Правительство Санкт-Петербурга
Комитет по образованию
Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа №266
с углубленным изучением иностранных языков
Адмиралтейского района Санкт-Петербурга

Принято
Педагогическим советом
Протокол № 1
от «31» 08 2020 г.

«Утверждаю»
Директор ГБОУ средней школы № 266
_____ /Э.Х. Папуциди/
Приказ № _____
от «31» _____ 2020 г.

ПОЛОЖЕНИЕ
о порядке организации и проведения работ по защите информации ограниченного доступа в ГБОУ средней школе № 266

1. Общие положения

1.1. Настоящее Положение разработано на основании требований:

- Федерального закона Российской Федерации от 25.07.2011г. №261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;
- Федеральный закон Российской Федерации от 30.12.2015г. №439-ФЗ «О внесении изменений в КоАП РФ»;
- 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»;

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».

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 средней школе № 266 (далее - ОУ) 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 ОУ.

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. Положение предназначено для практического использования должностными лицами, ответственным за защиту информации.

1.8. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами ОУ

1.9. За общее состояние защиты информации в ОУ отвечает его директор.

Персональная **ответственность за организацию и выполнение мероприятий по защите информации** в ОУ возлагается на заместителя директора по УВР.

Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с инструкцией «По работе пользователей информационной системы», утвержденной директором ОУ.

Проведение работ по защите информации в ИС с помощью встроенных средств безопасности, сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на **администратора ИС** (инженер, учитель информатики).

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

1.10. 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.

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

1.12. Положение может уточняться и корректироваться по мере необходимости.

2. Охраняемые сведения и актуальные угрозы

2.1.Охраняемые сведения - информация, обрабатываемая в ИС ОУ в соответствии с «Перечнем сведений конфиденциального характера в ОУ (Приложение 1), 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 средняя школа № 266 Адмиралтейского района Санкт-Петербурга» (Приложение 2);
- 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 ОУ,

актуальными являются только угрозы несанкционированного доступа (далее - НСД) к информационным ресурсам ИС с целью получения, разрушения, искажения и блокирования информации.

Применение средств технической разведки для перехвата информации, циркулирующей в ИС ОУ **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;
- 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 информации от НСД является обеспечение защиты информации путем выполнения требований Положения о методах и способах защиты информации в информационных системах персональных данных.

3.2. Целью технической защиты информации в ОУ 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 ОУ являются:

- исключение непреднамеренных действий сотрудников ОУ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации АС;
- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием АС (физический вынос информации на электронном носителе).

3.4. Директор ОУ 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 ГОУ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации;
- использование для защиты ИС от НСД встроенных средств защиты операционной системы (Windows 7 Pro, Windows 10), установленной на компьютере в соответствии с «Руководством по безопасной настройке»;
- использование программных /технических средств, сертифицированных по требованиям безопасности информации, для компьютеров с установленной операционной системой отличной от Windows 7 Pro, Windows 10 или подключенных к сетям связи общего пользования и (или) международного информационного обмена;
- 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 ОУ «Инструкции по работе пользователей информационной системы» (Приложение 3).

3.5. Документальное оформление мероприятий по защите объекта информатизации включает:
- приказ об организации работ по защите информации ограниченного доступа;
- акты классификации ИС;
- положение о порядке организации и проведения работ по защите информации ограниченного доступа в ОУ;
- технические паспорта;
- приказ о вводе в эксплуатацию;
- инструкции ответственного и по работе пользователей ИС;
- журнал учёта паролей пользователей для работы в ИС;
- журнал учёта машинных носителей информации;
- «Аттестат соответствия требованиям безопасности» или декларацию о соответствии требованиям безопасности.

4. Ввод в эксплуатацию информационных систем

4.1. Необходимым условием для ввода в эксплуатацию информационных систем ОУ является их соответствие требованиям Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных», постановления Правительства Российской Федерации от 17.11.2007 г. № 781 «Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и нормативно-методической документации ФСТЭК России по безопасности информации.

4.2. Директор ОУ 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 при условии классификации ИСПДн по 3 классу.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИС в соответствии с программой испытаний, согласованной с ОУ. 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 директора ОУ, подготавливаются и представляются на систему:
- акт классификации;
- 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 7 Pro, Windows 10 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 ОУ декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия **ответственным** разрабатываются и доводятся до сотрудников ОУ под роспись «Инструкция по работе пользователей ИСПДн» (Приложение 3) и рекомендации о порядке выполнения мероприятий по защите информации.

5. Особенности обработки информации, содержащей персональные данные

4.1. Все ПДн субъекта ОУ 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 ОУ 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.

4.3. ОУ 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.

4.4. 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.

4.5. 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.

4.6. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя директора ОУ или уполномоченного руководителем лицо.

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

4.8. 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.

4.9. 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.

4.10. 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.

4.11. 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 директора ОУ 4 или уполномоченного руководителем лицо.

4.12. 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 ОУ при обработке и защите его ПДн.

6. Обязанности и права должностных лиц

6.1. Директор организует работу по построению системы защиты ИС.

В частности,

- Назначает ответственного за организацию защиты информации из числа сотрудников ОУ.
- Утверждает состав комиссии по организации работ по защите информации.
- 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.

6.2. **Заместитель директора по УВР:**

- составляет Перечень сведений конфиденциального характера в ОУ;

отвечает за организацию и выполнение мероприятий по защите информации в ОУ;

- 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 ОУ, 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, 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 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 допуск к ИС;
- требует от пользователей устранения выявленных нарушений и недостатков, даёт 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 директору ОУ;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

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;

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

7.3. Контроль выполнения годового плана возлагается на директора ОУ.

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 директором.

8.4. Периодический контроль за эффективностью СЗИ осуществляет ответственный и представители отдела мобилизационной подготовки и защиты информации администрации Адмиралтейского района Санкт-Петербурга.

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 директор ОУ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

Приложение 1

Перечнем сведений конфиденциального характера в ГБОУ средняя школа № 266 Адмиралтейского района Санкт-Петербурга

Состав персональных данных обучающихся, их родителей (законных представителей)

– ФИО обучающего, родителя (законного представителя);
– Основной документ, удостоверяющий личность обучающего, родителя (законного представителя) (серия, номер, дата выдачи, кем выдан);
– Дата рождения обучающего, родителя (законного представителя);
– Место рождения обучающего;
– Гражданство обучающего, родителя (законного представителя);
– Адрес фактического проживания обучающего, родителя (законного представителя);
– Адрес регистрации обучающего, родителя (законного представителя), для временной регистрации – дата окончания регистрации;
– Телефон обучающего, родителя (законного представителя);
– Адрес электронной почты обучающего, родителя (законного представителя);
– СНИЛС обучающегося;
– Группа здоровья, физкультурная группа обучающегося;
– Откуда прибыл обучающийся, куда выбыл обучающийся (образовательная организация);
– Место работы родителя (законного представителя);
– Сведения о попечительстве, опеке, отношение к группе социально незащищенных обучающихся; документы (сведения), подтверждающие право на льготы, дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, многодетная семья, ребенок-сирота и т. п.);
– Изучение родного и иностранных языков;
– Сведения об успеваемости и внеучебной занятости (посещаемость занятий, оценки по предметам, расписание занятий, выбор предметов для сдачи ЕГЭ, государственной (итоговой) аттестации в 9 классе; сведения об участии в олимпиадах, грантах, конкурсах, наградах и т.п.);
– Участие в ГИА;
– Форма обучения, вид обучения, продолжение обучения после получения основного общего образования;
– Информация о выпускниках, их итоговой аттестации и трудоустройстве;
– Отношение к группе риска, поведенческий статус, сведения о правонарушениях;
– Сведения, содержащиеся в документах воинского учета;
– Документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний и т.п.);
– Виды помощи обучающимся, оказываемые образовательным учреждением - выплаты на питание, охват школьным питанием, компенсационные выплаты на питание.

Состав персональных данных работника

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные),
- сведения о воинском учете,
- данные о приеме на работу.
- сведения о переводах на другую работу,
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.

Приложение 2

«Перечнем информационных систем ГБОУ средняя школа № 266 Адмиралтейского района Санкт-Петербурга»

1. Автоматизированная информационная система управления (АИСУ) «Параграф»;
2. База «Метрополитена»;
3. База данных правонарушений.

Приложение 3

ИНСТРУКЦИЯ
администратора ИСПДн ГБОУ средняя школа № 266 Адмиралтейского района Санкт-Петербурга

1. Общие положения

1.1. Администратор информационных систем персональных данных (ИСПДн) (далее - Администратор) назначается приказом директора ГБОУ средняя школа № 266 Адмиралтейского района Санкт-Петербурга, на основании Положение о порядке организации и проведения работ по защите информации ограниченного доступа.

1.2. Администратор подчиняется директору школы.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ГБОУ средняя школа № 266 Адмиралтейского района.

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:
программного обеспечения автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное программное обеспечение (ПО));
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защите, в пределах, возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся специалистом ГБОУ средняя школа № 266 Адмиралтейского района, отвечающим за эту работу и(или) организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие

специальную проверку.
2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.
2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права и ответственность администратора ИСПДн

3.1 Администратор ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн, в том числе производить установку и настройку элементов ИСПДн, контролировать и поддерживать работоспособность ИСПДн и выполнять прочие действия в рамках должностных обязанностей.
3.2 Администраторы ИСПДн, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение 4

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
ГБОУ средняя школа № 266 Адмиралтейского района Санкт-Петербурга

1. Общие требования безопасности обработки информации в информационных системах персональных данных

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 266 с углубленным изучением французского языка Адмиралтейского района (далее - ГБОУ средняя школа № 266 Адмиралтейского района), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с "Перечнем защищаемых информационных ресурсов".

1.2. Действие настоящей Инструкции распространяется на ГБОУ средняя школа № 266 Адмиралтейского района.

1.3. Обработка защищаемой информации в ГБОУ средняя школа № 266 Адмиралтейского района разрешается на основании приказа руководителя ГБОУ средняя школа № 266 Адмиралтейского района.

1.4. Ответственность за организацию защиты информации в ГБОУ средняя школа № 266 Адмиралтейского района и выполнение установленных условий ее функционирования возлагается на администратора безопасности информации. Ответственность за выполнение мероприятий безопасности информации возлагается на лицо, производящее ее обработку (пользователя).

1.5. Допуск пользователей к работе в ГБОУ средняя школа № 266 Адмиралтейского района осуществляется в соответствии с "Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей", утверждаемом руководителем ГБОУ средняя школа № 266 Адмиралтейского района.

1.6. К самостоятельной работе на автоматизированных рабочих местах (АРМ), входящих в состав локальной сети ГБОУ средняя школа № 266 Адмиралтейского района, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.7. Помещения, в которых размещены технические средства ГБОУ средняя школа № 266 Адмиралтейского района. отвечают режимным требованиям и в нерабочее время закрываются в установленном порядке.

1.8. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении работников ГБОУ средняя школа № 266 Адмиралтейского района.

1.9. Техническое обслуживание и ремонт АРМ проводятся только уполномоченным лицом - инженером ЦИО ГБОУ средняя школа № 266 Адмиралтейского района. При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

1.10. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. Обязанности пользователя

2.1. При первичном допуске к работе в ГБОУ средняя школа № 266 Адмиралтейского района пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у должностного лица, выполняющего функции администратора безопасности информации в ГБОУ средняя школа № 266 Адмиралтейского района (далее - администратор безопасности).

2.2. Каждый работник ГБОУ средняя школа № 266 Адмиралтейского района, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ГБОУ средняя школа № 266 Адмиралтейского района, несет персональную ответственность[1] за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ГБОУ средняя школа № 266 Адмиралтейского района.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения

доступа только администратору безопасности ГБОУ средняя школа № 266 Адмиралтейского района.
2.2.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.
2.2.6. Немедленно ставить в известность администратора безопасности в следующих случаях:
- при подозрении компрометации личного пароля;
- обнаружения нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам ГБОУ средняя школа № 266 Адмиралтейского района;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ГБОУ средняя школа № 266 Адмиралтейского района;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных средств защиты;
- обнаружения непредусмотренных отводов кабелей и подключенных устройств;
- обнаружения фактов и попыток несанкционированного доступа и случаев нарушения установленного порядка обработки защищаемой информации.
2.3. Пользователю категорически запрещается:
2.3.1. Использовать компоненты программного и аппаратного обеспечения ГБОУ средняя школа № 266 Адмиралтейского района в неслужебных целях.
2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ГБОУ средняя школа № 266 Адмиралтейского района или устанавливать дополнительно любые программные и аппаратные средства.
2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.
2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (флеш-картах, DVD и CD-дисках, съемных дисках, картах памяти и т.п.).
2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа.
2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.
2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.
2.3.8. Производить перемещения технических средств АРМ без согласования с администратором безопасности.
2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего Акта.
2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.
2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.
2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.
2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.