ПРИНЯТО
Педагогическим советом
протокол № 5 от 16 мая 2020 г.

УТВЕРЖДЕНО
приказом № 129 от 20 мая 2020 г.
Директор МБУ «Лицей №6»
_____ Е.Ю. Мицук

МБУ «Лицей № 6»

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ, ОБУЧАЮЩИХСЯ (ВОСПИТАННИКОВ) И ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ ОБЩЕОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ГОРОДСКОГО ОКРУГА ТОЛЬЯТТИ «ЛИЦЕЙ № 6 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА АЛЕКСАНДРА МАТВЕЕВИЧА МАТРОСОВА»

1. Общие положения

1.1. Настоящее Положение о защите персональных данных (далее – Положение) в муниципальном бюджетном общеобразовательном учреждении городского округа Тольятти «Лицей № 6 имени Героя Советского Союза Александра Матвеевича Матросова» разработано на основании требований:

- Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных»;
- Федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Специальных требований и рекомендаций по технической защите конфиденциальной информации», утвержденных приказом Гостехкомиссии России от 30 августа 2002 г. № 282;
- «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного приказом ФСТЭК России от 05.02.2010 №58.

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 Лицее 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 Лицея.

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

1.3. 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.

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

1.5. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами Лицея.

1.6. За общее состояние защиты информации в Лицее отвечает директор Лицея.

1.7. Персональная ответственность за организацию и выполнение мероприятий по защите информации в Лицее возлагается на сотрудника Лицея, назначенного приказом.

1.8. Ответственность за обеспечение защиты информации возлагается непосредственно на пользователя информации в соответствии с инструкцией «По работе пользователей информационной системы» (Приложение 1).

1.9. Проведение работ по защите информации в ИС с помощью встроенных средств безопасности, сертифицированных лицензионных операционных систем и антивирусного программного обеспечения, выполнения требований настоящего Положения, возлагается на ответственного за защиту информации в Лицее (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 Лицея в соответствии с «Перечнем сведений конфиденциального характера в Лицее» (Приложение 2), 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: АСУ РСО, Аттестаты, Питание, участники ГИА, Личные дела обучающихся, Библиотека, Сотрудники трудовые книжки, Кадры аттестация, 1С-зарплата, Расписание, Организаторы ГИА; 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 Лицее, 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 лицея 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 Лицея; 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, утверждённого приказом ФСТЭК России от 05.02.2010 № 58.

3.2. Целью технической защиты информации в Лицее 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 Лицее являются: исключение непреднамеренных действий сотрудников Лицея, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации ИС; сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием ИС (физический вынос информации на электронном носителе).

3.4. Директор Лицея 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 Лицее, 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 XP Pro» (и более поздних версий Windows X Pro) 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 XP Pro» (и более поздних версий Windows X Pro) 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 шкафах.

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 Лицее; журнал учёта паролей пользователей для работы в ИС (при необходимости); журнал учёта машинных носителей информации.

4. Ввод в эксплуатацию информационных систем

4.1. Необходимым условием для ввода в эксплуатацию информационных систем Лицея 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 Лицея 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 Лицея 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 Лицеем. Испытания завершаются выдачей «Аттестата соответствия ИС требованиям безопасности информации».

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

4.5. Для декларирования соответствия ИС требованиям п. 3.1 комиссией, утвержденной приказом руководителя ГОУ, 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 XP Pro» (и более поздних версий Windows X Pro) их настройка проводится силами самого Лицея.

4.8. В случае положительных результатов испытаний СЗИ директор Лицея декларирует соответствие ИС требованиям безопасности информации.

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

5. Особенности обработки информации, содержащей персональные данные

5.1. Все ПДн субъекта Лицея следует получать у него самого (для обучающихся лицея от родителей (законных представителей)). 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 Лицея 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.

5.2. Лицей 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.

5.3. Субъект ПДн самостоятельно принимает решение о предоставлении своих ПДн и дает согласие на их обработку (Приложение 3).

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

5.5. Согласие на обработку ПДн оформляется в письменном виде.

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

- фамилию, имя, отчество, адрес родителя (законного представителя) субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения о документе, подтверждающем родство;
- наименование (фамилию, имя, отчество) и адрес оператора[1], 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.

5.7. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя директора Лицея.

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

5.9. 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.

5.10. 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.

5.11. 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.

5.12. 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 Лицея или уполномоченного руководителем лицо.

5.13. Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия должностных лиц Лицея при обработке и защите его ПДн.

[1] МБУ «Лицей №6» является оператором обработки персональных данных (Регистрационный номер 08-0029080. Дата внесения оператора в реестр 16.12.2008)

6. Обязанности и права должностных лиц

6.1. Директор организует работу по построению системы защиты ИС. В частности:

6.1.1. Назначает ответственного за организацию защиты информации из числа сотрудников Лицея.

6.1.2. Утверждает состав комиссии по организации работ по защите информации.

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

6.1.4. 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 Лицее;
- контролирует работу ответственного по организации и проведению работ по защите информации в Лицее;
- 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, лично отвечают за защиту информации, сохранность машинных и иных носителей информации;
- организует выполнение мероприятий по защите информации при использовании технических средств;
- участвует в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИС;
- участвует в определении правил разграничения доступа к информации в ИС, используемых в ОУ.

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 Лицея, 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;
- 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 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 директору Лицея; в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.

7. Планирование работ по защите информации

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.

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 ответственным.

8.4. Периодический контроль за эффективностью СЗИ осуществляет заместитель директора по УВР.

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.

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

Приложение 1.

Инструкция «По работе пользователей информационной системы»

1. Общие положения

1.1. Настоящая инструкция регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационной системы персональных данных (далее ИСПДн) МБУ «Лицей № 6».

2. Термины и определения

2.1. **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.2. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.3. **Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель *(ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.4. **Доступ к информации** – возможность получения информации и её использования *(ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.5. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.6. **Информация** - сведения (сообщения, данные) независимо от формы их представления *(ст. 2 ФЗ РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).*

2.7. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.8. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.

2.9. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.10. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.11. **Пароль** - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.12. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.13. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.14. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. Общие обязанности сотрудников

Каждый сотрудник МБУ «Лицей №6», являющийся пользователем ИСПДн, обязан:

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

3.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ).

3.3. Соблюдать правила работы с паролем своей учётной записи.

3.4. Немедленно вызывать администратора безопасности ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.5. Всем сотрудникам МБУ «Лицей №6», являющимся пользователями ИСПДн, категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн МБУ «Лицей №6» в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;
- оставлять без присмотра своё АРМ не активизировав блокировки доступа или оставлять своё АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

4. Обеспечение сохранности информации

4.1. Для обеспечения сохранности электронных информационных ресурсов МБУ «Лицей №6» необходимо соблюдать следующие требования:

4.1.1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

4.2. Субъектам доступа запрещается:

- Установка и использование при работе с электронно-вычислительными машинами вредоносных программ, ведущих к блокированию работы сети;
- Самовольное изменение сетевых адресов;
- Самовольное вскрытие блоков электронно-вычислительных машин, модернизация или модификация электронно-вычислительных машин и программного обеспечения;
- Несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров из одного подразделения в другое производится только администратором безопасности ИСПДн с предварительно удаленными сетевыми настройками.

4.3. Сведения, содержащиеся в электронных документах и базах данных МБУ «Лицей №6», должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

5. Парольная защита

5.1. Личные пароли выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- Длина пароля должна быть не менее 6 символов;
- В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- Пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-ти позициях.

5.2. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

5.3. Для обеспечения возможности использования имён и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале.

5.4. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

5.5. Смена паролей должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.

5.6. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

5.7. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

5.8. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учётной записью и паролем другого пользователя.

5.9. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

6. Антивирусная защита

6.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с администратором безопасности ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах администратора безопасности ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

6.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

- Приостановить обработку данных;
- Немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения администратора безопасности ИСПДн, владельца заражённых файлов, а также смежные структурные подразделения, использующие эти файлы в работе;
- Совместно с владельцем файлов, заражённых вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;
- Произвести лечение или уничтожение заражённых файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности ИСПДн).

7. Ответственность за нарушение правил работы

7.1. Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

7.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

7.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями), влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник МБУ «Лицей №6», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МБУ «Лицей №6» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

7.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

7.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса Российской Федерации.

Рассмотрено на Совете лицея: Протокол № 1 от 29 августа 2018 г.

Рассмотрено на Совете обучающихся: Протокол № 1 от 23 августа 2018 г.

Рассмотрено на Совете родителей: Протокол № 1 от 23 августа 2018 г.

ЛИСТ ОЗНАКОМЛЕНИЯ

с «Инструкцией пользователя информационной системы персональных данных»

Дата ознакомления	**ФИО сотрудника, ознакомившегося с документом**	**Должность сотрудника, ознакомившегося с документом**	**Подпись сотрудника, ознакомившегося с документом**
1	**2**	**3**	**4**

Приложение 2.

Перечень сведений конфиденциального характера в лицее

В настоящем Перечне предусматриваются категории сведений, представляющих конфиденциальную информацию (персональные данные) в МБУ «Лицей №6», разглашение которых может нанести материальный, моральный или иной ущерб интересам данного учреждения, его работникам и обучающимся

№ п/п	Перечень сведений	Срок действия
1	**Финансы**	
1.1	Сведения о бухгалтерском учете (за исключением годового баланса).	3 года
1.2	Сведения о финансовых операциях.	3 года
1.3	Сведения о величине доходов и расходов, о состоянии дебиторской и кредиторской задолженностях (за исключением годового баланса).	3 года
1.4	Сведения, содержащиеся в финансово - договорных схемах учреждения.	+ 1 год после окончания действия договора
1.5	Личные доходы сотрудников	постоянно
2	**Личная безопасность сотрудников**	
2.1	Персональные данные, сведения о фактах, событиях и обстоятельствах частной жизни сотрудника.	постоянно
2.2	Сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда.	На период действия
2.3	Информация о личных отношениях специалистов как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.	3 года
3	**Персональные данные об обучающихся**	
3.1	Персональные данные обучающегося.	постоянно
3.2	Персональные данные родителей (законных представителей).	постоянно
3.3	Сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством.	постоянно
4	**Персональные данные о детях, оставшихся без попечения родителей**	
4.1	Персональные данные детей, оставшихся без попечения родителей.	постоянно
4.2	Персональные данные кандидатов в усыновители, приемные родители, опекуны.	постоянно
5	**Безопасность**	

5.1	Сведения о порядке и состоянии защиты конфиденциальной информации.	постоянно
5.2	Сведения о защищаемых информационных ресурсах в локальных сетях учреждения.	постоянно
5.2	Сведения об охране учреждения, системе сигнализации, о наличии средств контроля и управления доступом.	постоянно

Приложение 3.

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(ФИО заявителя)

_____ серия _____№_____ выдан _____
(вид основного документа, удостоверяющего личность, серия, номер, когда и кем выдан)
_____
_____,
адрес регистрации:_____,
являясь законным представителем субъекта персональных данных,
_____,
(Ф.И.О. ребенка)

_____серия_____№_____ выдан _____
_____
(вид основного документа, удостоверяющего личность субъекта персональных данных, серия, номер, когда и кем выдан)

место рождения _____дата рождения _____
проживающего по адресу_____
на основании
_____
(документ, подтверждающий полномочия законного представителя, реквизиты документа)

даю свое согласие на обработку в муниципальное общеобразовательное учреждение «Лицей №6», 445012, Самарская обл., г.Тольятти, ул.Мурысева, 61 (далее МБУ «Лицей №6»), school6@edu.tgl.ru (8482)242653
(наименование оператора персональных данных обучающихся, адрес оператора ПД, e-mail, телефон)

моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство, тип документа и данные документа, подтверждающий родство заявителя (или законность представления прав ребенка), данные о месте регистрации, данные о месте пребывания, номер мобильного (сотового) телефона, адрес электронной почты (e-mail), тип документа и данные документа, подтверждающие право на вне/первоочередное предоставление места в образовательном учреждении (организации), реализующим основные общеобразовательные программы _____
(иные данные)

а также персональных данных моего ребенка, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность ребенка; данные документа, удостоверяющего личность ребенка; гражданство ребенка, тип документа, данные о месте регистрации ребенка (индекс, наименование муниципального образования/городского округа, района, улицы, номер дома, квартиры), данные о месте пребывания ребенка (индекс, наименование муниципального образования/городского округа, района, улицы, номер дома, квартиры), тип и реквизиты

документа, подтверждающего наличие ограничений по здоровью, _____

_____

(иные данные)

Я даю согласие на использование моих персональных данных и персональных данных моего ребенка в целях передачи данных в государственную информационную систему «Автоматизированная система управления региональной системой образования», их обработки для приема заявления и зачисления в общеобразовательное учреждение (организацию) Самарской области, предоставления информации о текущей успеваемости учащегося, ведения электронного дневника и электронного журнала успеваемости, а также хранения данных на бумажных и электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных и персональных данных моего ребенка, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией (органу исполнительной власти, осуществляющему полномочия в сфере образования в Самарской области, в Российской Федерации), размещение на школьном сайте и выставочных стендах общей информации об успехах учащегося, (фамилии, имени, класса, фотографий, не ущемляющих его честь и достоинство), обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством РФ.

Я проинформирован (на), что _____

(наименование оператора персональных данных)

гарантирует обработку моих персональных данных и персональных данных моего ребенка в соответствии с действующим законодательством РФ как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

"__ ___" _____ 20_ г. _____ /_____/

Подпись Расшифровка подписи

номер телефона _____