

УТВЕРЖДАЮ



Директор МБУ СШ г. Амурска

 В.В. Колганов

26 " июня 2025 г.

**Положение о порядке организации и проведении
работ по защите персональных данных
в Муниципальном бюджетном учреждении
дополнительного образования спортивной школе г. Амурска
Амурского муниципального района Хабаровского края**

г. Амурск

2025 г.

1. Общие положения

1.1. Положение о порядке организации и проведении работ по технической защите персональных данных в Муниципальном бюджетном учреждении дополнительного образования спортивной школе г. Амурска Амурского муниципального района Хабаровского края (далее соответственно – положение, МБУ СШ г. Амурска) является основным документом по защите персональных данных, содержащихся в базах данных, и определяет цели, порядок организации, планирования и выполнения мероприятий по технической защите персональных данных. Состав персональных данных представлен в локальном нормативном акте МБУ СШ г. Амурска «Перечень персональных данных».

1.2. Положение разработано в соответствии с требованиями законодательства Российской Федерации в части защиты персональных данных.

1.3. Требования настоящего положения направлены на предотвращение утечки защищаемой информации, несанкционированного доступа и специальных воздействий на информацию.

1.4. Основные направления работ по защите персональных данных (далее – ЗПДн):

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) разработка и практическая реализация организационных и технических мероприятий по защите:

информации, обрабатываемой средствами вычислительной техники (далее – СВТ);

информации, выводимой на экраны видеомониторов;

информации, хранящейся на физических носителях, в том числе, входящих

в состав информационной системы персональных данных (далее – ИСПДн);

3) своевременное обнаружение фактов несанкционированного доступа к информации;

4) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

5) недопущение вредоносного воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

6) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

7) постоянный контроль за обеспечением уровня защищенности информации.

1.5. Основные способы и меры защиты персональных данных:

1) привлечение лицензиатов ФСТЭК России для выполнения работ по технической защите персональных данных;

- 2) категорирование объектов информатизации;
- 3) противодействие утечке по техническим каналам, несанкционированному доступу, программно-техническому воздействию с целью нарушения целостности и доступности ПДн в процессе ее обработки, передачи и хранения;
- 4) применение автоматизированных систем в защищенном исполнении для обработки, хранения и передачи ПДн;
- 5) использование сертифицированных средств защиты ПДн от утечки по техническим каналам;
- 6) использование сертифицированных средств защиты ПДн от несанкционированного доступа (далее – НСД) и контроль их эффективности;
- 7) аттестация объектов информатизации по требованиям информационной безопасности.

1.6. Должностные лица, ответственные за выполнение требований настоящего положения:

- 1) ответственность за ЗПДн в МБУ СШ г. Амурска несет директор и все сотрудники, допущенные до работы с данной информацией;
- 2) организационно-методическое руководство работами по ЗПДн, выполнение работ по ЗПДн и контроль выполнения требований настоящего положения возлагается на сотрудников, допущенных к обработке персональных данных.

2. Порядок определения защищаемой информации

2.1. Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются в соответствии с законодательством Российской Федерации.

2.2. Сведения о персональных данных определены соответствующим перечнем, введенным в действие локальным актом МБУ СШ г. Амурска.

Организационные и технические мероприятия по ЗПДн осуществляются на основе требований нормативных правовых актов и документов в указанной сфере деятельности.

3. Порядок привлечения специализированных сторонних организаций при разработке и эксплуатации объектов информатизации и средств защиты

3.1. Организация работ по ЗПДн, реализация и контроль за эффективностью мер по ЗПДн возлагается на сотрудников, допущенных к обработке персональных данных.

3.2. Для выполнения мероприятий по ЗПДн могут привлекаться специализированные организации, имеющие соответствующие лицензии ФСТЭК России и/или ФСБ России.

3.3. При выполнении отдельных видов работ по ЗПДн с привлечением специализированных организаций назначаются соответствующие специалисты, ответственные за организацию и проведение данных работ.

3.4. Планируемые мероприятия по ЗПДн разрабатываются сотрудниками, допущенными к обработке персональных данных и включаются отдельным разделом в годовой план мероприятий организации по ЗПДн.

Раздел плана по ЗПДн предусматривает следующие подразделы:

мероприятия по выполнению решений ФСТЭК России, приказов и распоряжений вышестоящей организации по ЗПДн;

организационно-методическое обеспечение работ по ЗПДн (разработка, корректировка и согласование организационно-методических документов, планов, отчетов; составление заявок на технические устройства ЗПДн; обучение сотрудников);

контрольные мероприятия (оценка достаточности применяемых мер и средств ЗПДн; эффективность принимаемых мер ЗПДн в организации; участие в работе контролирующих органов).

4. Порядок разработки, ввода в действие и эксплуатации объектов информатизации

4.1. Порядок, методы и способы ЗПДн определяются нормативными правовыми актами и документами ФСБ России и ФСТЭК России.

4.2. Достаточность принятых мер по обеспечению безопасности ПДн при ее обработке в системах оценивается при проведении государственного контроля и надзора.

4.3. Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью СЗПДн, включающей организационные меры и средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки, а также используемые в ИСПДн информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

4.4. Эксплуатация СЗПДн и средств защиты в ее составе осуществляется в соответствии с технологическим процессом и инструкциями по эксплуатации средств защиты.

4.5. Для обеспечения защиты ПДн при эксплуатации СЗПДн и средств защиты необходимо соблюдать следующие требования:

доступ к защищаемой информации лиц, работающих в ИСПДн (пользователей, обслуживающего персонала), должен производиться в соответствии с порядком, установленным разрешительной системой доступа;

на период обработки ПДн в помещении, где размещаются основные технические средства и системы, могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации, допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в это помещение только в присутствии ответственного за обеспечение информационной безопасности;

при размещении в помещении нескольких технических средств отображения информации, должен быть исключен несанкционированный просмотр выводимой на них информации;

в случае компрометации парольной информации сотрудник, допущенный к обработке персональных данных, должен принять оперативные меры по замене паролей и идентификаторов, а также инициировать служебное расследование.

4.6. Все носители ПДн на бумажной, магнитной, оптической (магнито-оптической) основе, используемые в процессе обработки ПДн в ИСПДн, подлежат учету.

4.7. Временно не используемые учтенные носители информации должны храниться в специально оборудованных для этого местах, недоступных для посторонних лиц.

4.8. Периодический контроль включает в себя: контроль выполнения организационных мероприятий по ЗПДн в соответствии с годовым планом мероприятий по ЗПДн; инструментальный контроль эффективности внедренных средств защиты.

Инструментальный контроль проводится не реже одного раза в год с привлечением на договорной основе организаций, проводивших аттестацию этих объектов или других организаций, имеющих лицензию на соответствующий вид деятельности.

Инструментальный контроль является обязательным при вводе аттестованных рабочих мест в эксплуатацию; после установки, ремонта или замены средств ЗПДн; при изменении условий эксплуатации ОИ, размещения технических средств.

4.9. По результатам контроля составляется акт, в котором оценивается состояние СЗПДн, указываются имеющиеся нарушения и сроки их устранения, дается заключение.

Результаты работ докладываются директору МБУ СШ г. Амурска, который утверждает представляемый акт.

В случае имеющихся серьезных нарушений, работы на объекте информатизации приостанавливаются до их устранения.

5. Ответственность должностных лиц

5.1. Должностными лицами, ответственными за организацию и осуществление мероприятий по ЗПДн в организации являются:

- директор МБУ СШ г. Амурска;
- сотрудники, допущенные к обработке персональных данных.

5.2. Компетенция директора учреждения применительно к настоящему положению:

- определяет сотрудников школы, привлекаемых к ЗПДн;
- утверждает документы по ЗПДн;
- принимает решение о финансировании работ по ЗПДн;
- принимает решение о прекращении работ в случае выявления нарушений требований по ЗПДн, а также о возобновлении работ после их устранения.

5.3. Компетенция сотрудников, допущенных к обработке персональных данных:

- осуществляют годовое планирование мероприятий учреждения по ЗПДн и контроль за его выполнением;
- организуют разработку и внедрение необходимых организационно-технических мероприятий по ЗПДн в школе;
- представляют на утверждение директору учреждения документы по ЗПДн;
- оценивают эффективность принимаемых мер по ЗПДн и организует работы по устранению выявленных недостатков;
- формируют предложения по устранению недостатков по ЗПДн;
- выявляют нарушения в технологии обработки ПДн;
- проверяют правильность функционирования систем разграничения доступа к ПДн и наличие средств защиты ПДн;
- осуществляют документальное оформление проводимых защитных мероприятий;
- оказывают методическую помощь сотрудникам школы и проведении работ по ЗПДн.

6. Перечень локальных нормативных актов, необходимых для организации работы по защите персональных данных

Перечень сотрудников МБУ СШ г. Амурска допущенных к обработке персональных данных в ИСПДн.

Перечень сведений, содержащих персональные данные МБУ СШ г. Амурска.

Разрешительная система доступа к персональным данным, содержащимся в базах данных МБУ СШ г. Амурска.

Инструкция пользователя информационной системы персональных данных МБУ СШ г. Амурска.

Инструкция по организации парольной защиты.

Инструкция по антивирусной защите.

Инструкция по действиям пользователя в случае нештатной ситуации.

Инструкция администратора информационной безопасности.

Инструкция по архивации информационных ресурсов системы.

Инструкция по порядку учета и хранения съемных носителей.