



УТВЕРЖДАЮ

Директор ГБОУ СПО МО

ПТ имени С.П. Королева

И.А. Ласкина

« 24 » января 2014 г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ГБОУ СПО МО «ПРОФЕССИОНАЛЬНЫЙ ТЕХНИКУМ ИМЕНИ С.П. КОРОЛЕВА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании требований:

- Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных»;
- Федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об обеспечении безопасности персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Московской области от 27.11.2002 № 573/46 «Об утверждении положения о порядке обращения с информацией ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждений Московской области».

1.2. Под информацией ограниченного доступа понимаются сведения, доступ к которым ограничен нормативно-правовыми актами, в частности Указом Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», и отраженные в «Сводном перечне сведений конфиденциального характера», утвержденном постановлением Правительства Московской области от 27.11. 2002 № 573/46.

1.3. Персональные данные (далее - ПДн) относятся к информации ограниченного доступа (далее - информация), так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 "О персональных данных".

1.4. Цель данного Положения – определение порядка организации, и проведения работ в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» для построения эффективной системы защиты информации (далее - СЗИ) от несанкционированного доступа, и её последующей эксплуатации. В частности, с целью обеспечения защиты прав и свобод субъектов персональных данных при обработке их ПДн в информационных системах ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

1.5. Информационная система (далее - ИС) – совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

1.6. Информационная система персональных данных (далее - ИСПДн) - информационная система, представляющая собой совокупность содержащихся в базе данных ПДн, и обеспечивающих их обработку информационных технологий и технических средств.

1.7. ИСПДн является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, относящиеся к специальным категориям ПДн, биометрические и общедоступные ПДн.

1.8. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.

1.9. Требования настоящего Положения являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

1.10. За общее состояние защиты информации в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» отвечает его руководитель.

Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» возлагается на руководителей этих подразделений.

Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с инструкцией «По работе пользователей информационной системы», утвержденной руководителем ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

Проведения работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на администраторов ИС.

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту информации в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» (далее – ответственный).

1.11. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

1.12. При необходимости для оказания услуг в области аттестации ИС можно привлекать специализированные организации, имеющие лицензию на этот вид деятельности.

1.13. Положение может уточняться и корректироваться по мере необходимости.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И АКТУАЛЬНЫЕ УГРОЗЫ

2.1. Охраняемые сведения - информация, обрабатываемая в ИС структурных подразделениях ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» в соответствии с «Перечнем процессов и сведений ограниченного доступа, обрабатываемых в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты:

- ИС различного назначения, участвующие в обработке информации, в соответствии с «Перечнем информационных систем ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;
- помещения, где установлены ИС или хранится информация на бумажных носителях.

2.3. Актуальные угрозы безопасности объектов защиты.

В соответствии с моделями угроз безопасности персональных данных в ИСПДн, разработанными и утверждёнными в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», актуальными являются только угрозы несанкционированного доступа к информационным ресурсам ИС с целью получения, разрушения, искажения и блокирования информации. Данный вид угроз в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» относится к угрозам 3-го типа.

Применение средств технической разведки для перехвата информации, циркулирующей в ИС ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» маловероятно с учётом её характера.

Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности реализуются без применения сложных технических средств:

- обрабатываемой в ИС от НСД нарушителей и непреднамеренных действий сотрудников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;

- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в ЛВС при несанкционированном подключении к данной сети.

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Замыслом достижения целей защиты ИС от НСД является обеспечение защиты информации путем выполнения требований нормативных правовых актов, принятыми ФСТЭК России в исполнении части 4 статьи 19 Федерального закона Российской Федерации «О персональных данных» для четвертого уровня защищённости ПДн.

3.2. Целью технической защиты информации в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» является предотвращение НСД к информации при её обработке в ИС, связанные с действиями нарушителей, включая пользователей ИС, реализующих угрозы непосредственно в ИС, а также нарушителей, не имеющих доступ к ИС, реализующих угрозы из сетей международного информационного обмена с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

3.3. Целями организационных мероприятий по защите информации в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» являются:

- исключение непреднамеренных действий сотрудников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации ИС;
- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием ИС (физический вынос информации на электронном или бумажном носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями.

3.4. Руководитель ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п.1.1. настоящего Положения.

К таким мерам могут, в частности, относиться:

- назначение ответственного за организацию защиты информации;
- издание комплекта документов, определяющих политику в отношении обработки ПДн в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации
- выбор в качестве основного средства защиты ИСПДн, не подключённых к сети Интернет, операционных систем «Windows XP / 7 Professional» (далее - ОС), обладающих встроенными средствами защиты от НСД;

- настройка ОС на компьютерах ИС в соответствии с «Руководством по безопасной настройке»;
- сертификация вышеуказанных ОС по требованиям безопасности информации;
- выбор дополнительных технических средств, сертифицированных по требованиям безопасности информации, для компьютеров, подключенных к сетям связи общего пользования ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» и (или) Интернет;
- использование средств антивирусной защиты;
- предотвращение организационными мерами НСД к обрабатываемой информации;
- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации;
- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах;
- строгое соблюдение сотрудниками ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» «Инструкции по работе пользователей информационной системы».

3.5. Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ об организации работ по защите информации ограниченного доступа;
- положение о порядке организации и проведения работ по защите информации ограниченного доступа в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;
- список лиц, допущенных в соответствии с их должностными обязанностями к информации;
- акты определения уровня защищенности ИСПДн;
- технические паспорта ИС;
- инструкции ответственного и по работе пользователей ИС;
- журнал учёта паролей пользователей для работы в ИС;
- журнал учёта машинных носителей информации;
- декларацию о соответствии требованиям безопасности или «Аттестат соответствия требованиям безопасности».

4. ВВОД В ЭКСПЛУАТАЦИЮ ИНФОРМАЦИОННЫХ СИСТЕМ

4.1. Необходимым условием для ввода в эксплуатацию информационных систем ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» является их соответствие требованиям Федерального закона «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и нормативно-методической документации ФСТЭК России по безопасности информации.

4.2. Руководитель ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» самостоятельно принимает решение по организации работ по построению систем защиты ИС или с привлечением сторонней организации, имеющей лицензию ФСТЭК России на проведения таких работ, или силами самого образовательного учреждения.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИС в соответствии с программой испытаний, согласованной с ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева». Испытания завершаются выдачей «Аттестата соответствия ИС требованиям безопасности информации».

4.4. В случае проведения работ по построению системы защиты ИС силами самого образовательного учреждения оценка полученного результата проводится в форме декларирования.

4.5. Для декларирования соответствия ИС требованиям п. 3.1 комиссией, утвержденной приказом руководителя ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», подготавливаются и представляются на систему:

- акт определения уровня защищенности ИСПДн
- технический паспорт;
- организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам;
- модель угроз безопасности персональных данных;
- сертификаты средств защиты информации, используемые при построении системы защиты;
- инструкция по работе пользователей;
- инструкция ответственного за защиту информации.

4.6. При использовании для защиты ИС от НСД встроенных средств защиты операционных систем «Windows XP Pro» / Windows 7 Pro их настройка проводится силами самого образовательного учреждения.

4.7. Контроль эффективности СЗИ осуществляется представителями отдела мобилизационной подготовки и защиты информации Министерства образования Московской области с оформлением акта на выполнение требований ИС по защите информации.

4.8. В случае положительных результатов испытаний СЗИ руководитель ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия ответственным разрабатываются и доводятся до сотрудников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» под роспись «Инструкция по работе пользователей ИСПДн» и рекомендации о порядке выполнения мероприятий по защите информации.

5. ОСОБЕННОСТИ ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Правовое основание обработки ПДн ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»:

Федеральные законы Российской Федерации:

- «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
- Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ);
- Налоговый кодекс Российской Федерации (Федеральный закон от 05.08.2000 № 117-ФЗ),
- «О бухгалтерском учёте» от 06.12.2011 № 402-ФЗ;
- «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования» от 24.07.2009 N 212-ФЗ.

5.2. Цель обработки ПДн:

- обработка персональных данных сотрудников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» и сведений об их профессиональной служебной деятельности;
- обработка персональных данных учащихся;
- начисление денежного содержания сотрудникам ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;
- начисление стипендий студентам.

5.3. Перечень ПДн:

- паспортные данные;
- дата и место рождения;
- биографические сведения;
- сведения об образовании;
- сведения о семейном положении;
- сведения о месте регистрации, проживании;
- сведения о состоянии здоровья сведения о наличии/отсутствии судимости;

- иное (телефоны, ИНН, доходы, льготы).

5.4. Категории субъектов ПДн, персональные данные которых обрабатываются:

- сотрудники ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;
- студенты.

5.5. Все ПДн субъекта ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» следует получать у него самого. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах

получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение.

5.6. ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

5.7. Субъект ПДн самостоятельно принимает решение о предоставлении своих ПДн и дает согласие на их обработку.

Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федеральным законом от 27.07.2006 № 152 «О персональных данных».

5.8. Согласие на обработку ПДн оформляется в письменном виде.

Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва.

5.9. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя руководителя ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

5.10. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту тайны.

5.11. Субъект ПДн имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

5.12. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.13. Сведения о ПДн должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

5.14. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при получении письменного запроса субъекта ПДн или его законного представителя. Письменный запрос должен быть адресован на имя руководителя ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» или уполномоченного руководителем лицо.

5.15. Субъект в праве обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Москве и Московской области) или в судебном порядке неправомерные действия или бездействия должностных лиц ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» при обработке и защите его ПДн.

6. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

6.1. Директор организует работу по построению системы защиты ИС.

В частности,

1. Назначает ответственного за организацию защиты информации из числа сотрудников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

2. Утверждает комплект документов, определяющих политику в отношении обработки ПДн в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации.

3. Утверждает меры и состав средств СЗИ, предложенных для обеспечения безопасности ПДн при их обработке в ИСПДн. При этом оценивает соотношение вреда, который может быть причинен субъектам ПДн и принимаемых мер по защите ИСПДн.

6.2. Заместитель директора по безопасности:

- составляет Перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;

- составляет Список лиц, допущенных в соответствии с их должностными обязанностями к информации ограниченного доступа.

- контролирует работу ответственного по организации и проведению работ по защите информации в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;

- предотвращает организационными мерами НСД к обрабатываемой в ИС информации;

- контролирует порядок подготовки, учета и хранения документов конфиденциального характера;

- контролирует порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации.

6.3. Ответственный:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации при её обработке с помощью ИС;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- знакомит работников ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева», непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, организывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;
- проводит систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- проводит инструктаж пользователей ИС;
- контролирует выполнение администраторами ИС обязанностей по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)
- контролирует порядок учёта и хранения машинных носителей конфиденциальной информации;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИС;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших доступ к ИС;
- требует от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает руководителю ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева»;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

6.4. Заведующий отделением, начальник отдела кадров, сотрудник по учету контингента студентов:

- лично отвечают за защиту информации в структурных подразделениях, сохранность машинных и иных носителей информации;
- организуют выполнение мероприятий по защите информации при использовании технических средств;
- участвуют в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИС;
- участвуют в определении правил разграничения доступа к информации в ИС, используемых в ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

7. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

7.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний Роскомнадзора и ФСТЭК России;
- решений Московской областной комиссии по информационной безопасности.

7.2. Для подготовки и реализации организационных и технических мероприятий по защите информации ответственный составляет годовой план работ по защите информации.

7.3. Контроль выполнения годового плана возлагается на руководителя ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

8. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. С целью своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

8.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.

8.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева».

8.4. Периодический контроль за эффективностью СЗИ осуществляет ответственный и представители отдела мобилизационной подготовки и защиты информации Министерства образования Московской области на основании приказа Министерства образования Московской области от 14.04.2009 № 857.

8.5. Плановые и внеплановые проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться территориальными органами Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее - Роскомнадзор).

Допуск представителей этих органов для проведения контроля осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

8.6. Ответственный обязан присутствовать при всех проверках по вопросам защиты информации.

8.7. Результаты проверок отражаются в Актах проверок.

8.8. По результатам проверок контролирующими органами ответственный с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

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

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

8.10. При обнаружении нарушений руководитель ГБОУ СПО МО «Профессиональный техникум имени С.П. Королева» принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.