Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа с. Ленинское

УТВЕРЖДЕНО
приказом директора школы
от 12.04.2016 г. № 99

ПОЛОЖЕНИЕ
о порядке организации и проведении работ по защите конфиденциальной информации в МКОУ СОШ с. Ленинское

1. Общие положения

Настоящее Положение о порядке организации и проведения работ по защите конфиденциальной информации в муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа с. Ленинское» (далее Школа) определяет основные принципы, организацию, порядок осуществления работ, основные требования и рекомендации, способы и средства защиты циркулирующей в органе конфиденциальной информации, не содержащей сведения, составляющие государственную тайну (далее - конфиденциальная информация).

1.1 Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Указом Президента РФ № 351 от 17 марта 2008 года "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР- К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282, постановлением Правительства РФ от 17 ноября 2007 г. № 781 "Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и другими нормативно-методическими документами по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

1.2 Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя Школы.

1.3 Разработка мероприятий по защите информации в Школе осуществляется отдельным специалистом, назначаемым руководителем Школы для проведения таких

работ. Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии на право проведения соответствующих работ.

1.4 Сотрудники Школы, осуществляющих работы с использованием конфиденциальной информации, несут персональную ответственность за несоблюдение требований безопасности конфиденциальной информации.

2. Основные термины и понятия

В настоящем Положении используются следующие основные понятия и термины:

Объект защиты - материальный носитель конфиденциальной информации или место его нахождения, подлежащее защите.

Утечка информации - несанкционированное и целенаправленное получение конфиденциальной информации третьими лицами, которые могут ее использовать в своих интересах.

Утрата информации - несанкционированное разглашение конфиденциальной информации или утрата ее носителей субъектами, которым они были доверены

Защита информации - осуществление организационно-технических мероприятий, направленных на предотвращение утечки и утраты конфиденциальной информации.

Пользователь - сотрудник органа, имеющий доступ к информационным ресурсам органа, содержащим конфиденциальную информацию.

3. Цели и задачи разработки и внедрения системы защиты информации

Основными целями и задачами разработки и внедрения системы защиты информации в Школе являются:

предотвращение утечки и утраты информации, а также ее носителей; обеспечение условий быстрого, полного и всестороннего расследования случаев утечки информации;

устранение негативных последствий и условий в случае несанкционированной утечки или утраты информации;

обеспечение оптимальных условий накопления, хранения обработки и использования информации.

4. Объекты защиты информации

4.1. Защите в Школе подлежит(ат) речевая информация и информация, обрабатываемая средствами вычислительной техники (СВТ), носителей на бумажной, магнитной, магнито-оптической и иной основе.

Объектами защиты при этом являются:

-средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети, системы связи и передачи данных, технические средства приема, передачи и обработки информации

(телефонии, звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической и видео-информации, программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки конфиденциальной информации;

- технические средства и системы, не обрабатывающие непосредственно конфиденциальную информацию, но размещенные в помещениях, где она обрабатывается (циркулирует);
- защищаемые помещения,

4.2. Перечень сведений конфиденциального характера (Приложение 1), подлежащих защите, а также Перечень средств информатизации Школы, с использованием которых обрабатывается информация конфиденциального характера, разрабатывается специалистом по защите информации совместно со специалистами, эксплуатирующими указанные средства вычислительной техники, и утверждаются директором Школы.

4.4. Все сотрудники Школы должны быть ознакомлены с Перечнем сведений конфиденциального характера, в части, их касающейся.

4.4. Информационные системы персональных данных, используемые в подразделениях Школы с использованием средств вычислительной техники, должны быть проклассифицированы в соответствии с Приказом ФСБ России, ФСТЭК России и Министерства связи и информатизации России № 55/86/20 от 14 февраля 2008 года. Защита информационных систем персональных данных должна осуществляться в соответствии с требованиями методических документов, утвержденных ФСТЭК России 15 февраля 2008 г.

4.5 Порядок обращения со служебной информацией ограниченного доступа должен осуществляться в соответствии с требованиями Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденного Постановлением Правительства РФ от 4 ноября 1994 г. № 1244.

5. Порядок создания и ввода в действие объектов информатизации, на которых обрабатывается конфиденциальная информация

5.1. Организация работ по созданию и эксплуатации объектов информатизации и их средств защиты состоит из следующих этапов:

- предпроектное обследование объектов информатизации, на которых будет обрабатываться конфиденциальная информация;

- разработка аналитического обоснования необходимости создания средств защиты конфиденциальной информации и технического задания на их создание;

- проектирование объектов информатизации, включая разработку системы защиты информации в их составе;

5.2. Техническое задание на разработку системы защиты информации должно содержать;

- обоснование разработки;

- исходные данные создаваемого объекта информатизации, класс защищенности автоматизированной системы; перечень предполагаемых средств защиты информации; требования к средствам защиты информации на основе нормативно- методических документов и установленного класса защищенности автоматизированной системы.

5.3. На этапе ввода в действие объектов информатизации и системы защиты информации осуществляются:

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности;

приемо-сдаточные испытания средств защиты информации;

6. Источники угроз безопасности информации

6.1. При ведении переговоров и использовании технических средств для обработки и передачи информации возможны следующие каналы утечки и источники угроз безопасности информации:

(п. 6.1.1.-6.13 указываются в том случае если имеются защищаемые помещения)

6.1.1. акустическое излучение информативного речевого сигнала;

6.1.2. электрические сигналы, возникающие при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящим за пределы КЗ;

6.1.3. виброакустические сигналы, возникающие при преобразовании информативного акустического сигнала за счет воздействия его на строительные конструкции и инженерно-технические коммуникации ЗП;

6.1.4. несанкционированный доступ к обрабатываемой в АС информации и несанкционированные действия с ней;

6.1.5. воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;

6.1.6. побочные электромагнитные излучения информативных сигналов от технических средств и линий передачи информации;

6.1.7. наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ;

6.1.8. радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств.-? или при наличии паразитной генерации в узлах (элементах) технических средств;

6.1.9. радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации (закладочные устройства), модулированные информативным сигналом;

6.1.10. радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;

6.1.11. просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;

6.1.12. прослушивание телефонных и радио-переговоров;

6.1.13. хищение технических средств с хранящейся в них информацией или носителей информации.

6.2. Перехват информации или воздействие на нее с использованием технических средств могут вестись:

из-за границы КЗ из близлежащих строений и транспортных средств;

из смежных помещений, принадлежащих другим организациям и расположенных в том же здании, что и объект защиты;

при посещении организации посторонними лицами; за счет

несанкционированного доступа (несанкционированных действий) к информации, циркулирующей в АС, как с помощью технических средств АС, так и через вычислительные сети.

6.3. В качестве аппаратуры перехвата или воздействия на информацию и технические средства могут использоваться портативные возимые и носимые устройства, размещаемые вблизи объекта защиты либо подключаемые к каналам связи или техническим средствам обработки информации, а также электронные устройства съема информации (закладочные устройства), размещаемые внутри или вне защищаемых помещений.

6.4. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, за счет следующих действий:

- непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций, защищаемых помещений и их инженерно-технических систем;

- некомпетентных или ошибочных действий пользователей и администраторов.

7. Классификация автоматизированных систем

7.1. В целях дифференцированного подхода к защите конфиденциальной информации производится классификация автоматизированных систем (АС) по требованиям защищенности в соответствии с требованиями действующих нормативно-методических документов и оформляется актом. Класс защищенности АС может устанавливаться Школой.

В соответствии с руководящими документами Гостехкомиссии России автоматизированные системы, подлежащие защите от несанкционированного доступа, делятся на классы. Различают девять классов защищенности АС от НСД. Классы подразделяются на три группы.

К третьей группе относятся АС, в которой работает один пользователь, допущенный ко всей информации АС. Группа содержит классы - 3 А и ЗБ.

Ко второй группе относятся многопользовательские АС, в которых пользователи имеют одинаковые права доступа ко всей информации различного уровня конфиденциальности. Группа содержит классы - 2А и 2Б.

К первой группе относятся многопользовательские АС, в которых пользователи имеют различные права доступа к информации разного уровня конфиденциальности. Группа содержит классы - 1 А, 1Б, Ш, 1Г, 1Д.

7.2. Пересмотр класса защищенности АС производится в обязательном порядке, если произошло изменение, хотя бы одного из критериев, на основании которых он был установлен.

8. Защита конфиденциальной информации, циркулирующей в информационно-коммуникационных системах

8.1. С целью обеспечения безопасности конфиденциальных данных в сетевых версиях автоматизированных систем, применяется система разграничения доступа- к конфиденциальной информации с помощью программных, средств используемой сетевой операционной системы (ОС). Для этого администратор баз данных должен выполнять следующие мероприятия:

- устанавливать права доступа пользователей к ресурсам в соответствии с требованиями должностных регламентов;

- присваивать пользователям соответствующие, имена и пароли для доступа к конфиденциальной информации, находящейся в локальных сетях, при этом в качестве паролей могут использоваться сочетания букв и цифр общей длиной не менее восьми знаков;
- назначать периодичность смены паролей.

8.2. Включение информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается конфиденциальная информация, к сетям общего пользования, в том числе Интернет, осуществляется в соответствии с требованиями Указа Президента РФ № 351 от 17 марта 2008 года "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена".

8.3. Для обеспечения физической безопасности конфиденциальной информации, циркулирующей в ЛВС, осуществляются следующие мероприятия:

8.3.1. Ограничение доступа посторонних лиц к персональным компьютерам, а также сетевому оборудованию.

8.3.2. Резервное копирование информации, представляющей особую ценность (базы данных).

8.3.3. Периодический контроль ресурсов файл-серверов.

8.3.4. Применение антивирусных средств.

8.3.5. Обеспечение файл-серверов и сетевого оборудования источниками бесперебойного питания.

8.4. С целью обеспечения безопасности конфиденциальных информации, обрабатываемых с использованием средств вычислительной техники, каждый пользователь, обязан выполнять следующие требования:

8.4.1. Подключаться к ресурсам локальных сетей и автоматизированной системы только с закрепленного рабочего места,

8.4.2. При вводе пароля убеждаться, что при наборе гарантируется его конфиденциальность.

8.4.3. При временном убытии с рабочего места и в конце рабочего дня производить отключение от используемых ресурсов или производить перезагрузку операционной системы рабочей станции.

8.4.4. При использовании в работе магнитных носителей информации проверять их перед началом работы средствами антивирусной защиты.

8.4.5. При обнаружении действий, грозящих безопасности информационной системы, немедленно докладывать об этом лицам, ответственным за эксплуатацию данной системы и своему непосредственному начальнику.

9. Методы защиты информации

9.1. Защита информации на объектах информатизации Школы осуществляется по следующим направлениям:

- исключение или существенное затруднение возможности получения заинтересованными' лицами на этапе эксплуатации объектов органа охраняемых сведений;
- защита информации и критичных информационных процессов, в том числе от компьютерных вирусов и других программно-технических воздействий, от хищения технических средств с находящейся в них информацией или отдельных носителей-информации.

В этих целях:

- ограничивается доступ посторонних лиц в помещения, в которых размещаются объекты защиты;
- ремонт ПЭВМ осуществляется в режиме, исключающем считывание записанной или восстановление стертой на жестком диске конфиденциальной информации;
- с учетом классификации автоматизированных систем реализуется комплекс программно-технических мероприятий по управлению доступом к базам данных, регистрации и учета доступа к ресурсам автоматизированных систем, протоколирование всех действий пользователей, выполняемых в автоматизированной системе;

Одновременно с этими организационными и программно-техническими мероприятиями (организация допуска, физическая защита, охрана и т.д.) создаются условия, исключающие возможность хищения технических средств с хранящейся в них информацией или отдельных носителей информации. Путем соответствующего размещения технических средств, оборудования окон помещений, в которых они находятся, шторами или жалюзи должна исключаться возможность просмотра информации с экранов дисплеев и других средств ее отображения с помощью оптических средств.

10. Планирование работ по защите информации т контролю защиты информации

10.1. Работа по защите информации в Школе проводится в соответствии с годовым планом.

10.2. План должен содержать мероприятия по технической защите информации, выполняемые всеми структурными подразделениями Школы эксплуатирующими объекты информатизации, и направленные на выявление и учет факторов, которые воздействуют или могут воздействовать на конфиденциальную информацию.

В план включаются следующие разделы:

10.3.1. Мероприятия по выполнению решений Федеральной службы по техническому и экспортному контролю Российской Федерации;

10.3.2. Обследование объектов информатизации:

- соответствие классов защищенности автоматизированных систем и данных, отраженных в технических паспортах объектов информатизации, условиям, сложившимся на момент проверки;
- проверка выполнения установленных норм и требований по защите информации;
- разработка (совершенствование) системы защиты информации,

10.3.3. Организационно-методическое обеспечение работ по технической защите информации:

- разработка, корректировка и согласование организационно-методических документов, планов, отчетов;
- оценка эффективности принимаемых мер защиты информации на объектах информатизации.

10.3.4. Для каждого мероприятия по защите информации устанавливаются срок исполнения, материально-техническое обеспечение, ответственный за исполнение, ответственный за контроль, отметка о выполнении.

10.4. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

10.5. Контроль защиты информации в Школе осуществляется в целях:

- предупреждения и пересечения возможности получения
- техническими средствами разведки охраняемых сведений об объектах информатизации Школы;
- выявления и предотвращения утечки информации по техническим каналам;
- исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации;
- предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

10.6. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях Школы, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- проверка выполнения установленных норм и требований по защите информации,

- оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите автоматизированных систем от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных рабочих мест;

- проверка знаний должностных лиц по вопросам защиты информации и их соответствия необходимому уровню подготовки для конкретного рабочего места;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации на объектах информатизации Школы.

10.7. Повседневный контроль за выполнением мероприятий по защите информации осуществляет специалист, ответственный за защиту информации.

10.8. Периодический контроль за выполнением мероприятий по защите информация проводится комиссией по категорированию и классификации объектов информатизации Школы совместно со специалистом, ответственным за защиту информации (либо специально создаваемой в этих целях комиссией) не реже одного раза в год. Результаты обследования оформляются актом.

В ходе обследования проверяется:

- соответствие классов защищенности автоматизированных систем условиям, сложившимся на момент проверки;
- соблюдение организационно-режимных требований;
- выполнение требований по защите автоматизированных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите автоматизированных систем и средств вычислительной техники.

10.9. Периодический контроль состояния защиты информации осуществляется при проверке Школы комиссией Управления Федеральной службы по техническому и экспортному контролю Российской Федерации по Дальневосточному Федеральному округу.

Приложение № 1
к приказу № 49
от «12 » апреля 2016 года

Перечень сведений конфиденциального характера в муниципальном казенном общеобразовательном учреждении «Средняя общеобразовательная школа с. Ленинское»

В настоящем Перечне предусматриваются категории сведений, не составляющих государственную тайну, связанных с образовательным процессом МКОУ СОШ с. Ленинское (далее по тексту - Учреждение), разглашение которых может нанести материальный, моральный или иной ущерб интересам Учреждения.

Конкретные исполнители и руководители подразделений несут персональную ответственность за правильность определения сведений, составляющих служебную, коммерческую тайну или персональные данные. При этом они должны руководствоваться Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» в редакции указов Президента Российской Федерации от 23.09.2005 г. N 1И1; от 13.07.2015 г. N 357. Перечнем сведений, которые не могут составлять коммерческую тайну, введенным в действие Постановлением Правительства РСФСР от 05.12.1991 №35 (с изменениями от 03.10.2002), а также настоящим Перечнем.

Гриф «Конфиденциально» на документе проставляется исполнителем.

№ п/п	Перечень сведений	Срок действия
1	**Финансы**	
1.1	Сведения о бухгалтерском учете (за исключением годового баланса).	+3 года после окончания финансового года
1.2	Сведения о финансовых операциях.	-----
1.3	Сведения о величине доходов и расходов, о состоянии дебиторской и кредиторской задолженностях (за исключением годового баланса).	-----
1.4	Сведения, содержащиеся в финансово - договорных схемах Учреждения	+1 год после окончания

		действия договора
2	**Контракты**	
2.1	Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательств Учреждения	По условиям договора
3	**Торги, аукционы**	
3.1	Сведения о подготовке к торгам или аукционов.	+1 год после завершения торгов (аукциона)
4	**Безопасность**	
4.1	Сведения о порядке и состоянии защиты конфиденциальной информации.	постоянно
4.2	Сведения о защищаемых информационных ресурсах в автоматизированной и корпоративной сетях Учреждения	постоянно
4.3	Сведения об охране организации, пропускном и внутри объектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом.	постоянно
5	**Личная безопасность сотрудников**	
5.1	Персональные данные, сведения о фактах, событиях и обстоятельствах частной жизни сотрудника.	постоянно
5.2	Сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда.	На период действия
5.3	Информация о личных отношениях специалистов как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.	3 года