ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА В ГБПОУ МО «Электростальский колледж»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании требований:

- Федеральных законов Российской Федерации:
  - от 27.07.2006 г. № 152 «О персональных данных»,
  - от 27.07.2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
  - от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»,
  - от 30.12. 2001 г. № 197-ФЗ Трудовой кодекс Российской Федерации;
- постановлений Правительства Российской Федерации:
  - от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
  - 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 г. № 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».

Под информацией ограниченного доступа (далее – информации) 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. Они устанавливают условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

1.2. Персональные данные (далее –ПДн) относятся к информации ограниченного доступа, так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 "О персональных данных". Именно ПДн сотрудников и обучающихся составляют значительную часть в общем объёме информации, обрабатываемой в образовательных организациях.

1.3. Цель данного Положения –определение порядка организации и проведения работ в ГБПОУМО «Электростальский колледж» (далее – ГБПОУ) для построения эффективной системы защиты информации (далее - СЗИ) от несанкционированного доступа, и её последующей эксплуатации. В частности, с целью обеспечение защиты прав и свобод субъектов персональных данных при обработке их ПДн в информационных системах ГБПОУ.

1.4. Под обработкой информации понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств.

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 распространяется на все процессы обработки информации в ГБПОУ, как с использованием средств автоматизации, так и без использования таких средств, и являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами ГБПОУ.

1.10. Настоящее Положение вступает в силу с момента его утверждения директором ГБПОУ и действует бессрочно, до замены его новым Положением.

1.11. За общее состояние защиты информации в ГБПОУ отвечает его руководитель.

Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях ГБПОУ 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 ГБПОУ.

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

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту информации в ГБПОУ (далее –ответственный).

1.12. Все работники, допущенные к обработке информации, обязаны соблюдать конфиденциальность информации в течение срока действия трудового договора. Для этих сотрудников необходимо предусмотреть в трудовом договоре соглашение о неразглашении информации.

1.13. 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.

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

1.15. Положение может уточняться и корректироваться по мере необходимости. Все изменения в Положение вносятся приказом.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И АКТУАЛЬНЫЕ УГРОЗЫ

2.1. Охраняемые сведения - информация, обрабатываемая в информационных системах структурных подразделениях ГБПОУ в соответствии с «Перечнем процессов и сведений

ограниченного доступа, обрабатываемых в ГБПОУ МО «Электростальский колледж» (далее – колледж), а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты:

- ИСПДн различного назначения, участвующие в обработке информации, в соответствии с «Перечнем информационных систем ГБПОУ МО «Электростальский колледж»;
- помещения, где установлены ИСПДн или хранится информация на бумажных носителях в соответствии с «Перечнем мест хранения бумажных носителей персональных данных в ГБПОУ МО «Электростальский колледж».

2.3. Актуальные угрозы безопасности объектов защиты.

В соответствии с моделями угроз безопасности персональных данных в ИСПДн, разработанными и утверждёнными в ГБПОУ МО «Электростальский колледж», актуальными являются только угрозы несанкционированного доступа к информационным ресурсам ИСПДн 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 ИСПДн ГБПОУ 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 ИСПДн от НСД нарушителей и непреднамеренных действий сотрудников ГБПОУ;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в локальных вычислительных сетях ГБПОУ при несанкционированном подключении к данной сети;
- при подключении ИСПДн к сетям Интернет.

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Замыслом достижения целей защиты ИСПДн 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 четвёртого уровня защищённости ПДн.

3.2. Целью технической защиты информации в ГБПОУ является предотвращение НСД к информации при её обработке в ИСПДн, связанные с действиями нарушителей. Включая пользователей информационных систем. Реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступ к ИСПДн, реализующих угрозы из сетей Интернет с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

3.3. Целями организационных мероприятий по защите информации в ГБПОУ являются:

- организация режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (установка замков, систем сигнализации и видеонаблюдения и т.п.);
- исключение непреднамеренных действий сотрудников ГБПОУ, 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 электронных или бумажных носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями;
- обеспечение безопасного хранения материальных носителей ПДн (закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.);
- использование средств гарантированного уничтожения материальных носителей ПДн (средства измельчения, сжигания, размагничивания и т.п.);
- использование систем пожарной сигнализации и пожаротушения.

3.4. Руководитель ГБПОУ 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 ГБПОУ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации
- выбор в качестве основного средства защиты ИСПДн, операционных систем «Windows XP/7/8/10Professional» (далее - ОС), обладающих встроенными средствами защиты от НСД;
- настройка ОС на компьютерах ИС в соответствии с «Руководством по безопасной настройке» (настройка других технических средств защиты от НСД);
- сертификация вышеуказанных ОС (технических средств) по требованиям безопасности информации;
- определение режима разграничения прав доступа пользователей к информационной системе. Разграничение доступа – это когда вход в систему осуществляется по индивидуальному паролю пользователя (будь то пароль ОС или специального программного обеспечения).
- выбор дополнительных технических средств, сертифицированных по требованиям безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз. В частности, для ИСПДн, подключенных к сетям связи общего пользования ГБПОУ 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 ГБПОУ «Инструкции по работе пользователей информационной системы».

3.5. Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ об организации работ по приведению процессов обработки и обеспечения безопасности информации ограниченного доступа в соответствие требованиям законодательства;
- положение о порядке организации и проведения работ по защите информации ограниченного доступа в ГБПОУ;
- перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ;
- список лиц, допущенных в соответствии с их должностными обязанностями к обработке информации;
- перечень ИСПДн;

- акты определения уровня защищенности ИСПДн;
- технические паспорта ИС;
- список пользователей ИСПДн;
- перечень мест хранения бумажных носителей ПДн;
- 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 ГБПОУ 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 Приказа ФСТЭК России от 18.02.2013 г. № 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. Руководитель ГБПОУ самостоятельно принимает решение по организации работ по построению систем защиты ИСПДн или с привлечением сторонней организации, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, или силами самой образовательной организации.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИСПДн в соответствии с техническим заданием ГБПОУ (ГОСТ 34.602-89) и программой и методикой испытаний (ГОСТ 19.301-79), согласованной с ГБПОУ. В соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Испытания завершаются выдачей «Аттестата соответствия информационной системы требованиям безопасности информации».

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

4.5. Для декларирования соответствия ИСПДн требованиям п. 3.1 комиссией, утвержденной приказом руководителя ГБПОУ, 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 ИСПДн от НСД технических средств защиты информации их настройка проводится силами самой образовательной организации.

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

информации по обеспечению безопасности ПДн субъектов ПДн при их обработке с использованием средств автоматизации.

4.8. В случае положительных результатов испытаний СЗИ руководитель ГБПОУ декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия ответственным разрабатываются и доводятся до сотрудников ГБПОУ под роспись «Инструкция по работе пользователей ИСПДн» и рекомендации о порядке выполнения мероприятий по защите информации.

5. ОСОБЕННОСТИ ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕДАННЫЕ

5.1. Правовое основание обработки ПДн ГБПОУ:

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 ГБПОУ и сведений об их профессиональной служебной деятельности в целях ведения кадрового учёта;
- обработка персональных данных обучающихся, необходимых для оказания им услуг в области образования;
- начисление денежного содержания сотрудникам ГБПОУ и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;
- начисление стипендий обучающимся.

5.3. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объем обрабатываемых ГБПОУ ПДн соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

5.4. При обработке ПДн ГБПОУ обеспечивается их точность, достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. ГБПОУ принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных, или неточных ПДн.

5.5. Хранение ПДн ГБПОУ осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок их хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах ГБПОУ.

5.6. Перечень ПДн:

- фамилия, имя, отчество (в т.ч. предыдущие),
- паспортные данные или данные документа, удостоверяющего личность,
- дата рождения, место рождения,
- гражданство,
- отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
- данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке,
- данные документов о подтверждении специальных знаний,
- данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях,
- знание иностранных языков,
- семейное положение и данные о составе и членах семьи,
- сведения о социальных льготах, пенсионном обеспечении и страховании,
- данные документов об инвалидности (при наличии),
- данные медицинского заключения (при необходимости),
- стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
- должность, квалификационный уровень,
- сведения о заработной плате (доходах), банковских счетах, картах,
- адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства,
- номер телефона (стационарный домашний, мобильный),
- данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории РФ (ИНН),
- данные страхового свидетельства государственного пенсионного страхования,
- данные страхового медицинского полиса обязательного страхования граждан.

5.7. Категории субъектов ПДн, персональные данные которых обрабатываются:

- сотрудники ГБПОУ
- обучающиеся.

5.8. Все ПДн субъекта ГБПОУ 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 ГБПОУ 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.

5.9. ГБПОУ 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 работника только с его письменного согласия.

5.10. 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.

5.11. 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.

5.12. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя руководителя.

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

5.14. 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.

5.15. 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.

5.16. 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.

5.17. 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 ГБПОУ или уполномоченного руководителем лицо. Копии документов, содержащих ПДн, выдаются ГБПОУ в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче. При выдаче документов для ознакомления, а также запрашиваемых копий и справок, работник, занимающийся обработкой ПДн, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

5.18. Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Центральному федеральному округу) или в судебном порядке неправомерные действия или бездействия должностных лиц ГБПОУ при обработке и защите его ПДн.

5.19. Доступ к ПДн должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей. Доступ работников ГБПОУ к ИСПДн ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты ПДн с использованием технических и организационных мероприятий.

5.20. Предоставление ПДн третьим сторонам осуществляется только с предварительного письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных

законодательством Российской Федерации, в частности Федеральными законами «Об обязательном пенсионном страховании в Российской Федерации, «Об основах обязательного социального страхования, «Об обязательном медицинском страховании в Российской Федерации».

Существенным условием договоров с третьими сторонами, в рамках, исполнения которых передаются ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

ГБПОУ с согласия субъекта может поручать обработку ПДн третьим сторонам, а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

В случае если ГБПОУ поручает обработку третьей стороне, в поручении на обработку ПДн должны быть в обязательном порядке определены:

- перечень действий (операций) с ПДн, которые будут совершаться третьей стороной;
- цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре с оператором, в согласии и т. д.);
- обязанность третьей стороны соблюдать конфиденциальность ПДн и обеспечивать безопасность при их обработке;
- требования к защите ПДн.

Федеральным законодательством может устанавливаться обязанность ГБПОУ непосредственно направлять информацию, содержащую ПДн, третьим лицам (отчетность, налоговые декларации и т.д.) либо право третьих лиц запрашивать указанную информацию в пределах их полномочий.

В последнем случае передача информации осуществляется на основании письменных мотивированных запросов, оформленных на официальных бланках за подписью уполномоченного должностного лица. Запрос должен содержать цели и правовые основания затребования информации, срок предоставления такой информации, если иное не установлено законом.

Ответы на запросы направляются законным получателям ПДн только в письменном виде и только в затребованном объеме.

Получателями ПДн на законном основании, в том числе являются:

- Фонд социального страхования РФ;
- Пенсионный фонд РФ;
- Федеральная налоговая служба;
- Федеральная инспекция труда;
- иные органы надзора и контроля за соблюдением законодательства о труде;
- правоохранительные и судебные органы.

6. ОБРАЩЕНИЕ С МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Виды носителей

Персональные данные в ГБПОУ хранятся на материальных носителях двух видов:

- машинные магнитные носители (далее – МНИ);
- бумажные носители.

Организация обработки поступивших и создаваемых документов, содержащих ПДн, осуществляется в соответствии с принятыми в ГБПОУ нормами документооборота.

6.2. Хранение бумажных носителей

Бумажные (документальные) носители ПДн должны храниться в условиях, исключающих несанкционированный доступ к ним посторонних лиц - в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Хранение бумажных (документальных) носителей ПДн вместе с документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным (документальным) носителям ПДн.

Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях.

Для каждой категории персональных данных должны быть определены и занесены в Перечень мест хранения бумажных носителей этой категории. В этом перечне указывают:

- категории субъектов ПДн;
- категории ПДн;
- место хранения (номер или наименование помещения, в котором хранятся бумажные носители, номер шкафа (сейфа) в котором хранятся бумажные носители).

ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечению установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

6.3. Использование и обеспечение сохранности машинных носителей информации

В целях предотвращения разрушения и утери обрабатываемой на компьютере информации пользователь ИСПДн должен осуществлять копирование необходимой информации по мере ее обновления на учтенные в установленном порядке МНИ (такие как: внешние жесткие диски, гибкие магнитные диски, USB флэш-накопители, карты флэш-памяти, оптические носители и др.). Эти носители должны быть учтены в Журнале учёта машинных носителей информации (далее – Журнал).

В Журнале указывают:

- номер машинного носителя;
- тип носителя;
- Ф.И.О. работника;
- дата получения и подпись работника;
- Ф.И.О. Администратора ИСПДн;
- дата возврата и подпись Администратора ИСПДн;
- отметка об уничтожении;

Кроме того, в этом Журнале необходимо учесть машинные носители информации с ЭЦП, а также те, которые используются для передачи ПДн третьей стороне.

Ответственность за ведение и хранение Журнала несёт ответственный, который в конце каждого года проверяет наличие МНИ у пользователей.

В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки МНИ такой носитель уничтожается или с него стираются ПДн (способом, исключающим возможность восстановление данных).

Вынос резервных копий баз данных ИСПДн, содержащих информацию персонального характера, из ГБПОУ запрещен. Передача и копирование их допустима только для прямого использования с целью технологической поддержки ИСПДн.

7. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

7.1. Директор организует работу по построению системы защиты ИС.

В частности,

- Назначает ответственного за организацию защиты информации из числа сотрудников ГБПОУ.
- 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.

- 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.

7.2. Заместитель директора по безопасности:

- составляет Перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ;
- контролирует наличие в трудовых договорах с сотрудниками из «Списка лиц, допущенных в соответствии с их должностными обязанностями к информации ограниченного доступа» соглашения о неразглашении информации;
- контролирует работу ответственного по организации и проведению работ по защите информации в ГБПОУ;
- 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.

7.3. Ответственный:

- разрабатывает и своевременно обновляет организационно-распорядительные документы по вопросам защиты информации;
- своевременно направляет в Управление Роскомнадзора по ЦФО уведомление о намерении Оператора осуществлять обработку персональных данных и сообщает о происшедших изменениях в процессе обработки персональных данных;
- организовывает работу по получению согласия субъектов персональных данных на обработку персональных данных в случаях, предусмотренных законодательством в данной сфере;
- знакомит работников ГБПОУ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает 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 администратором 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 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 допуск 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 ГБПОУ;
- вносит предложения руководителю ГБПОУ о внесении изменений в процессы обработки информации, а также в ИСПДн, если это обусловлено необходимостью обеспечения соответствия законодательству в сфере персональных данных;
- вносит предложения руководителю ГБПОУ о поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с обработкой информации;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

7.4. Администратор ИСПДн:

- обеспечивает настройку и бесперебойную эксплуатацию программных и технических средств обработки ПДн, входящих в состав ИС;
- обеспечивает настройку, бесперебойную эксплуатацию и мониторинг средств защиты информации;
- настраивает права доступа работников к ПДн и средствам их обработки в соответствии с ролевой моделью доступа;
- проводит инструктаж пользователей ИС по правилам эксплуатации программных и технических средств обработки ПДн, а также СЗИ, входящих в состав ИСПДн;
- меняет пароли пользователей ИС не реже одного раза в три месяца либо при компрометации паролей;
- хранит дистрибутивы программного обеспечения средств обработки информации ИС;
- обеспечивает контроль действий представителей сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации ИС;
- предоставляет необходимую информацию при проведении проверок регулирующими органами;
- оказывает содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по вопросам использования средств обработки информации ИС, в рамках своей компетенции;
- незамедлительно уведомляет в случае обнаружения попыток или фактов несанкционированного доступа к ПДн о выявленных фактах ответственного.

7.5. Руководители структурных подразделений:

- 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 ГБПОУ.

8. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

8.1. 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.

8.2. Для подготовки и реализации организационных и технических мероприятий по защите информации ответственный составляется годовой план работ по защите информации.

8.3. Контроль выполнения годового плана возлагается на руководителя ГБПОУ.

9. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

9.1. 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.

9.2. Контролю подлежат как принятые меры организации обработки информации, так и меры по обеспечению её безопасности.

9.3. Рекомендуется в рамках проведения контроля проверить:

- актуальность описания процессов обработки информации;
- актуальность перечня ИСПДн;
- актуальность перечня лиц, доступ которых к информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- актуальность сведений, указанных в Политике в отношении обработки персональных данных организацией, проверка соблюдения ее положений и общедоступности;
- наличие письменных согласий субъектов ПДн и соответствия форм согласий требованиям законодательства;
- проверка соответствия оценки вреда, который может быть причинен субъектам ПДн текущей ситуации;
- наличие договоров с организациями, которым поручается обработка ПДн, на предмет наличия предусмотренных законодательством положений
- соответствие организации в ГБПОУ обработки информации, осуществляемой без использования средств автоматизации требованиям законодательства;
- проверка осведомленности работников ГБПОУ о положениях законодательства Российской Федерации о персональных данных, документов Организации, устанавливающих порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;
- актуальность сведений, указанных в Уведомлении об обработке персональных данных ГБПОУ (при необходимости - отправка нового Уведомления в Роскомнадзор).

9.4. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений ГБПОУ.

9.5. 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.

9.6. Плановые (п. 21 Административного регламента проведения проверок Роскомнадзором при осуществлении контроля (надзора) за соответствием обработки персональных данных требованиям законодательства в области персональных данных) и внеплановые (п. 27 Административного регламента) проверки за соответствием обработки персональных данных

требованиям законодательства могут осуществляться Управлением Роскомнадзора по Центральному федеральному округу (территориальный орган Федеральной службы по надзору в сфере связи и массовых коммуникаций).

9.7. ФСТЭК России проводит проверки технической стороны построения системы защиты информации (актуальность угроз, наличие сертификата соответствия на средства защиты, достаточность применяемых мер).

9.8. 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.

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

9.10. Результаты проверок отражаются в Актах проверок.

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

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

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

9.13. При обнаружении нарушений руководитель ГБПОУ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

10. ОТВЕТСТВЕННОСТЬ

10.1. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Лица, виновные в нарушении норм, регулирующих обработку информации, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

Прекращение доступа к персональным данным и/или увольнение не освобождает работника ГБПОУ от принятых обязательств по неразглашению ПДн, ставших доступными при выполнении должностных обязанностей.

К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как ГБПОУ и его должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции.

10.2. Описание видов ответственности

Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 30 Федерального закона Российской Федерации от 30.12. 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации» и Правилами внутреннего трудового распорядка ГБПОУ.

Лица, виновные в нарушении правил работы с информацией, могут привлекаться к административной ответственности по следующим основаниям:

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП);
- нарушение правил защиты информации (ст. 13.12 КоАП);
- разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет уголовную ответственность),

лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).

Уголовная ответственность за нарушение правил работы с ПДн может наступить в следующих случаях:

- незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрируемом произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан (ст. 137 УК РФ);
- неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ);
- неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);
- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или повлекшее тяжкие последствия (ст.274 УК РФ).

Заместитель директора по безопасности _____ /Лемехов Д.Б.