СОГЛАСОВАНО:
на Заседании Совета Учреждения
Протокол №11 от 22.11.2021

ПРИНЯТО:
на Педагогическом совете
Протокол №14 от 23.11.2021 г.

УТВЕРЖДЕНО:
Приказом директора № 01-06/205-осн от 27.12.2021 г.

Копылова Галина Михайловна

Подписан: Копылова Галина Михайловна
DN: CN=Копылова Галина Михайловна, SN=Копылова, G=Галина Михайловна, E=gimnazia6tbux@mail.ru, ИНН=222026611491, СНИЛС=09846702732, O="МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ""СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 103""", T=директор, L=Барнаул, S=Алтайский край, C=RU
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2023.04.28 12:51:11+07'00'
Foxit Reader Версия: 10.1.1

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите информации в информационных системах МБОУ «СОШ № 103»

1. Общие положения

1.1. Настоящий Порядок организации и проведения работ по защите информации в информационных системах (далее – Порядок) разработан с целью соблюдения надлежащих правил обращения с указанной информацией в муниципальном бюджетном общеобразовательном учреждении «СОШ № 103» (далее – МБОУ «СОШ № 103») и определяет единый для всех пользователей информационных систем МБОУ «СОШ № 103», порядок допуска к этим сведениям, а также меры ответственности, применяемые за нарушение требований, установленных настоящим Порядком.

1.2. Настоящий Порядок разработан на основе действующего законодательства Российской Федерации, в том Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», указа президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и других законодательных и нормативно-правовых актов, регулирующих вопросы защиты информации.

1.3. В настоящем Порядке отражены вопросы защиты:

– информационных систем персональных данных;

– других информационных систем, обрабатывающих сведения конфиденциального характера.

Общее название информации, обрабатываемой в данных системах, употребляемое в настоящем Порядке – защищаемые информационные ресурсы.

1.4. Защищаемые информационные ресурсы могут быть представлены в виде отдельных документов и отдельных массивов документов (на бумажных носителях), а также в виде документов (файлов) и массивов документов в информационных системах (библиотеках, архивах, фондах, банках данных и т.п.).

1.5. Действие настоящего Порядка распространяется на сотрудников МБОУ «СОШ № 103», работающих по трудовому договору (служебному контракту), заключенному с МБОУ «СОШ № 103», которые дали обязательство о неразглашении конфиденциальной информации, а также на лиц, работающих по гражданско-правовым договорам, заключенным с МБОУ «СОШ № 103» взявших на себя обязательство о неразглашении конфиденциальной информации, в порядке и на условиях, предусмотренных настоящим Порядком.

1.6. Порядок не распространяется на порядок обращения с документами, содержащими сведения, составляющие государственную тайну.

2. Перечень используемых определений, обозначений и сокращений

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

АТС – автоматическая телефонная станция.

ВТСС – вспомогательные технические средства и системы.

ЗП – защищаемое помещение.

КЗ – контролируемая зона.

КИ – конфиденциальная информация.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

ОТСС – основные технические средства и системы.

ПЭМИН – побочные электромагнитные излучения и наводки.

РФ – Российская Федерация.

СВТ – средства вычислительной техники.

СЛЗ – средства линейного электромагнитного зашумления.

СПЗ – системы электромагнитного пространственного зашумления

ТКУИ – технические каналы утечки информации.

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).

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к конфиденциальной информации – процедура оформления права работника МБОУ «СОШ № 103» для ознакомления со сведениями, относящимися к конфиденциальным.

Доступ к информации – возможность получения информации и ее использования.

Доступ к конфиденциальной информации – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита конфиденциальной информации – деятельность, направленная на предотвращение несанкционированного доступа к конфиденциальной информации и (или) её утечки.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Контрагент – сторона гражданско-правового договора, которой обладатель КИ передал эту информацию;

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обладатель конфиденциальной информации – лицо (физическое или юридическое), которое владеет сведениями, отнесенным к конфиденциальным, на законном основании, ограничило доступ к ним и установило в отношении ее режим конфиденциальности;

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, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен

Передача конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Предоставление конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Разглашение конфиденциальной информации – действие или бездействие, в результате которых сведения, отнесенные к конфиденциальным, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

3. Принципы отнесения сведений к категории конфиденциальных, состав защищаемой информации

3.1. К категории конфиденциальных относятся сведения:

– не относящиеся к сведениям, указанным в «Перечне сведений, которые не могут составлять коммерческую тайну», утвержденным постановлением Правительства РСФСР от 05.12.1991 № 35 (в ред. постановления Правительства РФ от 03.10.2002 № 731);

– не относящиеся к сведениям, составляющим государственную тайну;

– не защищенные действующим законодательством (авторским, патентным правом и т.п.);

– в отношении, которых МБОУ «СОШ № 103» обязано обеспечить реализацию необходимых мер защиты (персональные данные, служебная тайна);

– монопольное обладание, которыми позволяет МБОУ «СОШ № 103» при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

3.2. Сведения, отнесенные к конфиденциальным оформляются в виде «Перечня сведений конфиденциального характера МБОУ «СОШ № 103» (далее – Перечень сведений).

3.3. Перечень сведений конфиденциального характера должен включать:

– сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

– сведения, составляющие тайну следствия и судопроизводства;

– сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.);

– сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);

– сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

– служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации

– и федеральными законами (служебная тайна);

– сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации «Перечнем сведений, составляющих служебную информацию ограниченного распространения».

3.4. Указанный перечень может включать следующие классы сведений ограниченного распространения:

– сведения экономического характера;

– сведения по финансовым вопросам;

– сведения по науке и технике;

– сведения по транспорту и связи;

– сведения по вопросам внешней торговли и международных научно-технических связей;

– сведения, связанные с обеспечением безопасности органов государственной власти субъекта Российской Федерации и органов местного самоуправления.

4. Порядок защиты информации в информационных системах персональных данных МБОУ «СОШ № 103»

4.1. Обработка информации в информационных системах персональных данных (далее – ИСПДн) осуществляется с учетом требований Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.2. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

– регистрация событий безопасности;

– антивирусная защита;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности персональных данных;

– обеспечение целостности информационной системы и персональных данных;

– обеспечение доступности персональных данных;

– защита среды виртуализации;

– защита технических средств;

– защита информационной системы, ее средств, систем связи и передачи данных;

– выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее – инциденты), и реагирование на них;

– управление конфигурацией информационной системы и системы защиты персональных данных.

4.3. Для пользователей ИСПДн, работающих в МБОУ «СОШ № 103», обязательным является выполнение положений, инструкций и регламентов, утвержденных в приложениях к настоящему Порядку, а также отдельных положений, инструкций и регламентов, утвержденных директором МБОУ «СОШ № 103», если они регулируют вопросы обеспечения безопасности ПДн. Обязанность по ознакомлению сотрудников с настоящими регламентами лежит на ответственном за обеспечение безопасности обработки персональных данных.

5. Порядок отнесения сведений к категории конфиденциальных

5.1. Отнесение сведений к категории конфиденциальных осуществляется путем введения ограничений на разглашение и доступ к их носителям в следующем порядке:

5.1.1 «Перечень сведений» создается на основе перечней, составленных руководителями подразделений МБОУ «СОШ № 103». «Перечень сведений» (дополнения и изменения к нему) утверждается директором МБОУ «СОШ № 103».

5.1.2 Если сведения не предусмотрены указанным «Перечнем сведений», но, по мнению исполнителя, их разглашение может быть использовано в ущерб интересам МБОУ «СОШ № 103», он представляет директору МБОУ «СОШ № 103» аргументированные предложения о необходимости защиты этих сведений и внесении соответствующих дополнений в «Перечень сведений». До принятия окончательного решения защита данных сведений должна быть обеспечена в соответствии с требованиями настоящего Порядка.

5.1.3 Постановка грифа «Конфиденциально» на документе производится исполнителем на основании «Перечня сведений». Срок действия ограничений,

связанных с необходимостью защиты КИ определяется директором МБОУ «СОШ № 103».

5.2. Конфиденциальные сведения утрачивают необходимость защиты:

– по окончании установленного «Перечнем сведений» срока;

– по соглашению заинтересованных сторон, установивших эти ограничения;

– в иных случаях, определяемых лицом, подписавшим (утвердившим) документ, содержащий эти сведения.

5.3. Исполнителям документов с грифом «Конфиденциально» предоставляется право по истечении срока действия грифа снимать документы с особого учета. При этом зачеркивается гриф «Конфиденциально», что заверяется подписями исполнителя и работника, ответственного за учёт, с отражением в «Журнале регистрации конфиденциальных носителей» (далее – Журнал учета).

5.4. Решение о снятии грифа до истечения срока его действия принимает директор МБОУ «СОШ № 103», что заверяется подписью на документе с указанием даты.

5.5. Аннулирование грифа «Конфиденциально» отражается в «Журнале учета».

6. Порядок допуска к конфиденциальной информации

6.1. Все сотрудники, принимаемые на работу в МБОУ «СОШ № 103», должны:

– ознакомиться с настоящим Порядком, а также иными документами МБОУ «СОШ № 103», регламентирующими вопросы обеспечения ИБ;

– подписать индивидуальное письменное обязательство о неразглашении КИ в двух экземплярах по форме, утвержденной в МБОУ «СОШ № 103» (один экземпляр передается сотруднику, второй экземпляр хранится в личном деле сотрудника не менее 3-х лет после его увольнения).

6.2. Сотрудники МБОУ «СОШ № 103» не допускаются к работе с КИ до выполнения требований, указанных в пункте 8.1 настоящего Порядка.

6.3. Директор МБОУ «СОШ № 103» и его заместители имеют доступ к КИ, определенной в «Перечне сведений», в полном объеме.

6.4. Доступ сотрудников МБОУ «СОШ № 103» к КИ, определенной в «Перечне сведений», осуществляется в пределах, необходимых для исполнения должностных обязанностей.

6.5. Доступ сотрудников МБОУ «СОШ № 103» к КИ в ЛВС соответствует их должностным обязанностям и осуществляется в порядке, установленном в МБОУ «СОШ № 103».

7. Обязанности сотрудников МБОУ " СОШ № 103"

7.1. Руководство технической защитой конфиденциальной информации возлагается на АИБа.

7.2. Заместитель директора по УВР и системный администратор МБОУ «СОШ № 103» организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях учреждения.

7.3. Сотрудник, назначенный ответственным по технической защите конфиденциальной информации, осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в МБОУ «СОШ № 103».

7.4. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

7.5. Заместители директора, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную информацию, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения сотрудников МБОУ «СОШ № 103» (через ответственного сотрудника).

7.6. АИБ имеет право привлекать к проведению работ по технической защите КИ в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7.7. Сотрудники МБОУ «СОШ № 103» обязаны:

– знать и соблюдать требования настоящего Порядка;

– знать и неукоснительно выполнять все требования других нормативных документов, регламентирующих вопросы обеспечения ИБ в МБОУ «СОШ № 103»;

– соблюдать порядок работы с КИ, установленный в МБОУ «СОШ № 103»;

– принимать меры по защите КИ, соблюдать правила работы со средствами защиты информации и режим разграничения доступа к файлам с КИ при её обработке;

– не разглашать и не передавать третьим лицам КИ без письменного согласия лица, предоставившего эту информацию.

8. Ответственность сотрудников МБОУ «СОШ № 103» за разглашение конфиденциальной информации

8.1. Под разглашением КИ в настоящем Положении понимается действие или бездействие, в результате которых КИ в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без письменного согласия лица, предоставившего эту информацию.

8.2. Разглашение КИ влечет за собой дисциплинарную, гражданско-правовую или уголовную ответственность в отношении лица, нарушившего режим КИ.

8.3. За умышленное или неосторожное разглашение КИ, а также нарушение порядка обращения с КИ сотрудник МБОУ «СОШ № 103» может быть привлечен к дисциплинарной ответственности в соответствии с законодательством РФ (вплоть до увольнения).

8.4. За умышленное или неосторожное разглашение КИ, а также нарушение порядка обращения с КИ сотрудник МБОУ «СОШ № 103» может быть привлечен к административной, гражданско–правовой или уголовной ответственности в соответствии с законодательством РФ

8.5. По факту нарушения положений настоящего Порядка проводится служебное разбирательство, по результатам которого принимается соответствующее решение.

9. Требования к порядку учета, хранения и обращения конфиденциальных документов в МБОУ «СОШ № 103»

9.1. Директор МБОУ «СОШ № 103» устанавливает и утверждает порядок учета, хранения и обращения с конфиденциальными документами и их носителями. Данный порядок должен соответствовать требованиям настоящего Порядка.

9.2. В МБОУ «СОШ № 103» учет документов и магнитных носителей с КИ должен осуществляться лицами (далее - делопроизводителями), которым поручен прием и учет несекретной документации.

9.3. На документах, содержащих сведения ограниченного распространения, в правом верхнем углу первой страницы документа необходимо проставлять гриф «Конфиденциально» и номер экземпляра. Использовать другие ограничительные пометки или грифы («Для служебного пользования», «Банковская тайна» и т.п.) запрещено.

9.4. Отнесение конкретных документов к КИ должно производиться исполнителем (разработчиком) и/или лицом, подписывающим (утверждающим) документ на основании «Перечня сведений».

9.5. Документы с грифом «Конфиденциально» должны:

– должны учитываться отдельно от несекретной информации;

– быть с указанием количества экземпляров, фамилии исполнителя, номера его телефона и даты печати на последнем листе (на оборотной стороне). Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для делопроизводства. Черновики и варианты уничтожаются секретарем с отражением факта уничтожения в учетных формах. Недописанные по каким-либо причинам проекты документов уничтожаются лично исполнителем;

– передаваться сотрудникам подразделений под расписку после регистрации;

– пересылаться сторонним организациям заказными почтовыми отправлениями, а при наличии соответствующего договора через органы фельдсвязи или спецсвязи;

– тиражироваться с разрешения начальника подразделения. Разрешение оформляется на последнем листе (на оборотной стороне) тиражируемого документа. Учет тиражируемых документов осуществляется поэкземплярно;

– храниться в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

9.6. Входящая корреспонденция, адресованная МБОУ «СОШ № 103» и содержащая КИ должна иметь гриф «Конфиденциально».

Документы, прилагаемые к сопроводительному письму с грифом «Конфиденциально», считаются конфиденциальными.

Входящие конфиденциальные документы передаются получателю под расписку.

9.7. При необходимости направления документов с пометкой «Конфиденциально» в несколько адресов должен быть составлен указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем подразделения, готовившего документ.

9.8. Требования настоящего Порядка распространяются и на съемные машинные носители информации, содержащие КИ. Используемые для записи защищаемой информации носители должны быть учтены. На магнитном носителе должны быть проставлены регистрационный номер, гриф «Конфиденциально», дата и роспись работника, отвечающего за учет носителей.

9.9. Уничтожение дел, документов, машинных носителей с грифом «Конфиденциально», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

9.10. Передача документов и дел с грифом «Конфиденциально» от одного работника другому осуществляется с разрешения руководителя подразделения, с отметкой в соответствующих журналах учета.

9.11. При смене работника, ответственного за учет документов с грифом «Конфиденциально», составляется акт приема-сдачи этих.

10. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее

10.1. Доступ к КИ, нарушение ее целостности и доступности возможно реализовать за счет:

– НСД к КИ при ее обработке в информационных системах и ресурсах;

– утечки КИ по техническим каналам.

10.2. Детальное описание возможных ТКУИ, НСД к информации и специальных воздействий на нее содержится в Моделях угроз безопасности информационных систем МБОУ «СОШ № 103».

11. Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

11.1. Для добывания конфиденциальных сведений могут использоваться:

– портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки ПЭМИН;

– автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

– компьютерная разведка, использующая различные способы и средства НСД к информации и специальных воздействий на нее.

11.2. Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь – глобальным сетям.

11.3. Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи здания МБОУ «СОШ № 103».

11.4. Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

11.5. Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

11.6. НСД к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных АРМ, в ЛВС, в распределенных телекоммуникационных системах.

11.7. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

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

– случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

– некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

– просмотра информации с экранов дисплеев и других средств ее отображения.

11.8. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России. Наиболее опасной является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям администрации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

11.9. Оценка возможности НСД к информации в СВТ и АС осуществляется с использованием следующих руководящих документов ФСТЭК России:

– Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992).

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992).

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден

решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992).

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к КИ и режимов обработки данных в АС.

12. Организационные и технические мероприятия по технической защите конфиденциальной информации

12.1. Разработка мер, и обеспечение защиты КИ осуществляются специалистами, назначаемыми директором МБОУ «СОШ № 103» для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

12.2. Для защиты КИ должны использоваться сертифицированные по требованиям безопасности технические средства защиты.

12.3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

12.4. Ответственность за обеспечение требований по технической защите КИ возлагается на АИБа.

12.5. Техническая защита информации в ЗП.

Работы по технической защите КИ в ЗП должны включать следующие мероприятия:

12.5.1 Определение перечня ЗП по результатам анализа циркулирующей в них КИ и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

12.5.2 Назначение сотрудников, ответственных за выполнение требований по технической защите КИ в ЗП (далее – сотрудники, ответственные за безопасность информации).

12.5.3 Разработка частных инструкций по обеспечению безопасности информации в ЗП.

12.5.4 Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

12.5.5 Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите КИ.

12.5.6 Проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП.

12.5.7 Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

12.5.8 Оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных телефонов достаточно одного устройства на линию, выходящую за пределы ЗП.

12.5.9 Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

12.5.10 Обеспечение требуемого уровня звукоизоляции входных дверей ЗП.

12.5.11 Обеспечение требуемого уровня звукоизоляции окон ЗП.

12.5.12 Демонтирование или заземление (с обеих сторон) лишних (незадействованных) в ЗП проводников и кабелей.

12.5.13 Отключение при проведении совещаний в ЗП всех неиспользуемых электро-и радиоприборов от сетей питания и трансляции.

12.5.14 Выполнение перед проведением совещаний следующих условий: окна должны быть плотно закрыты и зашторены; двери плотно прикрыты.

12.6. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

12.6.1 При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

12.6.2 При невозможности обеспечения КЗ заданных размеров необходимо применение СПЗ в районе размещения защищаемого ОТСС, применение СЛЗ линий электропитания, радиотрансляции, заземления, связи.

12.6.3 Техническая защита информации в СВТ и АС от НСД в соответствии с требованиями руководящих документов ФСТЭК России должна обеспечиваться путем:

– проведения классификации СВТ и АС;

– выполнения необходимых организационных мер защиты;

– установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД;

– защита каналов связи, предназначенных для передачи КИ;

– защиты информации от воздействия программ-закладок и компьютерных вирусов.

12.7. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами ФСТЭК России.

12.7.1 Организация антивирусной защиты информации на объектах информатизации достигается путём:

– установки и применения средств антивирусной защиты информации;

– обновления баз данных средств антивирусной защиты информации;

– действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

12.7.2 Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

13. Планирование работ по технической защите конфиденциальной информации и контролю

13.1. В МБОУ «СОШ № 103» должны составляться годовые планы работ по технической защите КИ и контролю. Проекты планов ответственным по технической защите КИ сотрудником совместно с другими подразделениями МБОУ «СОШ № 103», выполняющими работы с защищаемой информацией, рассматриваются постоянно действующей технической комиссией и утверждаются директором МБОУ «СОШ № 103».

13.2. В годовые планы по технической защите КИ и контролю должны включаться:

– мероприятия по выполнению требований законодательства по вопросам защиты КИ;

– подготовка проектов распорядительных документов по вопросам организации технической защиты информации в МБОУ «СОШ № 103», инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на АРМ, в ЗП;

– аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите КИ;

– проведение периодического контроля состояния технической защиты информации;

– мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

– мероприятия по совершенствованию технической защиты информации на объектах МБОУ «СОШ № 103».

13.3. Контроль выполнения планов и отчетность по ним возлагается на ответственного по технической защите КИ сотрудника.

14. Аттестация рабочих мест

14.1. Аттестации на соответствие требованиям по технической защите КИ в реальных условиях эксплуатации подлежат системы и средства информатизации и связи, предназначенные для обработки и передачи КИ, а также помещения, предназначенные для ведения конфиденциальных переговоров. Указанная аттестация проводится в соответствии с «Положением по аттестации объектов информатизации по требованиям безопасности информации», утвержденным Председателем Гостехкомиссии России 25.11.1994. Аттестация систем правительственной и иной закрытой шифрованием связи проводится в соответствии с нормативными документами ФАПСИ.

14.2. По результатам аттестации выдается «Аттестат соответствия», получение которого дает право использования аттестованных систем и средств для обработки и передачи информации, составляющей конфиденциальную информацию, и ведения конфиденциальных переговоров в аттестованных помещениях.

14.3. Переаттестация систем и средств информатизации, связи и помещений проводится по истечении срока действия «Аттестата соответствия», при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации.

15. Взаимодействие с предприятиями, учреждениями и организациями

15.1. При проведении совместных работ МБОУ «СОШ № 103» с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита информации, составляющей конфиденциальную информацию, независимо от места проведения работ.

15.2. В технических заданиях на выполнение совместных работ с использованием КИ, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с ответственным по технической защите КИ сотрудником и взаимодействующих предприятий (учреждений, организаций).

15.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации – на исполнителей работ (пользователей) при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

16. Заключительные положения

16.1. Проверка наличия документов, магнитных носителей информации и дел с грифом «Конфиденциально» проводится один раз в год комиссией, назначаемой директором МБОУ «СОШ № 103», проверки оформляются актом.

16.2. Доступ правоохранительных органов РФ к КИ МБОУ «СОШ № 103», определенной в «Перечне сведений», осуществляется в соответствии с действующим законодательством РФ.

16.3. Раскрытие юридическим или физическим лицам сведений конфиденциального характера МБОУ «СОШ № 103» возможно в случае привлечения их к совместной хозяйственной, финансовой и иной деятельности, требующей передачи конфиденциальных сведений, и только в том объеме, который необходим для реализации целей и задач МБОУ «СОШ № 103», а также при условии принятия ими на себя обязательств по неразглашению и исключению неправомерного использования полученных сведений.

16.4. Право принятия решения на передачу (предоставление) конфиденциальных сведений третьим лицам предоставлено только МБОУ «СОШ № 103».

16.5. Конфиденциальные сведения других юридических или физических лиц, переданные МБОУ «СОШ № 103» для выполнения работ или

осуществления иной совместной деятельности, и в отношении которых МБОУ «СОШ № 103» взяло на себя обязательство о неразглашении и исключении неправомерного их использования, подлежат защите наравне с другими сведениями конфиденциального характера МБОУ «СОШ № 103».

16.6. Контроль состояния технической защиты конфиденциальной информации осуществляется:

– ФСТЭК России (силами Центрального аппарата и Управления по соответствующему федеральному округу);

– Управлением Федеральной службы безопасности;

– внутренней комиссией МБОУ «СОШ № 103» – не реже 1 раза в год;

– структурным подразделением ответственным по технической защите конфиденциальной информации сотрудником и пользователем – непрерывно.

16.7. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, МБОУ «СОШ № 103», наличия соответствующих документов по технической защите КИ, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.