ПРИНЯТО
педагогическим советом
гимназии
протокол № 4
от «14» апреля 2021 г.

Подписано цифровой подписью: Музюкина Ольга Юрьевна
DN: 1.2.643.3.131.1.1=120C303236323036313838363633, 1.2.643.100.3=120B303330333232036343137 39, email=zakupki_mu_uo@mail.ru, c=RU, st=Республика Башкортостан, l=г. Кумертау, o=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГИМНАЗИЯ № 1 ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА Н.Т. АНТОШКИНА ГОРОДСКОГО ОКРУГА ГОРОД КУМЕРТАУ РЕСПУБЛИКИ БАШКОРТОСТАН, givenName=Ольга Юрьевна, sn=Музюкина, cn=Музюкина Ольга Юрьевна

УТВЕРЖДАЮ
Директор МБОУ Гимназии № 1
им. Н.Т. Антошкина
_____ /О.Ю. Музюкина/
от «14» апреля 2021 г.

Положение
о порядке организации и проведения работ
по защите информации ограниченного доступа
в муниципальном бюджетном общеобразовательном учреждении Гимназии № 1
имени Героя Советского Союза Н.Т. Антошкина
городского округа город Кумертау Республики Башкортостан
(МБОУ Гимназия № 1 им. Н.Т. Антошкина)

1. Общие положения

1.1. Настоящее Положение разработано на основании требований:

- Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных»;
- Федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Правительства Российской Федерации от 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»,

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".

1.3. Цель данного Положения – определение порядка организации, и проведения работ в МБОУ Гимназии № 1 им. Н.Т. Антошкина 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 гимназии.

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

1.5. 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.

1.6. Положение предназначено для практического использования должностным лицам ответственным за защиту информации.
1.7. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами МБОУ Гимназии № 1 им. Н.Т. Антошкина.
1.8. За общее состояние защиты информации в МБОУ Гимназии № 1 им. Н.Т. Антошкина отвечает директор.
1.8.1. Ответственность за обеспечение защиты информации возлагается непосредственно *на пользователя информации* (приложение 1).
1.8.2. Проведения работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на техника МБОУ Гимназия № 1 им. Н.Т. Антошкина.
1.8.3. Контроль выполнения требований настоящего Положения возлагается на *ответственного за защиту информации* в МБОУ Гимназии № 1 им. Н.Т. Антошкина (далее – ответственный).
1.8.3.1. На ответственного за защиту информации в МБОУ Гимназии № 1 им. Н.Т. Антошкина (далее – ответственный) возлагается:
- проведения работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения;
- контроль выполнения требований настоящего Положения.
1.9. 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.
1.10. При необходимости для оказания услуг в области аттестации ИС можно привлекать специализированные организации, имеющие лицензию на этот вид деятельности.
1.11. Положение может уточняться и корректироваться по мере необходимости.

2. Охраняемые сведения и актуальные угрозы

2.1. Охраняемые сведения - информация, обрабатываемая в ИС МБОУ Гимназии № 1 им. Н.Т. Антошкина, к которой относятся:
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация относительно участников образовательных отношений;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально», представленная в виде носителей на бумажной, магнитной и иной основе.
2.2. Объекты защиты:
- ИС различного назначения, участвующие в обработке информации;
- 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина (приложение 2), *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 МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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 работников МБОУ Гимназии № 1 им. Н.Т. Антошкина,;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в ЛВС (локальной внутренней сети) при несанкционированном подключении к данной сети.

3. Организационные и технические мероприятия по защите информации

3.1. Направлением 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина, являются:

— исключение непреднамеренных действий работников МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина, самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п.1.8 настоящего Положения:

— назначение ответственного за организацию защиты информации;

— издание комплекта документов, определяющих политику в отношении обработки ПДн в МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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, 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 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 работниками МБОУ Гимназии № 1 им. Н.Т. Антошкина положение, приказов и других локальных актов по информационной безопасности, защите персональных данных;

4. Ввод в эксплуатацию информационных систем

4.1. Необходимым условием для ввода в эксплуатацию информационных систем МБОУ Гимназии № 1 им. Н.Т. Антошкина 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина 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.

5. Особенности обработки информации, содержащей персональные данные

5.1. Все ПДн субъекта МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина 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. МБОУ Гимназия № 1 им. Н.Т. Антошкина 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.

5.2. 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.

5.3. Согласие на обработку ПДн оформляется в письменном виде в соответствии с . Положением об обработке персональных данных работников МБОУ Гимназии № 1 им. Н.Т. Антошкина.

5.4. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу в соответствии с Положением об обработке персональных данных работников гимназии.

5.5. 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.

5.6. 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 в соответствии с Положением об обработке персональных данных работников МБОУ Гимназии № 1 им. Н.Т. Антошкина.

5.7. 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.

5.8. 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 гимназии или уполномоченного директором лицо.

5.9. Субъект вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия должностных лиц МБОУ Гимназии № 1 им. Н.Т. Антошкина при обработке и защите его ПДн.

6. Обязанности и права должностных лиц

6.1. Директор МБОУ Гимназии № 1 им. Н.Т. Антошкина организует работу по построению системы защиты ИС:

— назначает ответственного за организацию защиты информации (информационную безопасность) из числа работников МБОУ Гимназии № 1 им. Н.Т. Антошкина;

— утверждает состав комиссии по организации работ по защите информации.

— утверждает комплект документов, определяющих политику в отношении обработки ПДн в МБОУ Гимназии № 1 им. Н.Т. Антошкина, 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;

— 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;

— требует от работников МБОУ Гимназии № 1 им. Н.Т. Антошкина представления письменных объяснений по фактам нарушения режима конфиденциальности

6.2. Ответственный за организацию защиты информации (информационную безопасность):

— предоставляет и своевременно вносит дополнения в перечень сайтов федеральных органов управления образованием, учреждений образования федерального уровня, информационных сайтов федеральных программ и проектов, перечень федеральных информационно-образовательных порталов, а также описания новейших систем доступа к образовательным ресурсам сети Интернет, создаваемых на государственном уровне в рамках Федеральной целевой программы развития образования;

— проводит работу по организации и проведению работ по защите информации в МБОУ Гимназии № 1 им. Н.Т. Антошкина;

— совместно с техником предотвращает организационными мерами НСД к обрабатываемой в ИС информации;

— знакомит работников МБОУ Гимназии № 1 им. Н.Т. Антошкина, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;

— обеспечивает совместно с техником защиту информации, циркулирующей на

объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;

— проводит совместно с техником 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;

— принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИС;

— 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина 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 МБОУ Гимназии № 1 им. Н.Т. Антошкина

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 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 работниками МБОУ Гимназии № 1 им. Н.Т. Антошкина.

8.4. Периодический контроль в учебный модуль за эффективностью СЗИ осуществляет ответственный за организацию защиты информации (информационную безопасность) совместно с техником

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 за организацию защиты информации (информационную безопасность) 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 за организацию защиты информации (информационную безопасность) с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.

8.9. При обнаружении нарушений директор МБОУ Гимназии № 1 им. Н.Т. Антошкина принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

Приложение 1

ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

в МБОУ Гимназии № 1 им. Н.Т. Антошкина

№	Должность
ИСПДн – кабинет социального педагога (корпус №1, 1 этаж)	
1.	социальный педагог
ИСПДн – приемная (корпус №1, 2 этаж)	
2.	секретарь учебной части
3.	ответственный за кадровую работу
ИСПДн – кабинеты заместителя директора по УВР, ВР, АХЧ кабинет педагога-психолога (корпус №1, 2 этаж)	
4.	заместитель директора по УВР
5	заместитель директора по ВР
6.	педагог-психолог
7.	заместитель директора по АХЧ
ИСПДн – кабинет педагога-логопеда (корпус №2, 1 этаж)	
7.	учитель-логопед

Приложение 2

ПЕРЕЧЕНЬ СВЕДЕНИЙ ОГРАНИЧЕННОГО ДОСТУПА

в МБОУ Гимназии № 1 им. Н.Т. Антошкина

№ п/п	Содержание сведений	Правовое основание для включения в Перечень	Подразделения, использующие в работе сведения ограниченного доступа
1.	Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (персональные данные) Составление базы ПДн, ФИО, дата рождения, данные документов удостоверяющих личность, образование, дипломы, адреса проживания и регистрации, номера личных телефонов, а также любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу	ст. 85 Трудового кодекса РФ	секретарь учебной части ответственный за кадровую работу
2.	Персональные данные об обучающихся и их родителей (законных представителей) Составление базы ПДн, ФИО, дата рождения, данные документов удостоверяющих личность, адреса проживания и регистрации, родственные отношения, номера личных телефонов, а также любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу	ФЗ «О персональных данных» от 27.07.2006 г. № 152-ФЗ	заместители директора по УВР. ВР секретарь учебной части социальный педагог педагог-психолог учитель логопед
3.	Сведения по мобилизационной подготовке. Форма № 6, сведения об учащихся допризывного возраста.	ФЗ «О мобилиза-ционной подготовке и мобилизации в РФ»	секретарь учебной части ответственный за кадровую работу
4.	Выводы до завершения ревизии (проверки) и оформления ее результатов в виде акта (заключения)	ст. 15 ФЗ "О счетной палате РФ"	заместитель директора по АХЧ
5.	Паспорт антитеррористической защищённости учреждения,	Федеральный закон от 6 марта 2006 года N 35-ФЗ «О противодействии терроризму»	заместитель директора по АХЧ

Приложение 3

НОРМАТИВНО-ПРАВОВАЯ БАЗА
ОСУЩЕСТВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нормативно-правовая база

Федеральный закон от 27 июля 2006 г. №152-ФЗ "О персональных данных"
Федеральный закон от 27 июля 2006 г. №149-ФЗ "Об информации, информационных технологиях и о защите информации"
Постановление Правительства РФ от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
Приказ ФСТЭК России от 18 февраля 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"
Приказ ФСТЭК России от 11 февраля 2013 г. №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
Методический документ ФСТЭК России от 11 февраля 2014 г. "Меры защиты информации в государственных информационных системах"

Федеральный закон от 29.12.2010 г. № 436-ФЗ «О защитедетей от информации, причиняющей вред их здоровью и развитию»

Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей»

Информационная безопасность образовательной организации - состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.
Информационная безопасность является одним из составных элементов комплексной безопасности образовательной организации.

Приложение 4

МОДЕЛЬ УГРОЗ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АВТОМАТИЗИРОВАННОМ РАБОЧЕМ МЕСТЕ КАНЦЕЛЯРИИ (ПРИЕМНАЯ 1 ЭТАЖ), НЕИМЕЮЩИХ ПОДКЛЮЧЕНИЯ К СЕТЯМ МЕЖДУНАРОДНОГО ИНФОРМАЦИОННОГО ОБМЕНА

в МБОУ Гимназии № 1 им. Н.Т. Антошкина

Обозначения и сокращения.

АРМ - автоматизированное рабочее место
ВИ - видовая информация
ВТСС - вспомогательные технические средства и системы
ИСПДн - информационная система персональных данных
КЗ - контролируемая зона
МЭ - межсетевой экран
НДВ - недекларированные возможности
НСД - несанкционированный доступ
ОБПДн - обеспечение безопасности персональных данных
ОС - операционная система
ПДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПЭМИН - побочные электромагнитные излучения и наводки
РИ - речевая информация
СВТ - средство вычислительной техники
СЗИ - средство защиты информации
СПИ - стеганографическое преобразование информации
СЭУПИ - специальные электронные устройства перехвата информации
ТКУИ - технический канал утечки информации
ТСОИ - технические средства обработки информации
УБПДн - угрозы безопасности персональных данных

1. Термины и определения

В настоящем приложении используются следующие термины и их определения:

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

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного

распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им посвоим функциональному предназначению и техническим характеристикам.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

2. Общие положения.

2.1 ИСПДн подлежат классификации устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

2.2. Идентификация ИСПДн – выделение в ИТ-инфраструктуре областей учреждения (отдельных рабочих станций, узлов и сегментов сети), в которых осуществляется обработка ПДн, определение границ контролируемых зон для выделенных областей, присвоение наименований отдельным ИСПДн в составе ИТ-инфраструктуры учреждения, утверждение перечня защищаемых ИСПДн приказом директора МБОУ Гимназии № 1 им. Н.Т. Антошкина.

3. Исходные данные по ИСПДн.

3.1. Назначение и состав ИСПДн:

- ИСПДн предназначена для хранения и сбора ПДн работников гимназии, учащихся и их родителей (законных представителей), а именно: ФИО, даты рождения, пола, серии и номер документа удостоверяющего личность; сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством; персональные данные о детях, оставшихся без попечения родителей; персональные данные кандидатов в усыновители, приемные родители, опекуны.
- В состав ИСПДн входят: технические средства и их программное обеспечение и информационные ресурсы.

3.2. Условия размещения ИСПДн:

- территориально технические средства размещены в помещениях, находящихся в пределах контролируемой зоны МБОУ Гимназии № 1 им. Н.Т. Антошкина.

4. Классификация угроз безопасности.

4.1. Классификация ИСПДн - это присвоение каждой идентифицированной ИСПДн класса (К1, К2, К3, К4), соответствующего её индивидуальным признакам.

В соответствии с рекомендациями ФСТЭК России, класс ИСПДн определяется с учётом категорий и объёма обрабатываемых ПДн, и ей должен быть присвоен буквенно-цифровой индекс К1, К2, К3 или К4.

4.2. Типовым ИСПДн могут быть присвоены следующие классы:

- класс 1 (К1) – информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;
- класс 2 (К2) – информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;
- класс 3 (К3) – информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;
- класс 4 (К4) – информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

4.2.1. *Категория 1* – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Данные этой категории не обрабатываются в ИСПДн школы.

Разъяснение: данные о больничном или декретном отпуске, обрабатываемые в бухгалтерии – не являются ПДн 1 категории. Это не информация о состоянии здоровья и вообще не относится к персональным данным. Это информация о временной нетрудоспособности (именно так эти данные должны быть отражены в «Отчёте о внутренней нетрудоспособности» в разделе, описывающем бухгалтерскую систему).

4.2.2. *Категория 2* – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Это совокупность данных 3 категории с еще какими-либо данными. Например, сами по себе данные об образовании в совокупности с данными 4 категории (например, ФИО), не образуют данных 2 или 3 категории – это все так же останутся данные 4 категории. Но если данные об образовании обрабатываются вместе с данными 3 категории (ФИО и адрес прописки), то эта совокупность данных становится данными 2 категории.

4.2.3. *Категория 3* – персональные данные, позволяющие идентифицировать субъекта персональных данных.

Под идентификацией понимается – однозначное выделение субъекта из множества.

К персональным данным позволяющим идентифицировать человека относятся такие данные, которые позволяют установить личность человека.

Разъяснение: обработка только фамилии, имени и отчества – не позволяет идентифицировать человека, т.к. встречаются полные однофамильцы.

4.2.3.1. Наиболее часто встречающиеся совокупности данных, позволяющих идентифицировать субъекта:

паспортные данные (полностью);

ФИО (полностью) + дата рождения;

ФИО (полностью) + адрес проживания;

ФИО (полностью) + должность (если в базе данных указано название организации);

ФИО + фотография (качества не хуже, чем на паспорте).

Разъяснение: совокупность данных позволяющих идентифицировать субъекта (например, ФИО + дата рождения + адрес проживания) относится к 2 категории, как к данным позволяющим идентифицировать человека и получить о нем дополнительные сведения.

Разъяснение: обработка других данных о субъекте вместе с данными 3 категории (например, ФИО + дата рождения + данные об образовании), относит персональные данные к 2 категории.

4.2.4. *Категория 4* – обезличенные и / или общедоступные персональные данные.

Это данные не позволяющие идентифицировать человека. Наиболее часто встречающиеся совокупности данных, не позволяющих идентифицировать субъекта:

фамилия и инициалы + любые другие данные;

порядковый номер + любые другие данные.

Обезличивание данных, является одним из основных способов понижения класса ИСПДн.

4.3. В МБОУ Гимназии № 1 им. Н.Т. Антошкина обрабатываются следующие персональные данные: ФИО, даты рождения, пол, серии и номер документа удостоверяющего личность, домашние адреса и телефоны, семейное положение, а так же различные типы документов для участия в ГИА и ЕГЭ. Таким образом, категория ПДн (Хпд), обрабатываемых в ИСПДн может быть отнесена ко *2-й категории*, так как позволяют идентифицировать субъектаПДн и получить о нём дополнительную информацию, за исключением ПДн, относящейся к 1-й категории (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни).

В зависимости от объёма обрабатываемых ПДн (Хнпд) может быть присвоено значение *3* (в ИСПДН МБОУ Гимназии № 1 им. Н.Т. Антошкина одновременно отрабатываются данные менее чем 1000 субъектов персональных данных).

4.4. Класс ИСПДн МБОУ Гимназии № 1 им. Н.Т. Антошкина определяется в соответствии с таблицей №1.

Таблица 1

Хнпд / Хпд	**3**	**2**	**1**
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

По данным характеристикам обрабатываемых ПДн ИСПДн МБОУ Гимназии № 1 им. Н.Т. Антошкина относится к специальной информационной системе, так как в ИСПДн кроме обеспечения конфиденциальности ПДн, требуется обеспечить защищённость от уничтожения ПДн.

МБОУ Гимназии № 1 им. Н.Т. Антошкина может быть присвоен **класс 3 (К3 - специальная)** – информационные системы, для которых нарушение заданной

характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн.

5. Классификация угроз безопасности персональных данных.

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения **информативных сигналов**, содержащих **защищаемую информацию**, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы **обработки персональных данных**, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также **информационных технологий**, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

информационные технологии, применяемые при обработке ПДн;

технические средства, осуществляющие обработку ПДн (средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации) (далее - технические средства ИСПДн);

программные средства (операционные системы, системы управления базами данных и т.п.);

средства защиты информации;

вспомогательные технические средства и системы (**ВТСС**) - технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях (далее - служебные помещения), в которых расположены ИСПДн, их технические средства (различного рода телефонные средства и системы, средства вычислительной техники, средства и системы передачи данных в системе радиосвязи, средства и системы охранной и пожарной сигнализации, средства и системы оповещения и сигнализации, контрольно-измерительная аппаратура, средства и системы кондиционирования, средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения, средства электронной оргтехники, средства и системы электрочасофикации).

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и (или) случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

- источник УБПДн - субъект, материальный объект или физическое явление, создающиеУБПДн;

- среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

- носитель ПДн - физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

По способам реализации УБПДн выделяются следующие классы угроз:

- угрозы, связанные с **НСД** к ПДн (в том числе угрозы внедрения вредоносных программ);

- угрозы утечки ПДн по **техническим каналам утечки информации**;

- угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

- угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

- угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

- угрозы, реализуемые с использованием уязвимости системногоПО;

- угрозы, реализуемые с использованием уязвимости прикладного ПО;

- угрозы, возникающие в результате использования уязвимости, вызванной наличием вАС аппаратной закладки;

- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

- угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

- угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

- угрозы безопасности ПДн, обрабатываемых на АРМ;

- угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);

- угрозы безопасности ПДн, передаваемых по сетям связи;

- угрозы прикладным программам, с помощью которых обрабатываются ПДн;

- угрозы системному ПО, обеспечивающему функционирование ИСПДн.

6. Общая характеристика результатов несанкционированного или случайного доступа

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:
- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

Нарушение конфиденциальности может быть осуществлено в случае утечки информации:
- копирования ее на отчуждаемые носители информации;
- передачи ее по каналам передачи данных;
- при просмотре или копировании ее в ходе ремонта, модификации и утилизации программно-аппаратных средств;
- при "сборке мусора" нарушителем в процессе эксплуатации ИСПДн.

Нарушение целостности информации осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:
- микропрограммы, данные и драйвера устройств вычислительной системы;
- программы, данные и драйвера устройств, обеспечивающих загрузку операционной системы;
- программы и данные (дескрипторы, описатели, структуры, таблицы и т.д.) операционной системы;
- программы и данные прикладного программного обеспечения;
- программы и данные специального программного обеспечения;
- промежуточные (оперативные) значения программ и данных в процессе их обработки (чтения/записи, приема/передачи) средствами и устройствами вычислительной техники.

Нарушение **целостности информации** в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:
- конфигурацией сети;
- адресами и маршрутизацией передачи данных в сети;
- функциональным контролем сети;
- безопасностью информации в сети.

Нарушение доступности информации обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных **ресурсов системы**, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:
- средств обработки информации;
- средств ввода/вывода информации;
- средств хранения информации;
- аппаратуры и каналов передачи;
- средств защиты информации.

7. Типовые модели угроз безопасности ПДн, обрабатываемых в АРМ, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующихУБПДн:
- угрозы утечки информации по техническим каналам;
- угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:
- угрозы утечки акустической (речевой) информации;
- угрозы утечки видовой информации;
- угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям связи общего пользования. Угрозы из внешних сетей включают в себя:
- угрозы "Анализа сетевого трафика" с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей;
- угрозы получения НСД путем подмены доверенного объекта;
- угрозы типа "Отказ в обслуживании";
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.