


Министерство образования и науки Чеченской Республики
Частное общеобразовательное учреждение
«Гимназия Ринэйсэнс»

ПРИНЯТО: на Педагогическом совете ЧОУ «Гимназия Ринэйсэнс» Протокол № <u>1</u> от « <u>28</u> » <u>08</u> 20 <u>23</u> г.	СОГЛАСОВАНО: с Родительским советом ЧОУ «Гимназия Ринэйсэнс» Протокол № <u>1</u> от « <u>28</u> » <u>08</u> 20 <u>23</u> г.	УТВЕРЖДАЮ: Директор ЧОУ «Гимназия Ринэйсэнс» П.Р. Магамедова Приказ № <u>1/18</u> от « <u>28</u> » <u>08</u> 20 <u>23</u> г.
СОГЛАСОВАНО: с Общим собранием работников ЧОУ «Гимназия Ринэйсэнс» Протокол № <u>1</u> от « <u>28</u> » <u>08</u> 20 <u>23</u> г.		

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите персональных
данных при их обработке в информационных системах персональных
данных Частного общеобразовательного учреждения
«Гимназия Ринэйсэнс»

1. Общие положения

- 1.1. Положение о порядке организации и проведения работ по защите персональных данных при их обработке в информационных системах персональных данных в Частном общеобразовательном учреждении «Гимназия Ринэйсэнс» (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
- 1.2. Настоящее Положение определяет порядок организации работ, а также средства и меры по обеспечению безопасности персональных данных при их в обработке информационных системах в персональных данных Частном общеобразовательном учреждении «Гимназия Ринэйсэнс» (далее - ОУ).
- 1.3. В Положении используются следующие основные понятия:
 - 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);
- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- обезличивание персональных данных - действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;
- обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- оператор - государственный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2. Организация работ по обеспечению безопасности персональных данных

- 2.1. Безопасность персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн) обеспечивается с помощью системы защиты, включающей организационные и технические меры по защите персональных данных. Выбор и реализация методов и способов защиты персональных данных в ИСПДн осуществляется на основе ее класса исходя из угроз безопасности персональных данных.
- 2.2. Система защиты персональных данных ОУ должна обеспечивать:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа (далее - НСД) к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
 - своевременное обнаружение фактов НСД к персональным данным;
 - недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
 - возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
 - постоянный контроль обеспечения уровня защищенности персональных данных.
- 2.3. Разработка и проведение мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, осуществляется силами и средствами ОУ либо сторонними организациями на договорной основе, имеющими лицензии на право проведения работ по технической защите конфиденциальной информации.
- 2.4. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах ОУ приказом уполномоченного лица назначается администратор безопасности ИСПДн. В своей деятельности администратор безопасности руководствуется положениями внутренних документов ОУ, регламентирующих вопросы защиты персональных данных.
- 2.5. ИСПДн ОУ классифицируются в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 1 ноября 2012 г. № 1119.
- 2.6. Угрозы безопасности персональных данных при их обработке в ИСПДн определяются исходя из наличия вероятного нарушителя, возможных способов и средств реализации угроз. На их основе в соответствии с методическими документами Федеральной службы по техническому и экспортному контролю формируются модели угроз.
- 2.7. Моделями угроз необходимо руководствоваться на всех этапах жизненного цикла ИСПДн ОУ: при проектировании, вводе в эксплуатацию, в режиме эксплуатации, при модернизации, а также при проведении регламентных и ремонтно-профилактических работ.

3. Средства и меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

- 3.1. ОУ при обработке персональных данных принимает необходимые правовые, организационные и технические меры 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.

- 3.2. Средства защиты информации (далее - СрЗИ), применяемые в ИСПДн ОУ в установленном законодательством Российской Федерации порядке проходят процедуру оценки соответствия.
- 3.3. СрЗИ, эксплуатационная и техническая документация к ним подлежат учету в соответствии с определенным в ОУ порядком.
- 3.4. Все работы по установке, монтажу, испытанию и ремонту СрЗИ должны производиться ОУ при наличии лицензии на деятельность по технической защите конфиденциальной информации либо сторонней организацией, имеющей такую лицензию.
- 3.5. Установка и ввод в эксплуатацию средств защиты осуществляется в соответствии с эксплуатационной и технической документацией на данные СрЗИ.
- 3.6. Контроль соблюдения порядка и условий использования СрЗИ, предусмотренных эксплуатационной и технической документацией, возлагается на администратора безопасности ИСПДн.
- 3.7. Работники ОУ, использующие СрЗИ, применяемые в ИСПДн, должны быть обучены правилам работы с ними.
- 3.8. Для обеспечения безопасности персональных данных при их обработке в ИСПДн ОУ применяются следующие организационные меры:
 - обеспечение учета, хранения, обращения и уничтожения машинных носителей персональных данных;
 - ознакомление работников с внутренними требованиями ОУ по защите персональных данных;
 - обеспечение контроля доступа в помещения, в которых находятся технические средства обработки персональных данных, хранятся носители персональных данных;
 - размещение технических средств обработки персональных данных в пределах контролируемой зоны;
 - обеспечение пропускного режима на территорию ОУ, охраны помещений с установленными техническими средствами обработки персональных данных.
- 3.9. Для обеспечения безопасности персональных данных при их обработке в ИСПДн ОУ применяются следующие технические меры:
 - установление и реализация правил доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты персональных данных;
 - регистрация и учет действий пользователей, совершаемых с персональными данными в ИСПДн;
 - применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных;

- осуществление антивирусного контроля;
 - обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
 - применение средств межсетевое экранирования;
 - применение средств обнаружения и предотвращения вторжений;
 - анализ защищенности ИСПДн ОУ с применением специализированных программных средств (сканеров безопасности);
 - централизованное управление системой защиты персональных данных.
- 3.10. С целью поддержания достигнутого уровня защищенности персональных данных в ОУ реализована система контроля применяемых мер по защите ПДн. В ходе мероприятий по контролю осуществляется:
- проверка выполнения требований нормативных документов по защите персональных данных;
 - оценка обоснованности и эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
 - систематическое проведение мониторинга действий пользователей, доведение его результатов до сведения руководства ОУ, проведение разбирательств и составление заключений по фактам нарушения требований безопасности персональных данных.
- 3.11. Перечень мероприятий по контролю, его периодичность, а также ответственные лица устанавливаются Планом внутренних проверок состояния защиты ПДн.
- 3.12. Внутренний контроль принимаемых в ОУ мер по обеспечению безопасности персональных данных и уровня защищенности ИСПДн организует и осуществляет лицо, ответственное за обеспечение безопасности персональных данных.
- 3.13. Для проведения внешнего контроля и аудита безопасности персональных данных ОУ на договорной основе может привлекаться сторонняя организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации.

4. Организация резервного копирования и восстановления персональных данных

- 4.1. В целях обеспечения непрерывности деятельности и (или) восстановления функционирования ИСПДн в ОУ применяется система резервного копирования и восстановления данных.
- 4.2. Практическое решение задач, связанных с резервированием и восстановлением персональных данных возлагается на администраторов баз данных и администратора безопасности.

- 4.3. Для реализации функции восстановления баз данных осуществляется периодическое резервное копирование информации на внешние машинные носители информации.
- 4.4. Восстановление информации производится в случае ее частичной или полной утраты путем переноса данных с резервных копий на основные носители в соответствии с эксплуатационной документацией на используемую систему восстановления данных. По завершении восстановления осуществляется проверка работоспособности и целостности данных.
- 4.5. В случае применения системы «горячего резервирования» дальнейшая работа может производиться на дублирующем оборудовании. В этом случае данное оборудование переводится в разряд основного, а восстановленная система выполняет функции «горячего резерва».
- 4.6. При нарушении целостности (полной утрате) системного и (или) прикладного программного обеспечения его восстановление производится с исходных дистрибутивов.
- 4.7. В целях реализации возможности восстановления системы защиты персональных данных предусматривается ведение двух копий программных компонентов СрЗИ, их периодическое обновление и контроль работоспособности.
- 4.8. По всем случаям утраты персональных данных проводится анализ причин инцидента с составлением заключения в свободной форме. При этом первичная диагностика выполняется до начала процесса устранения, а по его завершению проводится полная диагностика ИСПДн.

5. Организация режима безопасности технических средств обработки персональных данных

- 5.1. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СрЗИ, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
- 5.2. Хранение машинных носителей информации должно осуществляться в запираемых шкафах, исключающих НСД к ним.
- 5.3. Размещение технических средств обработки персональных данных, в помещениях, в которых они установлены, должно осуществляться таким образом, чтобы была исключена возможность НСД к ним, в том числе просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.
- 5.4. Режим охраны помещений устанавливается исходя из внутреннего трудового распорядка.

- 5.5. Контроль соблюдения установленного режима работы в повседневной деятельности и охраны помещений возлагается на директора.
- 5.6. По окончании рабочего дня помещения закрываются на ключ.
- 5.7. Функции по организации пропускного режима на территорию ОУ или их часть могут выполняться сторонней организацией на основании договора. Договором должен быть определен порядок пропуска лиц на территорию ОУ, вноса и выноса имущества, а также охраны помещений в нерабочее время.
- 5.8. Допуск посетителя на территорию ОУ осуществляется при предъявлении документа, удостоверяющего его личность (паспорта, водительского удостоверения).

6. Заключительные положения

- 6.1. Иные права и обязанности работников, допущенных к обработке персональных данных с использованием средств автоматизации, определяются также их должностными инструкциями.
- 6.2. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством.
- 6.3. Данное Положение действует на основе законодательства Российской Федерации до внесения в них изменений и дополнений либо замены новым.