

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЧУРИЛКОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА»

391105, Рыбновский район, д. Чурилково, т. (49137) 35-2-47, факс: (49137) 35-2-47,
mail: churilkovo.school@yandex.ru, ОГРН: 1026200700613, ИНН/КПП: 6213006061/621301001

e-

Утверждено
Приказом директора школы
от 10.09.2013г. № 19-8

ПОЛОЖЕНИЕ
о информационной безопасности учебного процесса
МБОУ «Чурилковская СОШ»

д. Чурилково 2013г.

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в МБОУ «Чурилковская СОШ»

1.2. Мероприятия по защите конфиденциальной информации, проводимые в ОУ, являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы, являющиеся собственностью государства, находятся в ведении образовательных учреждений и организаций в соответствии с их компетенцией, подлежат обязательному учету и защите.

1.4. Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.5. Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.6. Объектами защиты в образовательных учреждениях являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);

- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее вспомогательные технические средства и системы (ВТСС);

- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (ЗП).

1.7. Ответственность за выполнение требований настоящего Положения возлагается на руководителя образовательного учреждения, руководителей (начальников) подразделений (департаментов, управлений, отделов), на начальника структурного подразделения защиты конфиденциальной информации, а также на специалистов допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

1.8. Непосредственное руководство работами по защите конфиденциальной информации осуществляет первый заместитель образовательного учреждения.

2. Охраняемые сведения

2.1. В образовательных учреждениях разрабатывается Перечень сведений конфиденциального характера. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера в соответствии с Указом Президента РФ от 6 марта 1997 года № 188.

Перечень сведений конфиденциального характера включает:

- 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 РФ 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 РФ 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 РФ и федеральными законами (служебная тайна).

Сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации "Перечнем сведений, составляющих служебную информацию ограниченного распространения".

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 РФ и органов местного самоуправления.

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

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

- несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;
- утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации образовательного учреждения.

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

4.1. Для добывания конфиденциальных сведений могут использоваться:

портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);

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

компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

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

Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий образовательных учреждений.

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

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

4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

4.3. 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.

4.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

Наиболее опасной для образовательных учреждений 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.

4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.

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 конфиденциальной информации и режимов обработки данных в автоматизированных системах.

5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются подразделением по защите конфиденциальной информации (службой безопасности) или отдельными специалистами, назначаемыми руководителем образовательного учреждения 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.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

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

5.4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на руководителя образовательного учреждения, эксплуатирующего объекты информатизации.

5.5. Техническая защита информации в защищаемых помещениях.

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

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

5.5.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации.

5.5.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

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

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

5.5.6. 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.

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

5.5.8. 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.

5.5.9. 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.

5.5.10. Обеспечение требуемого уровня звукоизоляции входных дверей ЗП.

5.5.11. Обеспечение требуемого уровня звукоизоляции окон ЗП.

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

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

5.5.14. Выполнение перед проведением совещаний следующих условий:

окна должны быть плотно закрыты и зашторены;

двери плотно прикрыты;

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

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

5.6.2. При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется проведение следующих мероприятий:

Применение систем электромагнитного пространственного зашумления (СПЗ) в районе размещения защищаемого ОТСС.

Применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.

5.6.3. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов Гостехкомиссии 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 конфиденциальной информации.

защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.7. 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 Гостехкомиссии России.

Организации 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.

5.7.1. Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над

эффективностью предусмотренных мер защиты информации на руководителя подразделения по защите конфиденциальной информации (ответственного) ОУ.

5.7.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

5.7.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

5.7.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

Входной антивирусный контроль всей информации поступающей с электронной почтой;

Входной антивирусный контроль всей поступающей информации из сети Internet;

Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а так же передача информации посредством электронной почты;

Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

Обязательная антивирусная проверка используемых в работе внешних носителей информации;

Постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

Внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

Восстановление работоспособности программных и аппаратных средств, а также непосредственно информации в случае их повреждения компьютерными вирусами.

5.7.5. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

5.7.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение по защите конфиденциальной информации или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность подразделение информационно-технической службы органа власти по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения информационно-технической службы органа власти по защите конфиденциальной информации.

5.7.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

5.7.8. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.7.9. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора образовательного учреждения.

5.8.1. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8.2. Формирование личных паролей пользователей осуществляется централизованно. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

5.8.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

5.8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4 настоящей Инструкции.

5.8.6 Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

5.8.7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения, периодический контроль – на специалиста по защите информации или ответственного сотрудника.

6. Обязанности и права должностных лиц

6.1. Руководство технической защитой конфиденциальной информации в образовательном учреждении возлагается на заместителя ОУ.

6.2. Руководители образовательных учреждений организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях подчиненных им подразделений.

6.3. Начальник структурного подразделения по технической защите конфиденциальной информации (ответственный сотрудник) осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в образовательном учреждении.

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

6.5. Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения

утечки (или предпосылок к утечке) этих сведений. Предложения докладываются заместителю образовательного учреждения (через структурное подразделение по технической защите конфиденциальной информации или ответственного сотрудника).

6.6. Заместитель образовательного учреждения имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7. Планирование работ по технической защите конфиденциальной информации и контролю.

7.1. В образовательном учреждении составляются годовые планы работ по технической защите конфиденциальной информации и контролю. Проекты планов разрабатываются структурным подразделением по технической защите конфиденциальной информации или ответственным сотрудником совместно с подразделениями образовательного учреждения, выполняющими работы с защищаемой информацией, рассматриваются постоянно действующей технической комиссией и утверждаются руководителем образовательного учреждения. Сроки разработки, представления и утверждения планов устанавливаются руководителем образовательного учреждения.

7.2. В годовые планы по технической защите конфиденциальной информации и контролю включаются:

мероприятия по выполнению постановлений и распоряжений Мэра Москвы, Правительства Москвы, руководителя образовательного учреждения по вопросам защиты конфиденциальной информации;

подготовка проектов распорядительных документов по вопросам организации технической защиты информации в образовательном учреждении, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах, 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 конфиденциальной информации;

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 образовательного учреждения.

7.3. Контроль выполнения планов и отчетность по ним возлагается на структурное подразделение по технической защите конфиденциальной информации или ответственного сотрудника.

8. Контроль состояния технической защиты конфиденциальной информации.

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня образовательного учреждения и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется:

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

Управлением Федеральной службы безопасности;

Внутренней комиссией образовательного учреждения – не реже 1 раза в год;

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

8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, постановлений и распоряжений Мэра Москвы, Правительства Москвы, руководителя образовательного учреждения, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

9. Аттестация рабочих мест

9.1. Аттестации на соответствие требованиям по технической защите конфиденциальной информации в реальных условиях эксплуатации подлежат системы и средства информатизации и связи, предназначенные для обработки и

передачи конфиденциальной информации, 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 ноября 1994 г. Аттестация систем правительственной и иной закрытой шифрованием связи проводится в соответствии с нормативными документами ФАПСИ.

9.2. По результатам аттестации выдается "Аттестат соответствия", получение которого дает право использования аттестованных систем и средств для обработки и передачи информации, составляющей конфиденциальную или служебную тайну, и ведения конфиденциальных переговоров в аттестованных помещениях.

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.

10. Взаимодействие с предприятиями, учреждениями и организациями

10.1. При проведении совместных работ образовательного учреждения с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита информации, составляющей конфиденциальную или служебную тайну, независимо от места проведения работ.

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

10.3. 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.