

Муниципальное казенное общеобразовательное учреждение
«Туруханская средняя школа №1»

ПРИКАЗ

Номер документа	Дата составления
62/2	01.09.2017г

Об утверждении Положения об информационной безопасности в
Муниципальном казенном общеобразовательном учреждении
«Туруханская средняя школа № 1»

В целях обеспечения выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", иных нормативных правовых актов в сфере защиты персональных данных и иной конфиденциальной информации, руководствуясь п. 5.4.3 Устава Муниципального казенного общеобразовательного учреждения «Туруханская средняя школа № 1», утвержденного Постановлением администрации Туруханского района от 26.04.2017г. № 597-п

Приказываю:

1. Утвердить:

1.1. Положение об информационной безопасности в Муниципальном казенном общеобразовательном учреждении «Туруханская средняя школа № 1» (Приложение 1);

1.2. Форму журнала регистрации выявленных в Муниципальном казенном общеобразовательном учреждении «Туруханская средняя школа № 1» нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение 2);

1.3. Форму акта выявления в Муниципальном казенном общеобразовательном учреждении «Туруханская средняя школа № 1» нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение 3).

2. Инспектору по кадрам Жёлтиковой Н.А. ознакомить работников МКОУ «Туруханская СШ №1», ответственных за организацию обработки персональных данных.

3 Контроль исполнения настоящего приказа оставляю за собой.

Директор



Рыбьянец Т.В.



**Положение об информационной безопасности
в Муниципальном казенном общеобразовательном учреждении
«Туруханская средняя школа № 1»**

1. Общие положения

Организация информационной безопасности в Муниципальном казенном общеобразовательном учреждении «Туруханская средняя школа № 1» (далее Оператор) посредством назначения ответственного должностного лица и/или создания соответствующей службы (далее - Служба) необходима в целях выполнения требований действующего законодательства Российской Федерации, иных нормативных правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

2. Задачи

Основные задачи Службы заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений директору Оператора по совершенствованию и развитию системы обеспечения безопасности и защиты информации, в том числе персональных данных.

3. Функции

Для выполнения поставленных задач Служба осуществляет следующие функции.

1. Готовит и представляет на рассмотрение директору Оператора проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.
2. Организует и проводит классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты

информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3. Разрабатывает и реализует комплекс организационных мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- а также от иных неправомерных действий в отношении такой информации;

4. Для защиты информации, в том числе персональных данных от неправомерного доступа Служба обеспечивает:

- контроль за строгим соблюдением принятого Оператором Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

5. Служба при создании и эксплуатации информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;
- согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

6. Служба:

- разрабатывает и реализует меры организационного и технического по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- организует и (или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

7. Служба разрабатывает и реализует меры по информированию и обучению персонала Оператора, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

8. Служба контролирует выполнение установленных требований по:

- осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:

- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- соблюдению парольной защиты;

- соблюдению установленного регламента работы с электронной почтой;

- соблюдению требований к программному обеспечению и его использованию.

9. В соответствии с установленными локальными актами требованиями Служба обеспечивает:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты информации, в том числе персональных данных;

- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
- подготовку и предоставление отчётов директору Оператора, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;
- постоянный контроль за обеспечением уровня защищенности информации.

4. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Служба взаимодействует:

- с директором Оператора;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

В ходе взаимодействия директор и сотрудники Службы:

- в установленном порядке, получают необходимую для осуществления деятельности Службы информацию, разъяснения, уточнения, нормативные и иные документы;
- готовит и в установленном порядке вносят директору Оператора предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;
- готовят и в установленном порядке предоставляют информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

5. Ответственность

Ответственный за обеспечение информационной безопасности несет ответственность перед директором Оператора согласно действующему законодательству и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных задач и функций;
 - работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений;
 - выполнения требований правил внутреннего трудового распорядка;
 - соблюдения правил противопожарной безопасности.
- сохранности имущества Оператора принявшие его на ответственное хранение, согласно действующему законодательству, локальным нормативным правовым актами и договором о материальной ответственности;

- за своевременное и качественное выполнение требований действующего законодательства Российской Федерации, иных нормативных правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;

- обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, настоящим Положением, трудовыми договорами и должностными инструкциями.

Приложение 2 к приказу
Муниципального казенного
общеобразовательного учреждения
«Туруханская средняя школа № 1»
№_62/2__ от 01.09.2017г
Форма

Начат «__» _____ 20__ г.

Окончен «__» _____ 20__ г.

На _____ листах

ЖУРНАЛ
журнала регистрации выявленных в Управлении образования администрации Туруханского района нарушений в сфере защиты персональных данных и иной конфиденциальной информации

№	Дата выявления нарушения	Где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены
1	2	3	4	5	6

Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
7	8	9	10

Приложение 3 к приказу
Муниципального казенного
общеобразовательного учреждения
«Туруханская средняя школа № 1»
№__62/2_ от 01.09.2017г

А К Т №

**о выявлении в Муниципальном казенном общеобразовательном
учреждении «Туруханская средняя школа № 1» нарушений в сфере
защиты персональных данных и иной конфиденциальной информации**

_____ « ____ » _____ 20__ г

Настоящий акт составлен в том, что в

_____ (наименование, где выявлено нарушение)

ФИО _____ и _____ должность _____ лица, _____ допустившего
нарушение _____

допущено нарушение установленных требований в сфере защиты
персональных данных и иной конфиденциальной информации.

Содержание нарушения _____

_____ Требования каких нормативных документов нарушены _____

Комиссия (или уполномоченное лицо), выявившая нарушения
Подписи

(подпись)

(Ф. И. О.)

(подпись)

(Ф. И. О.)

(подпись)

(Ф. И. О.)

С актом ознакомлены:

подпись лица, допустившего нарушение _____ (ФИО _____)

подпись должностного лица, где допущено нарушение _____ (ФИО _____)