

УТВЕРЖДАЮ
Директор МБОУ СОШ №1
ЗАТО Озерный

Сташкова Н.П.
«28» августа 2025 г.

ОПИСАНИЕ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА **обработки информации в сегменте АСУ СО ТО МБОУ СОШ №1 ЗАТО Озерный**

1. В процессе работы пользователь АСУ СО ТО создает файлы и массивы информации с применением прикладного программного обеспечения и подсистемы внешнего представления данных с последующим внесением данных в подсистемы АСУ СО ТО. Доступ к данным осуществляется через подсистему внешнего представления данных – программный компонент, обеспечивающий отображение информации из основных БД в графическом интерфейсе пользователя. Подсистема внешнего представления данных отображается посредством «тонкого клиента» – веб-браузера, через который осуществляется ввод данных путем заполнения форм, представленных в виде структурированных табличных форм. Доступ к программным модулям (компонентам системы) осуществляется на основе логина и пароля в соответствии с ролевой моделью разграничения прав доступа.

2. Вся информация хранится на жестких магнитных дисках на серверах, хранение метаданных осуществляется на жестких магнитных дисках автоматизированных рабочих мест пользователей. Ввод информации осуществляется с бумажных носителей информации путём ввода информации с клавиатуры, а также путем приема-передачи электронных сообщений через информационно-телекоммуникационную сеть «Интернет» с применением криптографических каналов связи на базе технологии ViPNet. Вывод информации осуществляется на электронные носители и на бумажные носители информации путем печати документов.

3. В процессе обработки в сегменте АСУ СО ТО МБОУ СОШ №1 ЗАТО Озерный на базе АРМ участвуют группы пользователей, имеющие доступ к АСУ СО ТО на объекте информатизации, на основании «Перечня лиц, допущенных к обработке персональных данных».

4. Перечень объектов доступа: несъемные жесткие магнитные диски (НЖМД), штатное программное обеспечение (ПО).

5. Перечень субъектов доступа: администратор безопасности информации, пользователи.

6. К работе на средствах вычислительной техники (СВТ) допускаются только сотрудники в соответствии с утвержденным «Списком лиц, допущенных к обработке персональных данных в АСУ СО ТО» и зарегистрированные в установленной системе защиты

информации от несанкционированного доступа (далее - СЗИ от НСД), после изучения организационно-распорядительной документации.

7. Подготовка персонального компьютера (далее – ПК) к работе:

- Включить ИБП, системный блок и монитор. После запроса системы необходимо набрать персональные логин и пароль на клавиатуре.

- Запустить программу антивирусного контроля и проверить жесткий диск и используемые съемные носители на наличие вирусов.

- При нарушении или сбое средств защиты информации (СЗИ), при отказе загрузки операционной системы или подключения защищенного хранилища - прекратить работу и пригласить администратора безопасности информации.

8. Перечень штатных средств доступа к информации на СВТ: представлен в Техническом паспорте на объекты информатизации автоматизированной системы управления сферой образования Тверской области (АСУ СО ТО).

9. На СВТ разрешается обработка персональных данных.

10. Если во время работы на ПК появилась необходимость временно покинуть рабочее место, пользователь обязан заблокировать ПК.

11. Описание реализованных правил разграничения доступа.

11.1. Обработка информации осуществляется только на предварительно учтенных носителях информации (защищаемых ресурсах) прошедших антивирусный контроль, причем каждый исполнитель для обработки информации использует только свой профиль пользователя, в котором администратором безопасности информации закреплены правила разграничения доступа: возможность доступа к дискам, папкам и файлам, возможность записи и чтения информации и т.д.

11.2. Запись производится только на учтенные носители информации.

11.3. Администратор безопасности информации организует и контролирует доступ пользователей к доступным ресурсам АСУ СО ТО и состояние информации на носителях.

11.5. Пользователи обязаны предъявлять, по требованию администратора безопасности информации, для проверки все числящиеся за ними документы и носители информации.

12. Пользователю **ЗАПРЕЩАЕТСЯ**:

- обрабатывать информацию в присутствии посторонних лиц;
- записывать информацию на неучтенные носители информации;
- использовать в работе пароли, если есть подозрение на их компрометацию;
- разглашать сведения о применяемой системе защиты и содержании информации;
- изменять и тиражировать программное обеспечение;
- вводить персональные данные под диктовку;
- производить передачу персональных данных по каналам связи без использования средств криптографической защиты.