются путем удаления файла с носителя (форматирования) или путем нарушения работоспособности флэш-карты или CD-диска.

9.18. Об уничтожении носителя информации составляется акт об уничтожении ПДн (приложение 6 к Положению по обработке и защите персональных данных).

9.19. По окончании рабочего дня сотрудники гимназии «Альбертина» закрывают в служебных помещениях окна, запирают данные помещения и включают сигнализацию (при наличии).

9.20. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

9.21. Уборка помещений и обслуживание технических средств ИСПДн должны осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

9.22. В обязанности администраторов ИСПДн входит управление учетными записями пользователей, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных,

а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн. Кроме того, в их обязанности входит обеспечение соответствия порядка обработки и безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемым к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных Федеральным законодательством.

9.23. В обязанности администраторов ИСПДн входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

9.24. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения представляющих угрозу для безопасности ПДн полномочий у одного лица не рекомендуется назначать администраторами ИСПДн их пользователей.

9.25. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях,

---

ознакомление с которыми подтверждается подписью назначаемых сотрудников.

9.26. Организация внутреннего контроля процесса обработки ПДн в гимназии «Альбертина» осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

9.27. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

9.27.1. Обеспечение соблюдения сотрудниками гимназии «Альбертина» требований настоящего Положения и нормативных правовых актов, регулирующих защиту ПДн.

9.27.2. Оценка компетентности персонала, задействованного в обработке ПДн.

9.27.3. Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

9.27.4. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

9.27.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений в процессе обработки ПДн и в работе технических средств ИСПДн.

9.27.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий.

9.27.7. Осуществление внутреннего контроля исполнения рекомендаций и указаний по устранению нарушений.

9.28. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

10. Передача (предоставление) персональных данных

10.1. При предоставлении ПДн или предоставлении доступа к ним третьей стороне должны выполняться на основании:

- действующего законодательства Российской Федерации;
- договора, существенным условием которого является обеспечение третьей стороной конфиденциальности ПДн и безопасности персональных данных при их обработке;
- письменного согласия субъекта ПДн на передачу его ПДн третьей стороне, за исключением случаев, предусмотренных законодательством Российской Федерации.

10.2. Трансграничная передача ПДн на территорию иностранных государств может осуществляться в соответствии с положениями ст. 12 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных в случаях:

- предусмотренных международными договорами Российской Федерации;
- предусмотренных законодательством Российской Федерации, если это необходимо в целях

защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

- исполнения договора, стороной которого является субъект ПДн;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

10.3. В целях информационного обеспечения в гимназии «Альбертина» могут создаваться специализированные справочники (телефонные, адресные книги и др.), содержащие персональные данные, к которым с письменного согласия субъекта ПДн может предоставляться доступ неограниченному кругу лиц.

10.4. Сведения о субъекте ПДн должны быть незамедлительно исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

11. Ответственность за нарушение законодательства в области обработки персональных данных

11.1. Директор и сотрудники допущенные к обработке ПДн несут ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

11.2. Сотрудники гимназии «Альбертина» несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

11.3. Сотрудник гимназии «Альбертина» может быть привлечен к ответственности в случаях:

11.3.1. Умышленного или неосторожного раскрытия ПДн.

11.3.2. Утраты материальных носителей ПДн.

11.3.3. Нарушения требований настоящего Положения и других нормативных документов гимназии «Альбертина» в части вопросов доступа и работы с ПДн.

11.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения его сотрудникам, клиентам и контрагентам материального или морального ущерба виновные лица несут уголовную, административную, дисциплинарную, гражданско-правовую и материальную ответственность, предусмотренную законодательством Российской Федерации.

Приложение 1
к приложению по обработке и защите
персональных данных
утверждено приказом директора
от 30.08.2019 г. № 69/1

Обязательство
о неразглашении конфиденциальной информации

Я, _____
(фамилия, имя, отчество)

в качестве сотрудника гимназии «Альбертина», в период трудовых (служебных) отношений с гимназией (его правопреемником) и в течение 5 лет после прекращения работы в гимназии, в соответствии с трудовым договором ,заключенного между мной и гимназией «Альбертина» от «___» _____ года, а также соответствующими положениями по обеспечению защиты и охраны конфиденциальной информации, действующими в гимназии, обязуюсь:

- не разглашать конфиденциальную информацию гимназии «Альбертина», которая мне будут доверена или станет известна по работе (службе);
- не передавать третьим лицам и не раскрывать публично конфиденциальную информацию гимназии «Альбертина» без его согласия;
- выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению сохранности конфиденциальной информации гимназии «Альбертина»;
- в случае попытки посторонних лиц получить от меня конфиденциальную информацию о гимназии «Альбертина» немедленно сообщить руководителям структурных подразделений;
- сохранять конфиденциальную информацию тех организаций, с которыми гимназии «Альбертина» имеются деловые отношения;
- не использовать знание конфиденциальной информации гимназии «Альбертина» для занятий любой деятельностью, которая может нанести ущерб гимназии;
- в случае моего увольнения все носители конфиденциальной информации гимназии «Альбертина» (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в передать администратору;
- об утрате или недостаче носителей конфиденциальной информации, личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации гимназии «Альбертина», а также о причинах и условиях возможной утечки сведений немедленно сообщать директору..

Я предупрежден, что в случае невыполнения любого из пунктов настоящего обязательства могу быть уволен из гимназии «Альбертина». До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности конфиденциальной информации гимназии «Альбертина».

Мне известно, что нарушение этих положений может повлечь уголовную, административную, дисциплинарную, гражданско-правовую и материальную ответственность, предусмотренную законодательством Российской Федерации.

С Перечнем информации конфиденциального характера и персональных данных, обрабатываемых в гимназии ознакомлен(а).

_____ _____ /
подпись) (расшифровка подписи)

« »_____20___г.

Приказ№69/1 от 30.08.2019 и «Альбертина» подтверждает, что данные Вами обязательства не ограничивают Ваших прав на интеллектуальную собственность. Об окончании срока действия обязательства руководство гимназии «Альбертина» уведомит Вас заблаговременно в письменной форме.

_____ / _____
подпись) (расшифровка подписи)

«____»_____20____г.

Обязательства составлены в двух экземплярах. Один экземпляр находится у сотрудника, второй хранится в гимназии «Альбертина» в качестве приложения к трудовому договору или личному делу сотрудника.

Один экземпляр обязательств получил.

_____ / _____
(подпись) (расшифровка подписи)

«____»_____20____

Приложение 2
к приложению по обработке и защите
персональных данных
утверждено приказом директора
от 30.08.2019 г. № 246

Типовое обязательство сотрудника, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных (служебных) обязанностей

Я, _____ _____
(Ф.И.О.)

_____
(должность)

паспорт серия _____ № _____ , выдан _____
_____

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных (служебных) обязанностей, в случае освобождения меня от замещаемой должности и увольнения, прекращения (расторжения) трудового договора.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника, или их утраты, а также за несоблюдение Федерального закона от 27 июля 2006 г. № 152-ФЗ я несу ответственность в соответствии со статьями 137, 140, 272 «Уголовного кодекса Российской Федерации», статьями 13.11, 13.12, 13.14 «Кодекса об Административных правонарушениях Российской Федерации», статьями 81 и 90 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ.

С Положением об обработке и защите персональных данных в гимназии «Альбертина» ознакомлен(а).

_____ _____
(должность) (подпись) (ф.и.о.)

Приложение 3
к приложению по обработке и защите
персональных данных
утверждено приказом директора
от 30.08.2019 г. № 69/1

Согласие
сотрудника на обработку персональных данных

Я,_____,
(Ф.И.О. сотрудника)

зарегистрированный(ая) по адресу:_____

паспорт: серия_____, №_____, выдан _____
_____, в соответствии со ст. 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» даю согласие на обработку своих персональных данных гимназии «Альбертина», расположенному по адресу: Калининградская область, г. Калининград, ул. Ялтинская, д. 126, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона № 152-ФЗ со всеми данными, которые находятся в распоряжении ГКОУ ВО
Гимназии «Альбертина» с целью начисления заработной платы, исчисления и уплаты, предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления органом установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд Российской Федерации, сведений подоходного налога в ФНС Российской Федерации, сведений в ФСС Российской Федерации, предоставлять сведения в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, а также предоставлять сведения в случаях, предусмотренных Федеральными законами и иными нормативно-правовыми актами, следующих моих персональных данных:

1. Перечень персональных данных, на обработку которых дается согласие:

- фамилия, имя, отчество (в т.ч. предыдущие), паспортные данные или данные документа, удостоверяющего личность, дата рождения, место рождения, гражданство, отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения, данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке, данные документов о подтверждении специальных знаний, данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях, знание иностранных языков, семейное положение и данные о составе и членах семьи, сведения о социальных льготах, пенсионном обеспечении и страховании, данные документов об инвалидности (при наличии), данные медицинского заключения (при необходимости), стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
- должность, квалификационный уровень, сведения о заработной плате (доходах), банковских счетах, картах, адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства, номер телефона (стационарный домашний, мобильный),
- данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН), данные страхового свидетельства государственного пенсионного страхования, данные страхового медицинского полиса обязательного страхования граждан.
- данные биометрические.
- данные антропометрические.

2. Перечень действий, на совершение которых дается согласие:

Разрешаю гимназии «Альбертина» производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных. Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

1. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данных между гимназии «Альбертина» и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

2. Сроки обработки и хранения персональных данных:

Обработка персональных данных, прекращается по истечении семи лет после окончания трудового договора сотрудника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные сотрудников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует с « ____»_____20 _ г.

_____/_____«_____»_____20 _ г.

(подпись) (ф.и.о. сотрудника) (дата подписи)

Приложение 4
к приложению по обработке и защите
персональных данных
утверждено приказом директора
от 30.08.2019 г. № 69/1

Форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый(ая), _____
(Имя, отчество субъекта персональных данных)

В соответствии с требованиями Федерального закона от 27 июля 2006г. № 152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена

_____
(Реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные, гимназия «Альбертина» не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:

_____
(Перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

- на получение сведений о гимназии «Альбертина» о месте его нахождения;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;
- на обжалование действия или бездействия гимназии «Альбертина» в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____ / _____
(Дата) (Фамилия, инициалы и подпись сотрудника)

Приложение 5
к приложению по обработке и защите
персональных данных
утверждено приказом директора
от 30.08.2019 г. № 246

Журнал
учета обращений субъектов персональных данных о выполнении их законных прав
гимназии «Альбертина»

Журнал начат « » 20 г.	Журнал завершен « » 20 г.
Должность	Должность
/ /	/ /

№	Дата обращения	ФИО посетителя	Вид обращения и его краткое содержание	Какое принято решение	Кто принимал (ФИО, должность)	Примечания

Акт
об уничтожении персональных данных

Председатель комиссии: _____
(ФИО, должность)

Члены комиссии:
1. _____
(ФИО, должность)

2. _____
(ФИО, должность)

составили настоящий акт в том, что «_____»_____20____г. произведено уничтожение персональных данных (конфиденциальной информации), находящейся на

(наименование ИС по утвержденной конфигурации, Ф.И.О. ответственного пользователя ИС, заводской или учетный номер системного блока ИС, носителя информации, тип удаляемых персональных данных (конфиденциальной информации), способ уничтожения информации).

Председатель комиссии:

(должность) _____ (подпись, ФИО)

Члены комиссии:

(должность) (подпись, ФИО)

_____ _____
(должность) (подпись, ФИО)

_____ _____
(должность) (подпись, ФИО)

_____ _____
(должность) (подпись, ФИО)

Приложение № 5
Утверждено приказом директор
гимназии
от 30.08.2019 г. № 69/1

Положение
о порядке учета, хранения и обращения со съемными носителями персональных данных

1. Общие положения

Настоящее Положение о порядке учета, хранения и обращения со съемными носителями персональных данных (далее Положение об учете съемных носителей ПДн) разработано в соответствии с Федеральным законом № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации», 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», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Действие настоящего Положения об учете съемных носителей ПДн распространяется на всех сотрудников гимназии «Альбертина», подрядчиков и представителей третьей стороны.

2. Основные термины, сокращения и определения

Администратор информационной системы - технический специалист, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (ПО) и оборудования вычислительной техники.

АРМ - автоматизированное рабочее место пользователя (персональный компьютер (ПК) с прикладным ПО) для выполнения определенной производственной задачи.

ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС - информационная система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

Машинный носитель информации - материальный носитель, используемый для хранения и передачи электронной информации.

ПК - персональный компьютер.

ПО - программное обеспечение вычислительной техники.

ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

Пользователь - сотрудник гимназии «Альбертина», использующий ПК и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей информации

3.1. Под использованием машинных носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки ПДн и обмена информацией между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных машинных носителей информации, которые являются собственностью гимназии «Альбертина» и подвергаются регулярной ревизии и контролю.

3.3. К машинным носителям ПДн предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Машинные носители конфиденциальной информации предоставляются по инициативе заместителей руководителя гимназии «Альбертина» в случаях:

- необходимости выполнения новым Пользователем своих должностных обязанностей;
- возникновения у Пользователя производственной необходимости.

4. Порядок учета, хранения и обращения со съемными машинными носителями персональных данных

4.1. Все находящиеся на хранении и в обращении съемные машинные носители с ПДн подлежат учету.

4.2. Каждый съемный машинный носитель ПДн должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдача съемных машинных носителей ПДн осуществляются уполномоченным сотрудником гимназии «Альбертина», назначенными соответствующими приказами. Факт выдачи съемного машинного носителя исполнителю фиксируется в журнале учета съемных машинных носителей ПДн (приложение 1 к Положению о порядке учета, хранения и обращения со съемными носителями персональных данных).

4.4. Пользователи получают учтенные съемные машинные носители ПДн от уполномоченного сотрудника гимназии «Альбертина» на время выполнения соответствующих работ, по окончании которых данные носители подлежат возврату. Факты выдачи и возврата съемных носителей ПДн фиксируются в Журнале.

4.5. При использовании Пользователями машинных носителей ПДн необходимо:

- соблюдать требования настоящего Положения;
- использовать машинные носители информации ПДн исключительно для выполнения своих служебных обязанностей;
- ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения;
- бережно относится к машинным носителям ПДн;
- обеспечивать безопасность машинных носителей ПДн информации всеми возможными способами;
- извещать администраторов ИС о фактах утраты (кражи) машинных носителей ПДн.

4.6. При использовании машинных носителей ПДн запрещается:

1. использовать их в личных целях;

2. передавать их другим лицам (за исключением администраторов ИС);

3. хранить их вместе с общедоступными данными на рабочих столах либо оставлять без присмотра или передавать на хранение другим лицам;

4. выносить их из служебных помещений для работы на дому.

4.7. Любое взаимодействие (обработка, прием и передача информации), инициированное сотрудником между ИС и неучтенными носителями информации, рассматривается как несанкционированное. Администратор ИС оставляет за собой право блокировать или ограничивать использование машинных носителей ПДн.

4.8. В случае выявления фактов несанкционированного и (или) нецелевого использования машинных носителей персональных данных инициируется служебная проверка, проводимая комиссией, назначаемой руководителем гимназии «Альбертина». По результатам служебной проверки составляется акт расследования инцидента (приложение 2 к Положению о порядке учета, хранения и обращения со съемными носителями персональных данных) и передается руководителю структурного подразделения для принятия мер в соответствии с действующим законодательством Российской Федерации.

4.9. Информация, хранящаяся на машинных носителях ПДн, подлежит обязательной проверке на предмет отсутствия вредоносного программного обеспечения.

4.10. При отправке или передаче ПДн адресатам на съемные машинные носители записываются только предназначенные им данные. Отправка ПДн адресатам на съемных машинных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.11. Вынос съемных машинных носителей ПДн для непосредственной передачи адресату осуществляется только с письменного разрешения директора гимназии.

4.12. В случае утраты или несанкционированного уничтожения съемных машинных носителей ПДн либо разглашения содержащихся на них сведений немедленно ставится в известность директор. По факту утраты составляется акт расследования инцидента и в журналы учета съемных носителей ПДн вносятся соответствующие отметки.

4.13. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

4.14. В случае увольнения или перевода сотрудника предоставленные ему машинные носители ПДн необходимо сдать лицу, ответственному за информационную безопасность. Лицо, ответственное за информационную безопасность, должно предпринять одно из следующих мер, направленных на невозможность несанкционированного доступа хранящейся на нем защищаемой информации:

- уничтожить машинные носители ПДн с составлением соответствующего акта об уничтожении;
- удалить информацию, содержащуюся на машинных носителях ПДн, с помощью специального программного обеспечения сертифицированного ФСТЭК России с составлением соответствующего акта об уничтожении (очистке);
- сдать в архив или перерегистрировать машинные носители ПДн на структурное подразделение и сделать соответствующую отметку в Журнале.

5. Ответственность

Пользователи и администраторы информационной системы, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 1
к Положению о порядке учета, хранения и обращения со съемными носителями персональных данных, утверждено приказом директора от 30.08.2019 г. № 246

Ж У Р Н А Л
учета машинных носителей персональных данных ИСПДН
гимназии «Альбертина»

Журнал начат «____» 20 г.	Журнал завершен «____» 20 г.
Должность	Должность
/	/
/	/

№ п/п	№Вид материального носителя	Учетный номер	Дата постановки на учет	Ответственное лицо	Подпись ответственного лица	Дата выдачи	Номер акта об уничтожении

Приложение 2
к Положению о порядке учета, хранения и обращения со
съемными носителями персональных данных, утверждено
приказом школы от 30.08.2019 г. № 69/1

Акт
расследования инцидента

1. Состав комиссии расследования инцидента:
Председатель комиссии: _____
(ФИО, должность)

Члены комиссии:
1. _____
(ФИО, должность)

2. _____
(ФИО, должность)

2. Характеристика организации.
Указать, были ли ранее аналогичные инциденты, отразить, как соблюдались требования по информационной безопасности.
3. Квалификация обслуживающего персонала, руководителей и специалистов объекта, ответственных лиц, причастных к инциденту.
4. Обстоятельства инцидента, допущенные нарушения требований законодательства.
Описываются обстоятельства инцидента и сценарий его развития, указывается, какие факторы привели к инциденту и его последствиям (нарушение законодательства, правил и др.).
5. Мероприятия по локализации и устранению причин инцидента.
Излагаются меры по ликвидации последствий инцидента и предупреждению подобных инцидентов, сроки выполнения мероприятий по устранению причин инцидента.
6. Заключение о лицах, ответственных за инцидент.
В этом разделе указываются лица, допустившие нарушения норм и правил безопасности, которые привели к инциденту. При этом указывается, какие требования нормативных документов не выполнены или нарушены конкретным лицом, исполнителем работ.
7. Ущерб от инцидента.

Председатель комиссии: _____
(должность) _____
(подпись, ФИО)

Члены комиссии: _____

(должность) (подпись, ФИО)

_____ _____

(должность) (подпись, ФИО)

Приложение № 6
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Положение
о разграничении прав доступа к обрабатываемым персональным данным

1. Общие положения

1.1. В данном документе представлен список лиц, ответственных за обработку ПДн в ИСПДн ГКОУ гимназии «Альбертина», а также их уровень прав доступа к обрабатываемым персональным данным.

1.2. Разграничение прав осуществляется на основании законодательства Российской Федерации, исходя из характера и режима обработки ПДн в ИСПДн.

1.3. Список должностных лиц, ответственных за обработку ПДн, а также их уровень прав доступа в ИСПДн представлен в таблице:

Группа	Уровень доступа к ПДн	Разрешенные действия с ПДн	Должность
Администратор ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	Сбор, систематизация, накопление, хранение, уточнение, использование, уничтожение.	Лицо назначенное приказом директора
Администратор безопасности ИСПДн	Обладает правами администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных). Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	Сбор, систематизация, накопление, хранение, уточнение, использование, уничтожение.	Лицо назначенное приказом директора
Пользователи ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	Сбор, систематизация, накопление, хранение, уточнение, использование, уничтожение.	Сотрудники школы согласно должностных обязанностей
Пользователи ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	Использование.	Сотрудники школы согласно должностных обязанностей

Приложение № 7
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Правила
рассмотрения запросов субъектов персональных данных
или их представителей

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила рассмотрения запросов) определяются порядок учета (регистрации), рассмотрения запросов субъектов ПДн или их представителей (далее - запросы).

2. Настоящие Правила рассмотрения запросов разработаны в соответствии Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Трудовым кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ, постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 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».

3. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн в школе;
- правовые основания и цели обработки ПДн;
- цели и применяемые в школе способы обработки ПДн;
- наименование и место нахождения в школе сведений о лицах (за исключением сотрудников школы), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн.
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- сроки обработки и хранения ПДн;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по ее поручению, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии со статьей 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5. Субъект ПДн вправе требовать от школы уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6. Сведения должны быть предоставлены субъекту ПДн в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

7. Сведения, предоставляются субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с школы (номер договора, дата заключения договора, условное словесное обозначение и(или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн школой, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9. Рассмотрение запросов является служебной обязанностью начальника, заместителей начальника и уполномоченных должностных лиц, в чьи обязанности входит обработка персональных данных (приложение 1 к Правилам рассмотрения запросов субъектов персональных данных и их представителей).

10. Должностные школы обеспечивают:

- объективное, всестороннее и своевременное рассмотрения запроса;
- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов ПДн;
- направление письменных ответов по существу запроса.

11. Ведение делопроизводства по запросам осуществляется специально назначенным сотрудником школы.

12. Все поступившие запросы регистрируются в день их поступления. На запросе проставляется штамп, в котором указываются входящий номер и дата регистрации.

13. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае если сведения, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Субъект ПДн вправе обратиться повторно в школу или направить повторный запрос в целях получения сведений, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в настоящем пункте, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

14. Школа вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Такой отказ должен быть мотивированным.

15. Прошедшие регистрацию запросы в тот же день докладываются руководителю школы, либо лицу, его заменяющему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

16. Руководитель школы, его заместители и другие должностные лица при рассмотрении и разрешении запроса обязаны:

- внимательно изучить существо запроса, в случае необходимости истребовать дополнительные материалы или направить сотрудников для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями

вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о ПДн Российской Федерации;

- принимать по ним законные, обоснованные и мотивир ованные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять порядок обжалования принятого решения.

17. Школа обязана сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

18. В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя уполномоченные должностные лица школы обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иного Федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

19. Школа обязана предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн.

20. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, уполномоченные должностные лица школы обязаны внести в них необходимые изменения.

21. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица школы обязаны уничтожить такие ПДн.

22. Школа обязана уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

23. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов персональных данных уполномоченные должностные лица школы обязаны осуществить блокирование (уведомление о блокировании ПДн) неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн с момента такого обращения или получения указанного запроса на период проверки.

24. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн уполномоченные должностные лица школы обязаны осуществить блокирование ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

25. В случае подтверждения факта неточности ПДн уполномоченные должностные лица школы на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязаны уточнить ПДн в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

26. В случае выявления неправомерной обработки ПДн уполномоченные должностные лица школы в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку ПДн. В случае если обеспечить правомерность обработки

ПДн невозможно, уполномоченные должностные лица школы в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязаны уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн школа обязана уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

27. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

28. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения сотрудником школы действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация незамедлительно докладываются руководителю школы.

29. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

30. Ответы на запросы печатаются на бланке установленной формы и регистрируются за теми же номерами, что и запросы.

31. Руководитель школы осуществляет непосредственный контроль соблюдения установленного законодательства Российской Федерации и настоящими Правилами рассмотрения запросов.

32. Руководитель школы осуществляет контроль работы с запросами и организацией их приема как лично, так и через своих заместителей. На контроль берутся все запросы.

33. Контролю подлежат: сроки исполнения поручений по запросам, полнота рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

34. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к Правилам рассмотрения запросов субъектов персональных данных и их представителей, утверждено приказом школы от 30.08.2019 г. № 69/1

Перечень
должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

гимназии «Альбертина»

№ п/п	Наименование должности	Категория персональных данных
1.	Директор гимназии	ПДн, обрабатываемые в связи с реализацией трудовых отношений, а также в связи с оказанием муниципальных услуг и осуществлением государственных функций. ПДн граждан, обрабатываемые в целях оказания муниципальных услуг и осуществлением муниципальных функций. ПДн граждан, обрабатываемые в целях оказания муниципальных услуг и исполнения муниципальных функций. ПДн гражданских служащих и сотрудников структурных подразделений.
2.	Заместители директора гимназии	
3.		
4.		
5.	Уполномоченные должностные лица, в чьи обязанности входит обработка персональных данных	

Приложение № 8
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила контроля) в гимназии «Альбертина» (далее - гимназия) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила контроля разработаны на основании Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

1.3. Школа использует информационные системы персональных данных (далее - ИСПДн) для выполнения основных целей и задач обработки ПДн, указанных в пункте 2 Положения по обработке и защите персональных данных.

1.4. Пользователями ИСПДн (далее - Пользователь) являются сотрудники школы, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющие доступ к аппаратным средствам, программному обеспечению (далее - ПО), данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.5. Контрольные мероприятия по обеспечению уровня защищенности ПДн и соблюдению условий использования СЗИ, а также соблюдению требований законодательства Российской Федерации по обработке ПДн в ИСПДн школы проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в школе и действующего законодательства Российской Федерации в области обработки и защиты ПДн;
- оценка уровня осведомленности и знаний сотрудников школы в области обработки и защиты ПДн;
- оценка обоснованности и эффективности применяемых мер и средств защиты ПДн.

Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в Школе разделяются на следующие виды:

2.

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся администратором ИС в соответствии с утвержденным планом (приложение 1 к правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных, утверждено руководителем школы) проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в школе.

2.3. Плановые контрольные мероприятия периодически проводятся постоянной комиссией в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты ПДн ИСПДн школы.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя школы.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает план внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий;
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в журнале учета событий информационной безопасности (приложение 2 к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий ответственное лицо или члены комиссии разрабатывают отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение руководителя школы.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки ПДн требованиям к защите ПДн в школе (приложение 3 к Правилам осуществления внутреннего контроля соответствия обработки персональным данным требованиям к защите персональных данных).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к

проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности ПДн информационных систем ПДн.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий в зависимости от целей мероприятий могут выполняться следующие проверки:

- соответствия полномочий Пользователя правилам доступа;
- соблюдения Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн;
- соблюдения администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в школе;
- соблюдения порядка доступа сотрудников в помещения школы, где ведется обработка персональных данных;
- знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- знание администраторами ИСПДн инструкций и регламентов по обеспечению безопасности информации в школе;
- порядок и условия применения средств защиты информации;
- состояние учета машинных носителей ПДн;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
- проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;
-технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты

Приложение 1
к Правилам осуществления внутреннего контроля соответствия
обработки персональным данным требованиям к защите
персональных данных, утверждено приказом директора
от 30.08.2019 г. № 69/1

План
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Специалист по кадрам
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Контроль обновления ПО и единообразия, применяемого ПО на всех элементах ИС	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Еженедельно	Ежегодно	Ответсвенные лица и ИБ
Поддержание в актуальном состоянии нормативно-организационных документов	Еженедельно	Ежемесячно	Специалист по кадрам
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Ответсвенные лица и ИБ

Приложение 2
к Правилам осуществления внутреннего
контроля соответствия обработки
персональным данным требованиям к защите
персональных данных, утверждено
приказом директора от 30.08.2019 г. № 69/1

Ж У Р Н А Л
учета событий информационной безопасности гимназии «Альбертина»

Журнал начат « »	_____ 20__г.	Журнал завершен « »		20 г.
Должность		Должность		
/	/	/		/

№ п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приказ№69/1 от 30.08.2019

Приложение 3
к Правилам осуществления внутреннего контроля
соответствия обработки персональным данным
требованиям к защите персональных данных,
утверждено приказом директора от 30.08.2019 г. №
69/1

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен о том, что «_____»_____20___г.
проведена
проверка_____
_____(комиссией)
(должность, Ф.И.О. сотрудника)

_____
_____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:_____
(название документа)

_____

В ходе проверки
проверено:_____
_____
_____
_____
_____

Выявленные нарушения:_____
_____
_____
_____
_____
_____

Меры по устранению
нарушений:_____
_____
_____
_____
_____

Срок устранения нарушений:_____
_____

Председатель комиссии:_____
_____
(фамилия и инициалы / подпись / должность)

Члены
комиссии:_____
_____
(фамилия и инициалы / подпись / должность)

Приложение № 9
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Правила работы с обезличенными персональными данными

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», определяют порядок работы с обезличенными данными гимназии «Альбертина. Термины и определения

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

- ПДн - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);
- обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;
- обезличивание ПДн - действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

2. Условия обезличивания

Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения классов ИСПДн и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». К методам обезличивания ПДн относятся:

- метод введения идентификаторов;
- метод изменения состава или семантики;
- метод декомпозиции;
- метод перемешивания.

Перечень должностей муниципальных служащих, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн (приложение 1 к правилам работы с обезличенными персональными данными);

- решение о необходимости обезличивания ПДн принимает руководитель школы;
- Сотрудники школы**,** непосредственно осуществляющие обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и способ обезличивания;
- сотрудники школы**,** обслуживающих базы данных с ПДн, совместно с ответственным за организацию обработки ПДн, осуществляют непосредственное обезличивание выбранным способом.

3. Порядок работы с обезличенными ПДн

Обезличенные ПДн не подлежат разглашению и нарушению конфиденциальности.

Обезличенные ПДн могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных ПДн необходимо соблюдение требований нормативных правовых актов Российской Федерации и Московской области.

Приложение 1
к правилам работы с обезличенными персональными
данными, утверждено приказом директора
от 30.08.2019 г. № 69/1

Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных в гимназии «Альбертина»

1. Директор гимназии
2. Заместители директора по УВР
3. Заместитель директора по УР
4. Заместитель директора по ВР
5. Заместитель директора по АХЧ
6. Главный бухгалтер
7. Секретарь

Приложение № 10
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
реагирования на инциденты информационной безопасности

1. Общие положения

1.1. Настоящая инструкция реагирования на инциденты информационной безопасности (далее - Инструкция реагирования) устанавливает порядок реагирования на инциденты информационной безопасности, разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработки и принятия мер по предотвращению возможных опасных последствий подобных нарушений, а также выявления, расследования и предотвращения иных инцидентов информационной безопасности в гимназии «Альбертина».

1.2. Инструкция реагирования разработана 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» и иными нормативными правовыми актами.

1.3. Настоящая Инструкция реагирования обязательна к соблюдению всеми работниками гимназии «Альбертина», участвующими в выявлении, разбирательстве и предотвращении инцидентов информационной безопасности (далее - ИБ).

1.4. Разбирательство по всем инцидентам ИБ проводится постоянно действующей комиссией по информационной безопасности (далее ПДК) с привлечением в необходимых случаях сотрудников других подразделений.

2. Выявление инцидента информационной безопасности

2.1. Основными источниками информации об инцидентах ИБ являются:

- факты, выявленные руководителем, заместителями руководителя гимназии, членами ПДК по ИБ, лицом ответственным по обеспечению информационной безопасности в школе, администратором информационной безопасности, назначенным приказом по гимназии, а также другими сотрудниками организации.
- результаты работы средств мониторинга ИБ, проверок и аудита (внутреннего или внешнего);
- журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
- обращения субъектов персональных данных с указанием инцидента ИБ;
- запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
- другие источники информации.

2.2. Основными видами инцидентов ИБ в гимназии являются:

- разглашение конфиденциальной или внутренней информации либо угроза такого разглашения;
- несанкционированный доступ лиц, не имеющих легального доступа к ресурсам или помещениям организации;
- превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников школы;
- компрометация учетных записей или паролей;
- вирусная атака или вирусное заражение;
- нарушение или сбои в работе системы резервного копирования;
- нарушение правил использования персональных данных.

2.3. Сотрудник школы может выявить признаки наличия инцидента ИБ путем анализа текущей

ситуации на предмет ее соответствия требованиям защиты информации, утвержденным в школе. Выявленные несоответствия дают основания предполагать факт возникновения инцидента ИБ. Любые сведения о происшествии или инциденте ИБ должны быть незамедлительно переданы выявившим их сотрудником администратору информационной безопасности.

3. Анализ исходной информации и принятие решения о проведения разбирательства

3.1. Администратор ИБ после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа администратор ИБ проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению администратора ИБ единичный инцидент ИБ, не повлекший негативные последствия и совершенный сотрудником школы впервые, фиксируется администратором ИБ в карточке данных об инциденте ИБ (приложение 1 к инструкции реагирования на инциденты информационной безопасности) с присвоением статуса «Разбирательство не требуется».

3.3. В случае наличия признаков инцидента ИБ, повлекшего негативные последствия, администратор ИБ классифицирует инцидент, определяет его предварительную степень важности, принимает решение о необходимости проведения расследования, информирует руководителя школы либо его заместителя об инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса в процессе расследования.

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте ИБ, администратор ИБ по согласованию с руководителем школы определяет и инициирует первоочередные меры, направленные на локализацию инцидента и минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

4.1. Цели и этапы разбирательства инцидента ИБ:

4.1.1. Целями разбирательства инцидентов ИБ являются:

- выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
- защита прав школы, установленных законодательством Российской Федерации;
- защита репутации школы и их информационных ресурсов;
- обеспечение безопасности персональных данных;
- защита прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых в школе;
- предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство инцидента ИБ состоит из следующих этапов:

- подтверждение/опровержение факта возникновения инцидента ИБ;
- классификация инцидента ИБ;
- подтверждение/корректировка уровня значимости инцидента ИБ;
- уточнение дополнительных обстоятельств (деталей) инцидента ИБ;
- получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;
- минимизация последствий инцидента ИБ;
- информирование и консультирование персонала школы по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;
- переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.

4.2. Порядок проведения разбирательства инцидента ИБ:

4.2.1. В процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

- дата и время совершения инцидента ИБ;
- ФИО, должность и подразделение нарушителя ИБ;
- классификация инцидента;
- уровень критичности инцидента ИБ;

- обстоятельства и мотивы совершения инцидента ИБ;
- информационные ресурсы, затронутые инцидентом ИБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента ИБ.

4.2.2. При инциденте ИБ, затрагивающем не более одного структурного подразделения, администратор ИБ информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При инциденте ИБ, затрагивающем более одного структурного подразделения, администратор ИБ информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя ИБ информация об отключении прав доступа администратором ИБ направляется руководителю предполагаемого нарушителя ИБ.

4.2.5. Осуществляющий разбирательство администратор ИБ в процессе проведения расследования инцидента ИБ при необходимости запрашивает информацию в структурных подразделениях, направляя запрос на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по инциденту ИБ осуществляющий расследование администратор ИБ проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента ИБ администратор ИБ запрашивает у руководителя структурного подразделения полученные от нарушителя ИБ объяснения. Объяснительная записка должна быть составлена, подписана нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем администратору ИБ в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя ИБ предоставить объяснительную записку администратор ИБ составляет акт, составленный в соответствии с установленным в школе порядком.

4.2.8. Администратор ИБ проводит оценку негативных последствий инцидента ИБ. В ходе данной оценки учитываются:

- прямой финансовый ущерб;
- репутационный ущерб;
- потенциальный ущерб;
- косвенные потери, связанные с недоступностью сервисов, потерей информации;
- другие виды ущерба или аспекты негативных последствий для Администрации или субъектов персональных данных.

4.2.9. С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа сотрудника к информационным ресурсам (ИР) на время проведения расследования. Подобное отключение инициируется администратором ИБ при условии его обязательного предварительного устного согласования с руководителем сотрудника.

4.2.10. В случае если у нарушителя ИБ были отключены права доступа к ИР на время проведения расследования, по его результатам администратор ИБ по согласованию с руководителем нарушителя ИБ принимает решение о возвращении в полном или ограниченном объеме ранее имеющихся у нарушителя ИБ прав доступа к ИР и инициирует возвращение указанных прав в соответствии в данным решением либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком доступа к информационным, программным и аппаратным ресурсам школы. Если нарушение ИБ было вызвано незнанием нарушителем ИБ правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по информационной безопасности, по результатам изучения соответствующих локальных нормативных актов школы.

4.2.11. Восстановление временно отключенных у нарушителя ИБ прав доступа к информационным ресурсам (разблокировка пользователя) может производиться только администратором ИБ.

5. Оформление результатов проведенного разбирательства

5.1. Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором ИБ в карточке данных об инциденте ИБ и учитывается при подготовке итогового заключения по инциденту ИБ.

5.2. Администратор ИБ формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

5.3. Итоговое заключение по инциденту ИБ администратор ИБ направляет всем заинтересованным руководителям структурных подразделений.

5.4. Администратор ИБ фиксирует завершение разбирательства в карточке инцидента ИБ и присваивает инциденту статус «Разбирательство завершено».

5.5. Администратор ИБ, при необходимости определения правовой оценки инцидента ИБ, может обратиться за консультациями в юридическое подразделение Администрации.

5.6. В случае выявления в инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, администратор ИБ передает все материалы по инциденту ИБ руководству школы для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6. Завершение разбирательства, превентивные мероприятия

6.1. По завершении расследования инцидента ИБ администратор ИБ передает имеющиеся материалы (в объеме, достаточном для принятия решения) руководителю нарушителя ИБ для решения вопроса о целесообразности привлечения нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов расследования руководитель структурного подразделения совместно с администратором ИБ в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем:

- анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя ИБ;
- доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов школы;
- обсуждение инцидента ИБ на совещании руководителей или собрании коллектива;
- отмена неактуальных прав доступа к информационным ресурсам;
- проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.3. О результатах проведенного расследования инцидента ИБ администратор ИБ письменно докладывает руководству школы.

7. Права, обязанности и ответственность участников разбирательства

7.1. Администратор ИБ имеет право:

- по согласованию с непосредственным руководителем нарушителя ИБ требовать у нарушителя ИБ письменные объяснения по обстоятельствам инцидента ИБ;
- запрашивать и получать от руководителей и сотрудников школы, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для расследования инцидента ИБ;
- инициировать отключение от информационных ресурсов сотрудников школы, нарушивших правила или требования ИБ, на период проведений расследования инцидента ИБ, если имеется существенный риск того, что продолжение работы сотрудника с информационными ресурсами может повлечь значительное увеличение ущерба или новые инциденты ИБ;
- по результатам расследования инцидента ИБ инициировать изменения в бизнес-процессах и информационных ресурсах школы с целью повышения их защищенности и снижения рисков инцидентов ИБ;
- инициировать процедуры привлечения нарушителя ИБ к дисциплинарной и (или) материальной ответственность согласно требованиям внутренних нормативных документов Администрации.

7.2. Администратор ИБ обязан:

- объективно проводить расследование каждого инцидента ИБ;
- определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;
- фиксировать в карточке данных об инцидентах ИБ всю исходную информацию об инциденте ИБ

и результаты его расследования;

- предоставлять отчеты и рекомендации по результатам проведенных расследований руководству гимназии;
- проводить анализ обстоятельств, способствовавших возникновению каждого инцидента ИБ, и на его основе совместно с отделом информационных технологий разрабатывать рекомендации и предложения по оптимизации бизнес-процессов, снижению ущерба от подобных инцидентов ИБ и предотвращению возможности их повторения в будущем.

7.3. Руководители структурных подразделений и сотрудники гимназии обязаны:

- предоставлять по запросам администратора ИБ устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения расследования инцидента ИБ;
- информировать администратора ИБ о выявленных инцидентах ИБ;

Приложение 1
к Инструкции реагирования на инциденты
информационной безопасности,
утверждено приказом директора
от 30.08.2019 г. № 69/1

Карточка данных об инциденте ИБ

Дата события
Номер события

Информация о сообщающем лице

Фамилия _____ Адрес _____
Организация _____
Телефон _____ Электронная почта _____

Описание события ИБ Описание события:

- Что произошло
- Как произошло
- Почему произошло
- Пораженные компоненты
- Негативное воздействие на ИСПДн
- Любые идентифицированные уязвимости

Детали события ИБ

Дата и время возникновения события _____
Дата и время обнаружения события _____
Дата и время сообщения о событии _____
Классификация события _____
Закончилось ли событие? *(отметить квадрат*) Да □ Нет □

Если «да», то уточнить, как долго длилось событие в днях/часах/минутах _____

Тип инцидента ИБ *(Отметить один квадрат, затем заполнить соответствующие поля ниже)*

Действительный □ Попытка □ Подозрение □

(один из) Намеренная □ *(указать типы угрозы)*

Хищение □
Мошенничество □
Саботаж/физический ущерб □
Вредоносная программа □

Хакерство/Логическое проникновение □
Неправильное использование ресурсов □
Другой ущерб □

(один из) Случайная □ *Определить:*

(указать типы угрозы)

Другие природные события □

Отказ ПО □ *Определить:*

Потеря существенных сервисов □

Отказ связи □

Отказ аппаратуры □
Пожар, наводнение □
Отказ электропитания □
(Один из) Ошибка □

Операционная ошибка □
Ошибка аппаратной поддержки □
Ошибка поддержки ПО □

Неизвестно □

Недостаточное кадровое обеспечение □
Другие случаи □
Определить:

(указать типы угрозы)

Ошибка пользователя □
Ошибка конструкции □
Другие случаи (включая истинные заблуждения) □
Определить:

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат

«неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)
Определить:

Пораженные активы

Пораженные активы (если есть) *(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)*

Информация/Данные _____
Аппаратура _____
Программное обеспечение _____
Средства связи _____
Документация _____

Негативное воздействие/влияние инцидента

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке

«значимость» указать уровень негативного воздействия на бизнес по шкале 1+10, используя сокращения (указатели категорий): (ФП) - финансовые потери/разрушение бизнес-операций, (КИ) - коммерческие и экономические интересы, (ПД) - информация, содержащая персональные данные, (ПО) - правовые и нормативные обязательства, (БО) - менеджмент и бизнес-операции, (ПП) - потеря престижа. Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»

	Значимость	Указатели	Стоимость
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	□		
Нарушение целостности *(т. е., несанкционированная модификация)*	□		
Нарушение доступности *(т. е., недоступность)*	□		
Нарушение неотказуемости	□		
Уничтожение	□		

Полные стоимости восстановления после инцидента

(Где возможно, необходимо Значимость Указатели Стоимость

указать общие расходы на восстановление после инцидента в целом

по шкале 1+10 для

«значимости» и в деньгах для «стоимости»)

Приказ№69/1 от 30.08.2019

Разрешение инцидента

Дата начала расследования инцидента _____

Фамилия лица (лиц), проводившего (их) расследование инцидента _____

Дата окончания инцидента _____

Дата окончания воздействия _____

Дата завершения расследования инцидента _____

Ссылка и место хранения отчета о расследовании _____

(один из)

Лицо

Причастные лица

Организованная группа

Легально учрежденная организация/учреждение

Случайность

Нет виновного

Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(один из)

Криминальная/финансовая выгода

Развлечение/хакерство

Политика/Терроризма

Реванш

Другие мотивы

Определить:

Действия, предпринятые для разрешения инцидента

(например, «никаких Действий», «поДручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)

Действия, запланированные для разрешения инцидента

(например, см. выше)

Прочие действия

(например, по-прежнему требуется проведение расследования для другого персонала)

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный

Незначительный

(Укажите любые Другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое

Администратор ИБ

Руководитель информационных технологий

Руководитель организации

Начальник отдела подразделения

(уточнить какого)

возложены обязанности в	Автор отчета	Начальник отдела кадров
области ИБ и которое	Полиция	Другое лицо
формулирует требуемые Действия		*(например, служба охраны, регулятивного органа, сторонняя организация) Определить:*

Привлеченные лица

Инициатор	Аналитик	Аналитик
Подпись _____	Подпись _ _____	Подпись _ _____
Фамилия _____	Фамилия_____	Фамилия_____
Роль _____	Роль _____	Роль _____
Дата _____	Дата _____	Дата _____

Приказ№69/1 от 30.08.2019

Приложение № 11
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
по организации антивирусной защиты при работе в информационной системе

1. Общие положения

Данная инструкция по организации антивирусной защиты при работе в информационной системе (далее - Инструкция по АВЗ) разработана в целях обеспечения антивирусной безопасности информационной системы (далее ИС) и регламентирует требования к организации антивирусной защиты в ИС, а также устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих ИС, за выполнение этих требований.

Установка средств антивирусного контроля и настройка их параметров на рабочих станциях (серверах) ИС осуществляется администратором безопасности информации, в соответствии с эксплуатационной документацией по применению конкретных антивирусных средств.

2. Порядок установки и обновления антивирусных средств

К применению в ИС допускаются только лицензионные антивирусные средства, принятые в промышленную эксплуатацию и прошедшие проверку оценки соответствия требованиям безопасности информации в установленном порядке.

Установка компонентов централизованного управления и серверных компонентов антивирусного комплекса, настройка его регулярного обновления осуществляется администратором безопасности информации.

Первичная установка антивирусного программного обеспечения (клиентских частей) на персональные компьютеры пользователей осуществляется администратором безопасности информации при подготовке автоматизированного рабочего места пользователя.

Обновления баз вирусных сигнатур и сканирующего модуля должны производиться автоматически после выпуска новой версии базы вирусных сигнатур и сканирующего модуля на сервере производителя, независимо от перезагрузок операционных систем автоматизированных рабочих мест пользователей.

Ни один элемент ИС, подверженный актуальной вирусной уязвимости, не должен эксплуатироваться без установленной клиентской части антивирусного комплекса.

3. Порядок проведения антивирусного контроля

На всех объектах вычислительной техники (рабочие станции, серверы) входящих в состав ИС, администратор безопасности информации обеспечивает антивирусный контроль в режиме реального времени.

На рабочих станциях пользователей и серверах ИС указанные специалисты дополнительно обеспечивают проведение полного сканирования всех машинных носителей информации средств вычислительной техники (стационарных либо съемных) антивирусными средствами не реже 1 раза в неделю (автоматическое сканирование по расписанию).

Кроме того, администратор безопасности информации осуществляет обязательный антивирусный контроль:

- любой информации (текстовых файлов любых форматов, файлов данных, исполняемых файлов), получаемой и передаваемой по телекоммуникационным каналам, а также информации на съемных носителях (магнитные и оптические диски, USB-диски и т.п.), получаемой от сторонних лиц и организаций (автоматическое сканирование в режиме реального времени);
- файлов, помещаемых в электронный архив. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц (автоматическое сканирование по расписанию).

Администратор безопасности информации осуществляет настройку антивирусной системы таким образом, что при обнаружении вируса (инфицированного файла) выполняются следующие действия:

- лечение (очистка) файла от обнаруженного вируса с предварительным созданием резервной копии;
- перемещение зараженного объекта в специально выделенную закрытую директорию (карантинную зону) на специализированном сервере при невозможности удаления из него тела вируса, «троянской программы», «сетевого червя» и т.п.;

- оповещение пользователя и администратора безопасности информации о результатах указанных выше действий согласно заданным адресам оповещения.

Администратор безопасности информации, обеспечивающий функционирование антивирусного комплекса ИС, обязан:

Ежедневно:

- проверять через соответствующие консоли централизованного управления информацию об автоматическом обновлении версий базы вирусных сигнатур и сканирующего модуля для каждой подсистемы комплекса;
- принимать и обрабатывать по мере поступления все заданные сообщения о действиях антивирусного комплекса;
- при выявлении попыток инфицирования средств вычислительной техники ИС, разобраться в их причинах (при необходимости с привлечением сотрудников, ответственных за эти средства вычислительной техники). При невозможности выяснить причины инфицирования средств вычислительной техники ИС в штатном режиме либо при выявлении злого умысла немедленно сообщить председателю комиссии по информационной безопасности Администрации города Серпухова;
- при вирусной атаке с конкретного средства вычислительной техники немедленно отключать (постоянно или временно) это средство вычислительной техники от сетевого оборудования.

Ежемесячно:

- анализировать все системные журналы антивирусного комплекса для составления общего отчета;
- после завершения отчетных мероприятий и после уведомления председателя комиссии по информационной безопасности школы очищать данные журналы и «карантинные зоны» на серверах за истекший месяц.

4. Действия сотрудников при обнаружении компьютерного вируса

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором безопасности информации должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе, если таковые имеются.

Администратор безопасности информации совместно с владельцем зараженных вирусом и неизлечимых файлов должен провести анализ необходимости их дальнейшего использования и по результатам данного анализа:

- провести чистку или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на гибком магнитном диске в организацию, с которой заключен договор на антивирусную сервисную поддержку.

5. Порядок восстановления информации и работоспособности средств вычислительной техники в случае реализованного вирусного воздействия

Действия администратора безопасности информации по ликвидации последствий воздействия вируса и восстановлению информации (работоспособности СВТ) должны быть следующими:

- выполнить действия, определенные настоящей Инструкцией по АВЗ и направленные на пресечение распространения вируса по сетевой инфраструктуре (изолировать инфицированное средство вычислительной техники);
- обеспечить получение новой базы вирусных сигнатур (при ее отсутствии у производителя, связаться с организацией, обеспечивающей сервисную поддержку антивирусного комплекса);
- выполнить действия по удалению тела вируса из всех зараженных файлов на всех средствах вычислительной техники, подвергшихся атаке;
- использовать службу устранения нанесенного ущерба, входящую в состав антивирусного комплекса при необходимости восстановления работоспособности средств вычислительной техники;
- обеспечить восстановление модифицированной (поврежденной) информации с применением

системы резервного копирования и восстановления при невозможности очистки зараженных файлов.

6. Ответственность при организации антивирусной защиты

Администратор безопасности информации несет ответственность за:

- обеспечение доступа к дистрибутивам и дополнениям антивирусных средств, своевременное обновление их версий и оповещение о появлении новых версий;
- работоспособность, корректную работу, своевременное обновление антивирусных средств и своевременную проверку дисков центральных серверов;
- организацию и контроль функционирования антивирусной защиты на средствах вычислительной техники ИС обнаружения инфицированных объектов;
- работоспособность, корректную работу, своевременное обновление антивирусных средств, своевременную проверку дисков локальных серверов и рабочих станций, а также поступающей и исходящей электронной почты.

За разработку или умышленное распространение компьютерных вирусов, троянских программ, макровирусов и других вредоносных программ сотрудники Администрации несут ответственность согласно действующему законодательству Российской Федерации.

Приложение № 12
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
по организации парольной защиты при работе в информационной системе

1. Общие положения

Личные пароли доступа к информационным ресурсам (далее - ресурсы) информационной системы (далее ИС) выдаются пользователям администратором безопасности информации.

Пароль, полученный пользователем от администратора безопасности информации, необходимо сменить при первом входе в систему.

Пользователи обязаны производить смену паролей не реже одного раза в месяц.

Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администратора безопасности информации и других сотрудников, которым по роду деятельности были предоставлены полномочия по управлению системой парольной защиты.

Все действия, выполненные под логином и паролем конкретного пользователя, считаются совершенными этим пользователем.

2. Правила формирования пароля

Средство вычислительной техники (далее - СВТ), применяемое для работы с парольной информацией, должно быть оснащено антивирусным программным обеспечением и иметь актуальные антивирусные базы. Перед созданием (генерацией) парольных данных, должна быть выполнена антивирусная проверка СВТ на отсутствие вредоносного программного обеспечения (вирусов, программ отслеживания клавиатурного ввода и прочих программных закладок). Программная среда СВТ не должна содержать нелицензионного программного обеспечения и программ, полученных из недостоверных источников (файл-обменные и социальные сети) через средства обмена быстрыми сообщениями и т.п.

При регистрации нового пользователя в ИС администратором безопасности информации устанавливается временный пароль, который должен быть сменен при первом входе в пользователя в систему с учетом требований настоящей инструкции.

При создании пароля пользователи обязаны придерживаться следующих правил:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:
- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например:!@#$%л&*()_+|—=\'{}[]:";'<>?,./).

Запрещается использовать в качестве пароля:

- имя входа в систему, простые пароли (например, 111, qwerty, abcd, !»№, asxz, fgrt, шлдщ, и т.п.), а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно установить, основываясь на информации о пользователе;
- один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 12345678, жцукенагш и т.п.);
- ранее использованные комбинации.

3. Правила ввода пароля

При вводе пароля пользователи обязаны придерживаться следующих правил:

- учитывать регистр, в котором был задан пароль;
- отключить возможность автоматического сохранения пароля;
- исключить возможность его фиксации посторонними лицами или техническими средствами (видеокамеры и др.).

4. Правила хранения пароля

При хранении паролей пользователи обязаны придерживаться следующих правил:

- хранить пароль на бумажном носителе только в личном сейфе владельца пароля или сейфе руководителя подразделения в опечатанном владельцем пароля конверте или пенале;
- не фиксировать пароль на внешних электронных носителях, в памяти устройств мобильной связи, в портативных компьютерах и прочих средствах, а также на материалах, не предназначенных для обработки (хранения) конфиденциальной информации;
- не сообщать другим пользователям личный пароль и не регистрировать их в системе под своим паролем;
- не направлять пароли пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет;
- своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

5. Запрещенные действия пользователей ресурсов ИС

Пользователям ресурсов ИС запрещается:

- использовать один и тот же пароль для доступа к ресурсам ИС и другим ресурсам (например, доступ в Интернет с домашнего компьютера, доступ к системам электронной коммерции и т. д.);
- использовать один и тот же пароль для доступа к различным ИС, если это не разрешено соответствующими эксплуатационными регламентами или инструкциями;
- сообщать пароль кому-либо, включая секретаря, руководителя, администратора, сотрудников обслуживающего персонала, без письменного разрешения администратора безопасности информации. Все пароли являются конфиденциальной информацией Администрации городского округа Серпухов Московской области;
- использовать клавиатуры и другие средства ввода, подключенные к СВТ по беспроводным технологиям, в том числе по технологии Bluetooth или с использованием инфракрасных передатчиков при вводе пароля для доступа к информации, размещенной в ИС;
- вводить пароль в области непосредственного действия диктофонов, камер видеонаблюдения, средств телефонной связи в состоянии вызова и других устройств визуальной или акустической регистрации информации;
- произносить вслух набираемый пароль или части пароля, а также выполнять ввод пароля при наблюдении за этим процессом посторонних лиц;
- сообщать пароль кому-либо по телефону;
- говорить о своем пароле в окружении посторонних лиц;
- упоминать о содержании пароля (например, «мой день рождения»);
- указывать свой пароль в анкетах или опросниках;
- сообщать свой пароль членам семьи;
- сообщать свой пароль сослуживцам перед уходом в отпуск.

6. Ответственность лиц, использующих пароли к ИС

Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении паролей и сроков их действия.

Приказ№69/1 от 30.08.2019

Приложение № 13
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
по порядку резервирования и восстановления работоспособности

технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) (далее - Порядок) определяет действия, связанные с функционированием информационной системы персональных данных (далее - ИСПДн) школы (далее - краткое наименование), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачей данной документа является:

- определение мер защиты от потери информации;
- определение действий по восстановлению информации в случае ее потери.

1.4. Действие настоящего Порядка распространяется на всех пользователей школы, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

1.6. Администратор ИСПДн назначается сотрудником, ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации.

1.7. Администратор безопасности назначается сотрудником, ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в журнале учета нештатных ситуаций.

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники школы (администратор безопасности, администратор ИСПДн), предпринимают меры по восстановлению работоспособности ИСПДн. Перечень указанных мер согласуется с вышестоящим руководством, за исключением случаев, когда ИСПДн должна быть восстановлена в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся

программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения ИСПДн включают:

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

3.3. Все помещения школы, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции 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 компьютеров;
- 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.

3.6. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замене без простоев должны использоваться методы кластеризации. Для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

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

3.9. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.10. Организационные меры.

Резервное копирование и хранение данных должно проводиться в следующем режиме:

- обрабатываемые персональные данные - не реже раза в неделю;
- технологическая информация - не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн, - не реже раза в месяц и каждый раз при внесении в них изменений (выход новых версий).

3.11. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета (приложение 1 к инструкции по порядку резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных).

3.12. На носителях, предназначенных для хранения резервных копий информации, должны быть указаны их регистрационные номера, а также даты проведения резервного копирования.

3.13. Носители должны храниться в несгораемом шкафу или помещении, оборудованном

системой пожаротушения.

Приказ№69/1 от 30.08.2019

Приложение 1
к Инструкции по порядку резервирования и
восстановления работоспособности технических
средств и программного обеспечения, баз данных и
средств защиты информации в ИСПДн, утверждено
приказом директора от 30.08.2019 г. № 69/1

Ж У Р Н А Л
учета резервного копирования в информационных системах персональных данных

гимназии «Альбертина»

Журнал начат « » 20 г.	Журнал начат « » 20 г.
Должность	Должность
/ /	/ /

№	Наименование информационной системы	Информация, подлежащая резервированию (содержимое каталога)	Периодичность проведения процедуры	Срок хранения информации	Ответственное должностное лицо	Гриф информации
1	2	3	4	5	6	7

Приказ№69/1 от 30.08.2019

Приложение № 14
Утверждено приказом
директора гимназии
«Альбертина
от 30.08.2019 г. № 69/1

Инструкция
по установке, модификации и техническому обслуживанию
программного обеспечения и аппаратных средств информационных
систем персональных данных

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (далее - Инструкция по установке) школы, включает в себя описание взаимоувязанного комплекса организационно - технических мер по проведению работ в части установки, модификации и технического обслуживания программного обеспечения и аппаратных средств информационной системы персональных данных (далее ИСПДн).

1.2. Требования настоящей Инструкции по установке распространяются на всех должностных лиц и сотрудников школы, использующих в работе информационные системы, в которых осуществляется обработка персональных данных.

1.3. Сотрудники школы, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями Инструкции по установке по мере необходимости.

1.4. Ознакомление с требованиями Инструкции по установке осуществляет администратор информационной безопасности под роспись с выдачей электронных копий соответствующих приложений и разделов непосредственно для повседневного использования в работе.

1.5. В случае невозможности исполнения требований настоящей Инструкции по установке в полном объеме, например, в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний, злоумышленных действий, степень соблюдения требований настоящей Инструкции по установке определяется администратором ИСПДн по согласованию с лицом, ответственным за защиту персональных данных (далее ПДн) школы.

2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств рабочих станций школы должны производиться только на основании заявок руководителей структурных органов школы. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения.

2.2. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн школы, отражаются в техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации.

2.3. В заявке, обозначенной в п. 2.1 настоящей Инструкции по установке (приложение 1 к инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных), указываются наименование ИСПДн и реквизиты ответственного за ее эксплуатацию сотрудника, после чего данная заявка передается администратору ИСПДн для выполнения работ по внесению изменений в конфигурацию ИСПДн школы.

2.4. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций школы предоставляется администратору информационной безопасности, а также лицу, ответственному за защиту ПДн.

2.5. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме администратора информационной безопасности и/или лица, ответственного за

Приказ№69/1 от 30.08.2019

защиту ПДн, запрещено.

2.6. Установка и настройка программного средства осуществляется администратором ИСПДн согласно эксплуатационной документации.

2.7. Запрещается установка и использование на ИСПДн (серверах) программного обеспечения (ПО), не входящего в перечень ПО, разрешенного к использованию в школе.

2.8. Руководители структурных подразделений осуществляют контроль за отсутствием на ИСПДн сотрудников подразделения, ПО и данных, не связанных с выполнением должностных обязанностей.

2.9. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у администратора ИСПДн. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с Инструкцией по организации антивирусной защиты ИСПДн.

2.10. После установки (обновления) ПО администратор информационной безопасности должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и совместно с пользователем ИСПДн проверить правильность настройки средств защиты.

2.11. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства сотрудники немедленно докладывают руководителю своего подразделения и администратору информационной безопасности. Использование программного средства до получения специальных указаний запрещается.

2.12. После завершения работ по внесению изменений в состав аппаратных средств защищенных ИСПДн системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) администратором информационной безопасности.

2.13. При изъятии ИСПДн из состава рабочих станций ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как администратор информационной безопасности ИСПДн снимет с нее средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом о затирании остаточной информации за подписью администратора ИСПДн (приложение 2 к инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных).

2.14. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ИСПДн с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у администратора информационной безопасности.

3. Ответственные за соблюдение требований и контроль выполнения Инструкции по установке

3.1. Ответственность за соблюдение требований настоящей Инструкции возлагается на сотрудников Администрации персонально.

3.2. Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на администратора информационной безопасности.

3.3. Ответственность за общий контроль информационной безопасности возлагается на ответственного за защиту ПДн школы.

Приложение 1
к Инструкции по установке модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных, утверждено приказом директора от 30.08.2019 г. № 69/1

Заявка
на внесение изменений в состав программного (аппаратного) обеспечения

Прошу дать указания ответственным сотрудникам для организации установки (изменения настроек) _____

(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач: _____

следующим пользователям: _____

(фамилия, имя, отчество)

Изменения на ИСПДн произведены (не произведены) по следующей причине: _____

Выполнены следующие работы:

Выполнены следующие изменения в настройках средств защиты: _____

Администратор ИБ ИСПДн

«__»_____20 г. _____ _____

(Подпись) (Фамилия, инициалы)

Приказ№69/1 от 30.08.2019

Приложение 2
к Инструкции по установке модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных, утверждено приказом директора от 30.08.2019 г. № 69/1

Акт
о затирании остаточной информации

Все файлы, содержащие информацию, находившиеся на _____ НЖМД
(Модель, серийный №),

передаваемом _____
(С какой целью) (кому: должность, Ф.И.О.)

ИС _____
(наименование ИС)

уничтожены (затерты) посредством программы _____.

Администратор ИБ ИСПДн

«__»_____20 г. _____ _____
(Подпись) (Фамилия, инициалы)

Приложение № 15
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
по обращению с криптографическими средствами защиты информации

1. Общие положения

1.1. Настоящая инструкция по обращению регламентирует порядок обращения с шифровальными (криптографическими) средствами, предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, а также порядок допуска к работам с шифровальными средствами.

1.2. К шифровальным (криптографическим) средствам (средствам криптографической защиты информации - СКЗИ) относятся:

- средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее передаче по каналам связи и (или) при ее обработке и хранении;
- средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;
- средства электронной подписи (ЭП) - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;
- средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

1.3. Сотрудники допускаются к работе с СКЗИ после прохождения необходимой подготовки.

1.4. Лицо, ответственное за обеспечение безопасности эксплуатации средств криптографической защиты информации назначается и освобождается от исполнения обязанностей, предусмотренных настоящей инструкцией приказом руководителя школы.

1.5. Ответственное лицо в своей работе непосредственно подчиняется руководителю школы.

1.6. Функциональными обязанностями ответственного лица являются:

- взаимодействие с органами лицензирования и сертификации ФСБ России, разработчиками (производителями) СКЗИ и поставщиками услуг в области шифрования информации;
- разработка и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ, в том числе открытых и закрытых ключей шифрования (криптоключей), электронной подписи (ЭП) и сертификатов открытых ключей;
- координация и контроль деятельности операторов СКЗИ при работе с СКЗИ;
- разработка и участие в согласовании технической и организационно-распорядительной документации, связанной с применением СКЗИ в школе;
- ведение журнала учета экземпляров средств криптографической защиты информации и средств защиты информации школы (приложение 1 к инструкции по обращению с криптографическими средствами защиты информации);

- участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации, в том числе в случае компрометации действующих криптоключей;

- участие в разборе конфликтных ситуаций;

- доклад непосредственному руководителю о выявленных нарушениях операторов СКЗИ и/или сотрудников школы и/или третьих лиц в отношении СКЗИ, а также о принятие необходимых мер по устранению данных нарушений.

1.7. Все сотрудники, допущенные к работе со СКЗИ, должны ознакомиться с инструкцией по обращению под роспись и строго выполнять требования следующих документов:

- инструкции по обращению с криптографическими средствами защиты информации;
- эксплуатационной документации на СКЗИ;
- организационно-распорядительных документов школы, регламентирующих работу со СКЗИ.

1.8. Разработка и проведение мероприятий по обеспечению безопасности при проведении работ со СКЗИ осуществляется лицом, уполномоченным руководить данными работами (ответственным за обеспечение безопасности эксплуатации СКЗИ).

1.9. Пользователям, которым необходимо получить доступ к работе со СКЗИ, необходимо пройти самостоятельное обучение правилам указанной работы.

2. Требования по размещению, специальному оборудованию и охране помещений, в которых производятся работы с СКЗИ

2.1. Размещение, специальное оборудование, охрана и режим в помещениях, в которых ведется работа со СКЗИ (далее - помещения), должны обеспечивать безопасность информации СКЗИ путем сведения к минимуму возможности неконтролируемого к ним доступа и, просмотра процедур работы со СКЗИ посторонними лицами.

2.2. Порядок допуска в помещения определяется внутренней организационно-распорядительной документацией школы. Доступ лиц в эти помещения должен быть ограничен в соответствии со служебной необходимостью. Рекомендуется использовать технические системы ограничения доступа в эти помещения. Допуск в помещения вспомогательного и обслуживающего персонала (уборщиц, электромонтеров, сантехников и т.д.) производится только в случае служебной необходимости в сопровождении ответственного за режим после принятых мер, исключающих визуальный просмотр конфиденциальных документов.

2.3. Входные двери помещений должны быть изготовлены из прочных материалов и оборудованы запирающими устройствами, гарантирующими надежное закрытие помещений в нерабочее время. Для контроля за входом в рабочее время рекомендуется устанавливать элементы систем контроля доступа.

2.4. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения.

2.5. Для предотвращения просмотра извне окна помещений должны быть защищены (оборудованы жалюзи или шторами и т.п.).

2.6. Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.

2.7. По окончании рабочего дня помещения закрываются и опечатываются и/или сдаются под охрану.

2.8. Сдачу ключей и помещений, а также получение ключей и вскрытие помещений производят сотрудники, работающие в этих помещениях, по утвержденному директором гимназии списку с образцами подписей этих сотрудников. Дубликаты ключей от входных дверей должны храниться в сейфе ответственного лица, назначаемого руководителем школы.

2.9. Перед вскрытием помещений должна быть проверена целостность оттисков печатей

и/или исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководство и отдел безопасности.

2.10. В случае утраты ключа от входной двери помещения руководитель школы немедленно ставится в известность.

2.11. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, в которых предусматривается порядок вызова должностных лиц школы, вскрытия помещений, очередность и порядок спасения конфиденциальных документов и дальнейшего их хранения.

2.12. Для непосредственного хранения СКЗИ, носителей с дистрибутивами СКЗИ, эксплуатационной и технической документации к СКЗИ помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей или кодовыми замками, а также при необходимости - приспособлениями для опечатывания замочных скважин.

3. Порядок обращения со средствами криптографической защиты информации

3.1. Уполномоченный сотрудник школы получает СКЗИ непосредственно у их производителя или организации, предоставляющей СКЗИ. Безопасность в процессе доставки обеспечивается организационными мерами.

3.2. При транспортировке СКЗИ, носителей с дистрибутивами СКЗИ должны быть обеспечены условия, исключающие возможность физических повреждений и внешнего воздействия на записанную информацию, а также ее копирование.

3.3. Все поступающие СКЗИ, носители с дистрибутивами СКЗИ, эксплуатационная и техническая документация к ним должны браться на учет в специальных журналах установленной формы, ведение которых относится к компетенции уполномоченного сотрудника.

3.4. Носители с дистрибутивами СКЗИ должны храниться в сейфе (металлическом шкафу, хранилище).

3.5. При вскрытии сейфа, в котором хранятся носители с дистрибутивами СКЗИ, должна быть проверена целостность печатей и/или замков и/или оттисков печатей. В случае нарушения целостности печатей и/или замков и/или оттисков печатей сотрудник обязан немедленно сообщить об этом лицу, ответственному за обеспечение безопасности эксплуатации СКЗИ.

3.6. Хранение носителей с дистрибутивами СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

3.7. В случае отсутствия у сотрудника индивидуального хранилища носители с дистрибутивами СКЗИ по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

3.8. Не допускается:

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, не имеющим к ним допуска, выводить ключевую информацию на дисплей и принтер; вставлять ключевой носитель в дисковод ИСПДн при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровка информации, заверение файлов ЭП, подтверждение ее подлинности), а также в дисководы других ИСПДн;
- записывать на ключевом носителе постороннюю информацию;
- вносить какие-либо изменения в программное обеспечение средств шифрования и ЭП;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

3.9. Посторонние лица не должны допускаться к работе с компьютером, на котором установлены СКЗИ.

3.10. Пользователь СКЗИ несет ответственность за проведение в полном объеме

организационных и технических мероприятий, обеспечивающих выполнение настоящей инструкции по обращению.

4. Установка и эксплуатация средств криптографической защиты информации

4.1. Установка (инсталляция) СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

4.2. Установка СКЗИ производится только лицами, имеющими соответствующие полномочия и подготовку (приложение 2 к инструкции по обращению с криптографическими средствами защиты информации).

4.3. К эксплуатации СКЗИ и средств ЭП допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на данные СКЗИ.

4.4. Перед установкой СКЗИ необходимо проверить программное обеспечение ИСПДн на отсутствие вирусов и программных закладок.

4.5. Системные блоки ИСПДн с установленными СКЗИ должны опечатываться специально выделенной для этих целей печатью. Наряду с этим допускается применение других средств контроля их вскрытия.

4.6. Размещение и установка СКЗИ осуществляются в соответствии с требованиями документации на СКЗИ. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

4.7. Перед непосредственной установкой программного обеспечения СКЗИ необходимо осуществить контроль целостности дистрибутива. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления ежедневного контроля установленного программного обеспечения, а также его окружения.

4.8. В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на ИСПДн с СКЗИ должна быть прекращена. По данному факту должно быть проведено служебное расследование и проведены работы по анализу и ликвидации негативных последствий данного нарушения.

4.9. Пересылка (передача) носителей криптоключей может осуществляться через фельдъегерскую или специальную связь, а также в специально выделенном нарочному и опечатанном ответственным лицом конверте.

4.10. Ключевая информация на носителях уничтожается оператором СКЗИ путем переформатирования с использованием средств ЭП. После переформатирования допускается использование данных носителей операторами СКЗИ при условии записи на них новой ключевой информации.

4.11. Операторы СКЗИ делают запись об уничтожении ключей в соответствующем журнале учета экземпляров средств криптографической защиты информации и средств защиты информации школы (приложение 1 к инструкции по обращению с криптографическими средствами защиты информации). Ответственное лицо периодически проверяет данные записи.

4.12. Перед уничтожением секретных ключей следует расшифровать архивную информацию, хранящуюся в зашифрованном виде, и зашифровать ее, используя новые ключи.

4.13. Выведенные из эксплуатации открытые ключи ЭП сохраняются в архивах в течение 5 (пяти) лет для обеспечения в последующем возможности выполнения процедуры разбора конфликтных ситуаций.

5. Восстановление конфиденциальной связи после компрометации действующих криптоключей

5.1. Компрометация ключевой информации - это утрата или хищение действующих криптоключей (в том числе с их последующим обнаружением), разглашение или несанкционированное копирование ключевой информации, передача действующих криптоключей по линии связи в открытом виде, угроза разглашения ключевой информации вследствие увольнения

по любой причине сотрудника, имеющего к ней доступ, а также любые другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

5.2. К событиям, связанным с компрометацией криптоключей, относятся следующие:

1. утрата ключевых носителей;
2. хищение ключевых носителей;
3. обнаружение ключевых носителей после утраты или хищения;
4. увольнение сотрудников, имевших доступ к ключевой информации;
5. нарушение правил хранения и уничтожения секретного ключа;
6. возникновение подозрений на утечку информации или ее искажение;
7. нарушение печати на сейфе с ключевыми носителями;
8. случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и при этом не исключаются несанкционированные действия злоумышленника).

5.3. Первые четыре события должны трактоваться как явная компрометация криптоключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

5.4. При обнаружении признаков, указывающих на возможную компрометацию закрытых ключей, носителей и/или конфиденциальной информации, оператор СКЗИ должен самостоятельно определить факт компрометации и оценить значение этого события, после чего немедленно оповестить.

5.5. Лицо, ответственное за обеспечение безопасности эксплуатации СКЗИ, обязано сообщить о компрометации закрытых ключей, носителей и/или конфиденциальной информации руководителю школы.

5.6. Лицо, ответственное за обеспечение безопасности эксплуатации СКЗИ, обязано оперативно оповестить всех операторов СКЗИ о факте (или предполагаемой) компрометации.

5.7. Расследование факта (или предполагаемой) компрометации должно проводиться на месте происшествия уполномоченными лицами.

5.8. Результатом расследования является квалификация или отказ в квалификации данного события как компрометации действующих криптоключей.

5.9. При установлении факта компрометации действующих криптоключей скомпрометированные секретные ключи шифрования уничтожаются.

5.10. Ответственное лицо должно оповестить остальных операторов СКЗИ о замене скомпрометированных криптоключей.

6. Права и ответственность за нарушение требований инструкции по обращению с криптографическими средствами защиты информации

6.1. Оператор СКЗИ имеет право:

- запрашивать и получать от сотрудников школы сведения, справочные и другие материалы, необходимые для осуществления его деятельности.
- принимать участие в совещаниях по вопросам, входящим в его компетенцию (по решению руководителя школы);
- участвовать в семинарах (конференциях и т.п.) на темы информационных технологий и защиты информации в качестве слушателя;
- ставить перед руководством школы вопросы о создании надлежащих условий для исполнения своих должностных обязанностей.

6.2. Ответственное лицо имеет право:

- требовать от операторов СКЗИ безусловного соблюдения установленной технологии обработки электронных документов и выполнения инструкций по обращению и обеспечению безопасности информации;
- инициировать обращение к руководству школы с требованием о прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования СКЗИ, средств и систем защиты информации;

- запрашивать и получать от операторов СКЗИ и/или администрации школы сведения, справочные и другие материалы, необходимые для осуществления его деятельности;

- принимать участие в совещаниях по вопросам, входящим в его компетенцию (по решению руководителя школы);

- участвовать в семинарах (конференциях и т.п.) об информационных технологиях и защите информации в качестве слушателя;

- вносить руководству школы предложения по совершенствованию деятельности в области шифрования информации;

- ставить перед руководством школы вопросы о создании надлежащих условий для исполнения своих обязанностей.

6.3. Оператор СКЗИ несет ответственность (дисциплинарную, административную, материальную, уголовную) за:

- разглашение конфиденциальной информации, к которой он допущен, рубежи ее защиты, в том числе сведения о криптоключах;

- несоблюдение требований по обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

- необеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ;

- несоблюдение регламента эксплуатации СКЗИ;

- неинформирование руководства школы о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним, а также о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой конфиденциальной информации;

- ненадлежащее и несвоевременное выполнение своих функциональных обязанностей;

- необеспечение сохранности принимаемой и достоверности передаваемой информации;

- несвоевременное, а также некачественное исполнение документов и поручений руководства ШКОЛЫ;

- нерациональное использование выделенных финансовых, материальных и информационно-вычислительных ресурсов.

6.4. Ответственное лицо несет уголовную, административную, дисциплинарную, гражданско-правовую и материальную ответственность, предусмотренную законодательством Российской Федерации, за:

- несоблюдение требований к обеспечению безопасности информации ограниченного доступа с использованием СКЗИ;

- необеспечение сохранности принятых на ответственное хранение программных и технических СКЗИ;

- несоблюдение регламента эксплуатации СКЗИ;

- неинформирование директора о ставших ему известных попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документов к ним, а также о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ;

- ненадлежащее и несвоевременное выполнение своих функциональных обязанностей;

- несвоевременное, а также некачественное исполнение документов и поручений руководства ШКОЛЫ;

- нерациональное использование выделенных финансовых, материальных информационно - вычислительных ресурсов.

Приложение 1
к Инструкции по обращению с криптографическими
средствами защиты информации,
утверждено приказом директора от 30.08.2019 г. №
69/1

Ж У Р Н А Л
учета экземпляров средств криптографической защиты информации и средств защиты информации

гимназии «Альбертина»

Журнал начат « »	_____ 20___г.	Журнал завершен « »	20 г.
Должность		Должность	
/	_____ /	/	/

Журнал учета СЗИ

№	Регистрационный номер	Наименование	Сведения об установке средства защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	Ф.И.О. производившего установку, подпись	Дата изъятия / удаления	Ф.И.О. производившего изъятие / удаление, подпись	Причина изъятия / удаления	
1									
2									

Журнал учета СКЗИ

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов		
				От кого получены	Дата и номер сопроводительного письма	Ф.И. О. пользователя СКЗИ	Дата и расписка в получении (установку)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении
1													
2													

Приложение 2
к Инструкции по обращению с криптографическими
средствами защиты информации,
утверждено приказом директора от 30.08.2019 г. №
69/1

**Форма о подготовке и допуске к самостоятельной работе
со средствами криптографической защиты информации**

_____
(Должность, фамилия, имя, отчество сотрудника)

_____
(Наименование СКЗИ, по которому осуществлялась подготовка)

Подготовка начата_____, окончена_____.

Оператор СКЗИ обязан:

- не разглашать конфиденциальную информацию, к которой допущен, рубежи ее защиты, в том числе сведения о криптоключах;
- соблюдать требования по обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- сообщать сотруднику, ответственному за эксплуатацию СКЗИ, сведения о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей сотрудников, связанных с использованием СКЗИ;
- немедленно уведомлять ответственного за обеспечение безопасности эксплуатации средств криптографической защиты информации о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Заключение - указать степень усвоения пройденного материала, результаты выполнения контрольных работ, возможность допуска к самостоятельной работы со СКЗИ.

С заключением ознакомлен(а):

_____(Подпись)_____(ФИО)

Приложение № 16
Утверждено приказом
директора
гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам автоматизированной системы

гимназии «Альбертина»

1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику школы, допущенному к работе с конкретной подсистемой автоматизированной системы (далее АС) должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет работать в системе. Сотрудникам, в случае производственной необходимости, могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в АС одного и того же имени пользователя (—группового имени") запрещено.

2. Процедура регистрации (создания учетной записи) пользователя для сотрудника школы и предоставления ему (или изменения его) прав доступа к ресурсам АС инициируется заявкой начальника отдела, в котором работает данный сотрудник. Форма заявки приведена в приложении №1 к инструкции «По внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам автоматизированной системы школы ».

3. В заявке указывается:

3.1. Содержание запрашиваемых изменений (регистрация нового пользователя АС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам АС ранее зарегистрированного пользователя).

3.2. Должность, фамилия, имя и отчество сотрудника.

3.3. Имя пользователя (учетной записи) данного сотрудника.

4. Полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю.

5. Заявку визирует заместитель руководителя школы, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам АС.

Приказ №476 от 30.12.2019г.

6. На основании заявки администратор сети производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к сетевым ресурсам АС, включению его в соответствующие задачам группы пользователей и другие необходимые действия. Учетные записи всех пользователей должны быть —привязаны" к конкретным АРМ.

7. Заключительным этапом удовлетворения заявки, является издание приказа по школе о наделении сотрудника правами пользователя конкретной ИСПДн (с указанием конкретного перечня прав).

8. Исполненные заявки должны находиться у лица ответственного за организацию работы по защите персональных данных. Они могут впоследствии использоваться:

8.1. Для восстановления и полномочий пользователей после аварий в АС.

8.2. Для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам системы при разборе конфликтных ситуаций.

Приказ№69/1 от 30.08.2019

Приложение № 1
к инструкции по внесению изменений в списки
пользователей и наделению их полномочиями
доступа к ресурсам автоматизированной системы
школы утверждено приказом директора от
30.08.2019 г. № 69/1

Заявка
на допуск к информационным ресурсам конфиденциального характера автоматизированных систем гимназии «Альбертина»

Прошу допустить сотрудника _____

_____
(должность, ФИО сотрудника, № кабинета, рабочий телефон)

1. К нижепоименованным информационным ресурсам гимназии

_____
(наименование программы, файла, массива, архива, базы данных и т.п.)

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

2. К информации, содержащейся в почтовом ящике гимназии (отдела)_____
(с полномочиями на чтение, изменение, копирование, удаление, размножение) необходимое подчеркнуть

3. К информации, содержащейся на диске межсетевого обмена (First)

_____
(наименование папки отдела, файла)

с полномочиями на чтение, изменение, копирование, удаление, размножение
необходимое подчеркнуть

4. К принтерам общего пользования _____

Заместитель директор гимназии _____

Приказ №476 от 30.12.2019 г.

_____
(должность, ФИО, подпись.) _____ «____» 20____г.

СОГЛАСОВАНО: _____

ответственный за информационную безопасность гимназии

Приложение № 17
Утверждено приказом
директора гимназии
«Альбертина»
от 30.08.2019 г. № 69/1

Инструкция
пользователя по обеспечению безопасности обработки персональных данных
при возникновении внештатных ситуаций

1. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных (далее-ИСПДн) в гимназии «Альбертина» (далее - гимназия) меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

- определение мер защиты от прерывания;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников школы, имеющих доступ к ресурсам ИСПДн.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

Все нештатные ситуации заносятся в журнал «учета нештатных ситуаций, фактов вскрытия и опечатывания, выполнения профилактических работ, установки и модификации аппаратных и программных средств» (приложение 1 к Инструкции пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций).

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники гимназии предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с руководителями структурных подразделений. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 - Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 - Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

- отказ элементов ИСПДн и средств защиты из-за:
- повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;
- сбоя системы кондиционирования.
- отсутствие администратора ИСПДн и администратора безопасности более чем на сутки из-за:
- химического выброса в атмосферу;
- сбоев общественного транспорта;
- эпидемии;

- массового отравления персонала;
- сильного снегопада;
- торнадо;
- сильных морозов.

Уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к прерыванию работоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки в непосредственной близости.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн
включают:

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

Все критичные помещения школы (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.2. Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников школы, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение должностных лиц школы, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администраторы ИСПДн и администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.