Государственное бюджетное общеобразовательное учреждение
средняя общеобразовательная школа № 282
с углубленным изучением иностранных языков Кировского района Санкт-Петербурга
198217, г. Санкт-Петербург, бульвар Новаторов, д. 104, лит. А

ПРИНЯТО
Решением Совета ГБОУ СОШ № 282
Санкт-Петербурга
Протокол №7 от 25.08.2021

УТВЕРЖДЕНО
Приказом от 25.08.2021 №62.4
директор ГБОУ СОШ № 282
Санкт-Петербурга
_____В.В. Гребень

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B9E6EE00CE6C3C42B76C6FACB58F3008
Владелец: Гребень Виктория Васильевна
Действителен: с 31.01.2024 до 25.04.2025

ПОЛОЖЕНИЕ О ЗАЩИТЕ ИНФОРМАЦИИ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ № 282 С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ИНОСТРАННЫХ ЯЗЫКОВ КИРОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании требований Федерального Закона Российской Федерации от 27.07.2006 г. № 152 «О персональных данных»; Федерального Закона Российской Федерации от 27.07.2006 г. 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» и иных нормативно-правовых актов.

1.2. Под информацией, требующей защиты, понимаются сведения о Государственном бюджетном общеобразовательном учреждении средней общеобразовательной школе № 282 Кировского района Санкт-Петербурга (далее – ГБОУ № 282) и его деятельности.

1.3. Персональные данные являются составной частью конфиденциальной информации (далее – информация).

1.4. Цель данного Положения - на основании действующих законодательных актов и руководящих документов по защите информации создать необходимые организационно-правовые основы для построения эффективной системы защиты информации от несанкционированного доступа (СЗИ НСД) при обработке в автоматизированных системах ГБОУ № 282.

1.5. Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1.6. Положение определяет порядок организации в ГБОУ № 282 порядок работ по разработке и эксплуатации СЗИ НСД к АС.

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

1.8. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами ГБОУ № 282.

1.9. За общее состояние защиты информации в ГБОУ № 282 отвечает ответственный за организацию обработки персональных данных и администратор безопасности персональных данных ГБОУ № 282.

Ответственность за обеспечение защиты информации возлагается непосредственно на пользователей информации.

Проведение работ по защите информации в АС с помощью встроенных средств безопасности лицензионных операционных систем и антивирусного программного обеспечения возлагается на администратора безопасности АС.

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту конфиденциальной информации ГБОУ № 282.

1.10. Положение может уточняться и корректироваться по мере необходимости.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И ПОТЕНЦИАЛЬНЫЕ УГРОЗЫ

2.1. Охраняемые сведения - информация, обрабатываемая средствами вычислительной техники (СВТ) АС в ГБОУ № 282, а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты (объекты информатизации):

- АС различного назначения, участвующие в обработке информации;
- технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается;
- помещения, где установлены АС.

2.3. Потенциальные угрозы безопасности объектов информатизации.

В качестве угроз безопасности объектов информатизации в ГБОУ № 282 рассматриваются:

- использование технических средств для несанкционированного доступа (НСД) к информационным ресурсам АС с целью получения, разрушения, искажения и блокирования информации;

- преднамеренные действия нарушителей посредством НСД к АРМ, к носителям информации, к вводимой и выводимой информации, к программному обеспечению;
- непреднамеренные действия сотрудников ГБОУ № 282, приводящие к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации СВТ.

2.4. Перехват информации или воздействие на неё с использованием технических средств могут вестись:

- из-за границы контролируемой зоны из близлежащих строений и транспортных средств;
- при посещении ГБОУ № 282 посторонними лицами.

2.5. Применение средства технической разведки для перехвата информации, циркулирующей на объектах информатизации ГБОУ № 282 маловероятно с учётом её характера персональные данные на сотрудников и обучающихся детей.

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

- обрабатываемой АС от НСД и непреднамеренных действий;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в ЛВС при несанкционированном подключении к данной сети.

3. ДЕКЛАРИРОВАНИЯ СООТВЕТСТВИЯ И ВВОД В ЭКСПЛУАТАЦИЮ АС

3.1. Необходимым условием для ввода в эксплуатацию АС является её соответствие требованиям ФСТЭК России по безопасности информации. Руководство ГБОУ № 282 при условии классификации информационной системы персональных данных (ИСПДн) по 3 классу проводит её оценку соответствия декларированием соответствия АС требованиям нормативно-методической документации ФСТЭК России.

3.2. Для проведения классификации в ГБОУ № 282 создается комиссия. Состав комиссии утверждается приказом директора.

3.3. При декларировании соответствия АС требованиям безопасности информации настройки СЗИ с помощью встроенных средств защиты операционной системы «Windows» (или другой ОС) компьютера от НСД проводятся силами ГБОУ № 282.

3.4. Контроль эффективности СЗИ осуществляется представителями информационной безопасности администрации Санкт-Петербурга и Комитета образования Санкт-Петербурга с оформлением протокола испытаний АС на выполнение требований по защите от НСД.

3.5. В случае положительных результатов испытаний АС Руководство ГБОУ № 282 декларирует соответствие АС требованиям безопасности информации.

3.6. По результатам декларирования соответствия ответственным по информационной безопасности ГБОУ № 282 разрабатываются и доводятся до исполнителей инструкции и рекомендации о порядке выполнения мероприятий по защите информации.

4. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

4.1. Результатом достижения целей защиты информации является обеспечение защиты информации путем строгого соблюдения действующих норм и требований ФСТЭК России, созданием СЗИ НСД к АС и принятием эффективных организационных мер,предписанных руководящими документами.

4.2. Целями технической защиты информации в ГБОУ № 282 являются:

- исключение утечки информации с помощью технических средств разведки;
- предотвращение НСД посторонних лиц к информации, ее разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

4.3. Целями организационных мероприятий по защите информации в ГБОУ № 282 являются:

- исключение непреднамеренных действий сотрудников ГБОУ № 282, 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).

4.4. С целью закрытия возможных каналов утечки информации при её обработке и хранении на АС применяются следующие меры защиты:

- использование встроенных средств защиты операционной системы, установленной на компьютере;
- использование технических средств, сертифицированных по требованиям безопасности информации;
- предотвращение организационными мерами НСД к обрабатываемой информации;
- осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах;
- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации.

5. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

5.1. Руководство ГБОУ № 282:

- отвечает за организацию работ по защите информации в ГБОУ № 282;
- утверждает перечни сведений конфиденциального характера, защищаемых помещений, основных технических систем и средств, также другие документы по вопросам защиты информации;
- утверждает акты классификации АС.

5.2. Руководство ГБОУ № 282 и ответственный за информационную безопасность ГБОУ № 282 отвечает за организацию работ по защите информации в ГБОУ № 282:

- обеспечение безопасности обработки информации с помощью АС;
- порядок подготовки, учета и хранения документов конфиденциального характера, а также машинных носителей конфиденциальной информации;
- порядок передачи информации другим органам и организациям, а также между сотрудниками ГБОУ № 282.

5.3. Руководство ГБОУ № 282 и ответственный за информационную безопасность ГБОУ № 282:

- разрабатывает организационно-распорядительные документы по вопросам защиты информации;
- обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает работы по аттестации объекта вычислительной техники на соответствие нормативным требованиям;
- проводит систематический контроль работы СЗИ, применяемых на объектах информатизации, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;
- не допускает подключения к АС (ЛВС) устройств, не прошедших специальные исследования, не имеющих предписания на эксплуатацию;
- совместно с работниками ГБОУ № 282 осуществляет планирование мероприятий по подготовке АС к работе со сведениями конфиденциального характера, организовывает их выполнение и контроль их эффективности;
- 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 Руководству ГБОУ № 282;
- в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

5.4. Руководство ГБОУ № 282 и ответственный за информационную безопасность ГБОУ № 282 имеет право:

- контролировать исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;
- требовать от работников устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требовать от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- рекомендовать запрещать эксплуатацию систем обработки и передачи информации при несоблюдении требований по защите информации;
- определяет порядок и осуществляет контроль ремонта сертифицированных АС;
- вносить предложения по совершенствованию СЗИ НСД, изменению категорий объектов информатизации, степени конфиденциальности обрабатываемой информации.

5.5. Руководство ГБОУ № 282 и ответственный за информационную безопасность ГБОУ № 282:

- лично отвечают за защиту информации, 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 АС;
- участвуют в определении правил разграничения доступа к информации в системах и средствах информатизации, используемых в ГБОУ № 282.

6. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

6.1. Планирование работ по защите информации проводится на основании:

- рекомендаций актов проверок контрольными органами;
- результатов анализа деятельности в области защиты информации;
- рекомендаций и указаний ФСТЭК России;
- решений Комитета по информатизации и связи Санкт-Петербурга.

7. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. С целью своевременного выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения 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.

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

7.3. Повседневный контроль выполнения организационных и технических мероприятий, направленных на обеспечение защиты информации, проводится Руководством ГБОУ № 282 и ответственным по безопасности ГБОУ № 282.

7.4. Периодический контроль может осуществляться представителями ФСТЭК России, территориальных органов ФСБ России, управления информационной безопасности Санкт-Петербурга.

Допуск представителей этих органов для проведения контроля состояния защиты информации осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем

(заместителем) соответствующего органа.

7.5. Руководство ГБОУ № 282 и ответственный за информационную безопасность ГБОУ № 282 обязаны присутствовать при всех проверках по вопросам защиты информации

7.6. Результаты проверок отражаются в Актах проверок.

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

7.8. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

7.9. При обнаружении нарушений Руководство ГБОУ № 282 принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.