Приложение к приказу МБОУ «Северский лицей»
От 05.05.2026 № 75(од)

Утверждено приказом директора
МБОУ «Северский лицей»
от 05.05.2026 № 75 (од)

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ЭЛЕКТРОННОМ ВИДЕ В МБОУ «СЕВЕРСКИЙ ЛИЦЕЙ»

I. Общие положения

1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных (далее ИСПДн) Муниципальное бюджетное общеобразовательное учреждение «Северский лицей» (далее МБОУ «Северский лицей»), от несанкционированного доступа, неправомерного их использования или утраты.

2. Положение определяет обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

3. Положение разработано на основании ст.24 Конституции Российской Федерации, Федерального закона Российской Федерации «О персональных данных» № 152-ФЗ от 27.07.2006 г., закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., нормативных правовых актов Российской Федерации в области трудовых отношений.

4. В настоящем Положении используются следующие основные понятия:

1) Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) – работнику, абитуриенту, обучающемуся, выпускнику;

2) Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

3) 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;

4) 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;

5) 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;

6) Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

7) 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;

8) Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

9) Информационная система персональных данных (далее 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;

10) 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;

11) Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

12) 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.

5. Персональные данные обрабатываются в МБОУ «Северский лицей» для осуществления основной деятельности МБОУ «Северский лицей» и кадрового учета работников.

6. Оператором персональных данных является МБОУ «Северский лицей».

7. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.

8. Персональные данные являются конфиденциальными.

9. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания и в отношении общедоступных персональных данных.

II. Порядок получения и обработки персональных данных.

10. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений, защиты персональных данных, нормативными и распорядительными документами МБОУ «Северский лицей», на основе согласия субъектов на обработку их персональных данных.

11. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальной и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни.

12. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции

почтовой связью и в иных случаях, предусмотренных законодательством Российской Федерации

13. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации.

14. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

15. В случае достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами.

16. Правила обработки и использования конкретных персональных данных устанавливаются отдельными регламентами и инструкциями МБОУ «Северский лицей».

17. Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных.

18. Перечень отдельных должностей, имеющих право на обработку персональных данных предоставляется работникам должностным лицам, определенным отдельными Приказами, распорядительными документами и иными письменными указаниями директора МБОУ «Северский лицей».

19. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями МБОУ «Северский лицей».

III. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных.

20. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

21. На получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

22. Требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

23. На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

24. На обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

25. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

26. Обязанности Оператора при сборе персональных данных:

1) В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2) В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3) В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

4) В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

5) В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6) В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в подпунктах 3 - 5, Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

27. Права Оператора на передачу персональных данных третьим лицам.

1) Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации

2) Передача персональных данных субъекта третьим лицам должна производится в соответствии с Регламентом передачи персональных данных третьим лицам (Приложение 1).

IV. Ответственность за разглашение персональных данных.

28. Оператор, а также должностные лица, виновные в нарушении требований Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

29. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.

V. Особенности обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации.

30. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

31. Не допускается обработка персональных данных в ИСПДн с использованием средств автоматизации при отсутствии установленных и настроенных средств защиты информации;

32. Работники учреждения обязаны соблюдать правила и технологии обработки информации в ИСПДн, отраженные в нормативных документах, принятых приказом руководителя учреждения.

33. Для входа в информационную систему персональных данных работник учреждения должен ввести имя и пароль. Не допускаются режимы безпарольного (гостевого) доступа к какой-либо информации, содержащейся в информационной системе персональных данных.

VI. Порядок обработки персональных данных на внешних электронных носителях

34. Обработка персональных данных может осуществляться в виде документов в электронном виде (файлы, базы данных) на внешних электронных носителях информации.

35. При обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

36. Электронные носители информации, содержащие персональные данные, используются в соответствии с Инструкцией по порядку учета и хранения съемных носителей персональных данных и учитываются в журнале учета.

37. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

38. При несовместимости целей обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

39. Внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

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 (удаление, вымарывание).

VII. Основные принципы построения системы комплексной защиты информации.

40. Построение системы обеспечения безопасности персональных данных информационных систем персональных данных МБОУ «Северский лицей» и их 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.

41. Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных (далее СЗПДн) МБОУ «Северский лицей» в соответствии с действующим законодательством в области защиты персональных данных и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал информационных систем персональных данных МБОУ «Северский лицей» должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту персональных данных.

42. Системность

Системный подход к построению СЗПДн МБОУ «Северский лицей» предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информационной системы персональных данных МБОУ «Северский лицей».

43. Комплексность

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

44. Непрерывность защиты персональных данных

Защита персональных данных – 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 информационной системы персональных данных.

ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационных систем персональных данных в незащищенное состояние.

45. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем персональных данных в целом и ее системы защиты информации, в частности.

46. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем персональных данных 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.

47. Персональная ответственность

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

48. Принцип минимизации полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

49. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе, обеспечивающих деятельность информационных систем персональных данных МБОУ «Северский лицей», для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

50. Гибкость системы защиты персональных данных

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.

51. 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.

52. 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 информационной системы персональных данных.

53. Научная обоснованность и техническая реализуемость

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

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

54. Специализация и профессионализм

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

55. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных 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.

VIII. Меры, методы и средства обеспечения требуемого уровня защищенности

56. Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационных систем персональных данных подразделяются на:

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

57. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных 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.

58. 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.

59. Организационные (административные) меры защиты.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования информационных систем персональных данных, использование ресурсов информационных систем персональных данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с информационными системами персональных данных 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 персональных данных (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация политики информационной безопасности персональных данных в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность рассматриваемых в целом. Эти решения закрепляются в локальных актах МБОУ «Северский лицей». Примером таких решений могут быть:

1) принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, определение ответственных за ее реализацию;

2) формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;

3) принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне МБОУ «Северский лицей» в целом;

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

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

На организационном уровне определяются процедуры и правила достижения целей и решения задач политики информационной безопасности персональных данных. Эти правила определяют:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных, а так же их установить ответственность;
- кто имеет права доступа к персональным данным;
- какими мерами и средствами обеспечивается защита персональных данных;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

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

2) определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;

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

4) организовать меры противодействия несанкционированного доступа на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Для осуществления мероприятий по защите персональных данных в ИСПДн учреждением разрабатываются и утверждаются приказом руководителя учреждения соответствующие регламенты и инструкции.

60. Сотрудник, ответственный за защиту ИСПДн и работающий с персональными данными на электронных носителях, ведет следующую документацию:

1) Журнал учета машинных носителей информации;

2) Журнал учета обращений субъектов персональных данных;

3) Инструкцию по порядку учета и хранения съемных носителей персональных данных;

4) Инструкцию об организации учета, хранения и выдачи машинных носителей, содержащих персональные данные ИСПДн.

61. При работе в сети Интернет все работники МБОУ «Северский лицей» должны выполнять требования Регламента использования ресурсов глобальной сети Интернет (Приложение № 2)

62. 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.

Сервер баз данных находится в отдельном помещении, доступ в которое разрешен только работникам, имеющими соответствующее разрешение от руководства организации. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах или металлических шкафах с замками. Вход в помещение осуществляется через дверь, оснащенную замками. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находиться в помещении только в присутствии работников, имеющих право находиться в данном помещении в связи с выполнением своих должностных обязанностей. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется с письменного разрешения директора МБОУ «Северский лицей».

Физическая защита зданий, 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.

63. Аппаратно-программные средства защиты ИСПДн.

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 персональных данных и информационных системах по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

1) средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем персональных данных;

2) средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн;

3) средства обеспечения и контроля целостности программных и информационных ресурсов;

4) обязательное резервирование всей информации, имеющей конфиденциальный характер;

5) дублирование информации с использованием различных физических и аппаратных носителей;

6) средства оперативного контроля и регистрации событий безопасности;

7) криптографические средства защиты персональных данных.

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

1) обеспечена физическая целостность всех компонент информационных систем персональных данных;

2) каждый работник (пользователь) или группа пользователей информационных систем персональных данных имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

3) все изменения конфигурации технических и программных средств информационных систем персональных данных производятся строго установленным порядком (регистрируются и контролируются);

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

5) специалистами МБОУ «Северский лицей» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Приложение № 1
к Положению о защите персональных данных,
обрабатываемых в электронном виде

Регламент предоставления/передачи персональных данных

I. Общие положения.

1. Настоящий регламент (далее - Регламент) устанавливает правила предоставления персональных данных (далее ПДн), обрабатываемых в Муниципальном бюджетном общеобразовательном учреждении «Северский лицей» (далее МБОУ «Северский лицей») и содержащих конфиденциальную информацию, лицам, не являющимся зарегистрированными пользователями ИСПДн или третьим лицам. Основной задачей регламента является формализация процессов передачи ПДн третьим лицам и защита от утечки конфиденциальной информации в соответствии с требованиями Федерального закона Российской Федерации «О персональных данных» № 152-ФЗ от 27.07.2006 г.

2. Под термином Оператор, понимается государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

3. Под термином «Третье лицо» (уполномоченное лицо) понимаются государственные, муниципальные и другие организации, которым на основании договора Оператор передает (поручает обработку) ПДн.

4. Положения регламента обязательны для выполнения всеми работниками учреждения, имеющими доступ к ПДн и взаимодействующими с внешними организациями и лицами, не являющимися работниками МБОУ «Северский лицей». Все пользователи ИСПДн обязаны ознакомиться с настоящим Регламентом под роспись в специальном журнале учета.

5. Документы, содержащие персональные данные, имеющие конфиденциальный характер, не подлежат разглашению (распространению) без разрешения соответствующего должностного лица, уполномоченного относить информацию к разряду информации ограниченного доступа.

6. Поступившие в МБОУ «Северский лицей» документы, разработанные в других организациях, содержащие конфиденциальную информацию, не подлежат разглашению (распространению) без разрешения (письма) соответствующей организации (или его уполномоченного должностного лица), которой данная информация отнесена к конфиденциальной информации (персональным данным).

II. Порядок предоставления информации субъекту персональных данных

7. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

9. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

10. После получения запроса работником МБОУ «Северский лицей», уполномоченный работник в соответствии с запросом осуществляет:

1) снятие копий с документов, содержащих необходимую информацию о персональных данных субъекта;

2) вывод на бумажный носитель необходимой информации, содержащейся в электронном виде в ИСПДн МБОУ «Северский лицей»;

3) формирование полученных документы в личное дело, которое вкладывается в пакет, обеспечивающий конфиденциальность документов, находящихся внутри;

4) доведение до сведения субъекта персональных данных о готовности предоставить информацию о его персональных данных;

5) передачу пакета с личным делом непосредственно субъекту персональных данных или его представителю с пометкой в Журнале учета обращений субъектов персональных данных.

III. Порядок передачи персональных данных третьим лицам

11. Предоставление/передача документов и/или электронных носителей, содержащих конфиденциальную информацию, работникам организаций, не являющимися зарегистрированными пользователями ИСПДн или третьим лицам, осуществляется секретарем руководителя/специалистом по кадрам МБОУ «Северский лицей», либо должностным лицом, ответственным за прием/передачу информации.

12. Передача конфиденциальной информации осуществляется после подписания сторонами «Соглашения о конфиденциальности», если иное не предусмотрено действующим законодательством Российской Федерации.

13. Поступившие в МБОУ «Северский лицей» документы, разработанные в других организациях, содержащие ПДн конфиденциального характера регистрируются в

Журнале учета приема/передачи персональных данных, которые ведутся секретарем руководителя МБОУ «Северский лицей».

14. В случае необходимости передачи персональных данных в электронном виде по открытым каналам связи, должны использоваться криптографические средства защиты информации, режим применения которых должен быть согласован обеими сторонами.

15. Документы, содержащие персональные данные, пересылаются другим организациям заказными или ценными почтовыми отправлениями, а также могут быть переданы курьером.

16. При необходимости направления документов, содержащих персональные данные, нескольким адресатам составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения, подготовившего документ.

17. Для отправления документов, содержащие персональные данные используются пакеты, изготовленные из плотной бумаги. На пакете указываются адрес получателя, а под ним - отправителя корреспонденции и регистрационные номера вложенных в пакет документов.

18. При направлении нескольких экземпляров одного документа на пакете и в реестре после регистрационного номера документа в скобках указываются номера экземпляров.

19. Адресат и другие надписи на пакетах печатаются с помощью печатающего устройства или четко и разборчиво пишутся от руки шариковой ручкой (черного, синего или фиолетового цвета).

20. Должностное лицо, на которое возложены функции по документационному обеспечению, отправляющее документы, содержащие персональные данные, сверяет номера и экземпляры, указанные на документах, с номерами и экземплярами, указанными на пакете и вкладывает в пакет. Пакет запечатывается.

IV. Ответственность

21. Требования Регламента обязательны для выполнения всеми пользователями ПДн МБОУ «Северский лицей»

22. Работники МБОУ «Северский лицей», нарушившие положения данного Регламента, несут административную и/или дисциплинарную ответственность в соответствии с действующим законодательством и/или локальными нормативными актами учреждения и/или условиями трудового договора.

23. За разглашение ПДн конфиденциального характера, а также иные действия, направленные на нарушение защищенности информации и требований по защите информации в ИСПДн МБОУ «Северский лицей» должностные лица могут быть привлечены к ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение № 2
к Положению о защите персональных данных,
обрабатываемых в электронном виде

Регламент использования ресурсов глобальной сети Интернет

Настоящий Регламент разработан для повышения эффективности работы работников Муниципальное бюджетное общеобразовательное учреждение «Северский лицей» (далее МБОУ «Северский лицей»), использующих электронные информационные ресурсы глобальной сети Интернет, и повышения уровня информационной безопасности локальных информационно-вычислительных сетей МБОУ «Северский лицей».

В МБОУ «Северский лицей» устанавливается контроль и специфицируются виды информации, к которым разрешается доступ работников. В случае нарушения работником МБОУ «Северский лицей» данного Регламента он отстраняется от использования ресурсов сети Интернет.

1. Назначение доступа к ресурсам сети Интернет

Доступ к ресурсам сети Интернет предоставляется работникам МБОУ «Северский лицей»» для выполнения ими прямых должностных обязанностей. Глобальная сеть Интернет используется для:

- доступа к гипертекстовым страницам (WWW);
- доступа к файловым ресурсам Интернета (FTP);
- доступа к специализированным (правовым и др.) базам данных;
- ответов на официальные запросы граждан;
- обмена электронной почтой с официальными лицами других структур по неконфиденциальным вопросам производственного характера;
- повышения квалификации работников, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, служебным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей, и др.

2. Доступ к Интернет-ресурсам

МБОУ «Северский лицей» обеспечивает доступ пользователей локальной сети к ресурсам Интернет по специальным каналам связи в соответствии с установленными в МБОУ «Северский лицей» правилами и настоящим Регламентом.

Открытие и контроль доступа регулируется ПАО «Ростелеком». Самостоятельная организация дополнительных точек доступа в глобальную сеть Интернет (удаленный доступ, VPN и пр.) запрещена.

3. Регистрация пользователя

Каждому физически подключенному к сети компьютеру назначается ответственный за этот компьютер пользователь. Подключение выполняется обслуживающей организацией. За все деструктивные действия, произведенные в сети, отвечает работник - пользователь конкретного компьютера.

4. Основные ограничения при работе в сети Интернет

<u>При работе в сети Интеренет запрещается:</u>

- посещение пользователем ресурсов с непристойным и противоправным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию и т.д.);
- посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к деятельности МБОУ «Северский лицей» и деятельности пользователя;
- массовая рассылка не связанных со служебной деятельностью электронных писем (mass mailing). Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю. Здесь и далее под электронными письмами понимаются сообщения электронной почты и других подобных средств личного обмена информацией;
- несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также рассылка писем, содержащих грубые и оскорбительные выражения и предложения;
- использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных для осуществления действий, не связанных с выполнением служебных обязанностей;
- не допускается осуществление попыток несанкционированного доступа к ресурсам сети, проведение или участие в сетевых атаках и сетевом взломе, за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса;
- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю;
- передача компьютерам или оборудованию сети информации, не имеющей отношения к выполнению служебных обязанностей, создающей паразитную нагрузку на рабочие станции локальной сети и (или) оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сетей и доступности отдельных ее элементов.
- передача кому бы то ни было учетных данных пользователя;
- применение имен и паролей учетных записей, используемых в локальной сети МБОУ «Северский лицей», на иных (сторонних) компьютерах;
- установка и использование сетевых и автономных компьютерных игровых приложений на рабочей станции;
- посещение ресурсов трансляции потокового видео и аудио (вебкамеры, трансляция ТВ - и музыкальных программ в Интернете), создающих большую загрузку сети и мешающих нормальной работе остальных пользователей;
- загрузка развлекательных материалов;
- передача конфиденциальной информации третьей стороне;
- подключение к электронной сети под чужим логином и паролем;
- проведение незаконных операций в глобальной сети Интернет;
- любые попытки деструктивных действий по отношению к нормальной работе электронной системы МБОУ «Северский лицей» и ресурсам сети Интернет (рассылка вирусов, ip-атаки и т.п.);
- нарушение закона об авторском праве: копирование и использование материалов и программ, защищенных законом об авторском праве;

– совершение иных действий, противоречащих действующему законодательству Российской Федерации.

5. Соблюдение правил, установленных владельцами ресурсов.

Владелец любого информационного или технического ресурса сети Интернет может установить для этого ресурса собственные правила его использования. Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

6. Недопустимость фальсификации.

Значительная часть ресурсов сети Интернет не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его, и используемые им средства доступа к сети. При этом пользователю запрещается:

- использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа);
- фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в сеть;
- использование несуществующих обратных адресов при отправке электронных писем.

Ответственность за все действия в сети Интернет, произведенные под именем и с паролем пользователя им самим или другими физическими, или юридическими лицами и организациями, полностью лежит на самом пользователе. МБОУ «Северский лицей» не несет никакой юридической, материальной или иной ответственности за качество, содержание, законность и любое другое свойство полученной или переданной пользователем информации в нарушение действующего законодательства Российской Федерации.

МБОУ «Северский лицей» не несет никакой юридической, материальной и иной ответственности за использование пользователем платных услуг других организаций, предоставляющих услуги в сети Интернет.

7. Контроль использования ресурсов сети Интернет

МБОУ «Северский лицей» оставляет за собой право в целях обеспечения безопасности электронной системы производить выборочные и полные проверки всей электронной системы и отдельных файлов без предварительного уведомления работников.