УТВЕРЖДЕНО
приказом №346 от «04» 07 2022 г.
Директор ГАПОУ СО «ТМК»
И.В.Белякова

И 305-2022

ИНСТРУКЦИЯ
по работе в локальной вычислительной сети ГАПОУ СО «ТМК»

(взамен И 128-2016)

г.Тольятти
2022 г.

1. Общие положения.

1.1. Настоящая Инструкция регулирует порядок использования сотрудниками ГАПОУ СО «ТМК» (далее – Учреждение) таких сервисов локальной вычислительной сети (далее – ЛВС) как общие ресурсы.

1.2. Общие ресурсы размещаются на серверах Учреждения и предназначены для хранения документов, связанных исключительно с выполнением должностных обязанностей. Запрещается использовать ресурсы корпоративной сети для осуществления любого рода личной или посторонней коммерческой деятельности.

1.3. Инструкция разработана на основании предложений от подразделений Учреждения, лицензионных требований используемого в ЛВС программного обеспечения, с учетом технических возможностей оборудования и количества имеющихся у Учреждения лицензий на доступ к серверам под управлением оперативной системы Microsoft Windows Server 2008 R2, к базам данных 1С:Предприятие, на антивирусное программное обеспечение.

1.4. Настоящая Инструкция разрабатывается отделом информационных технологий (далее – отдел ИТ), утверждается приказом директора Учреждения.

1.5. Действующая редакция Инструкции размещается на общем сетевом ресурсе «Информация» в папке «Отдел ИТ информирует».

1.6. Каждый сотрудник, подключаемый к ЛВС Учреждения, обязан ознакомиться с данной Инструкцией и соблюдать её.

2. Получение доступа.

2.1. Перечень лиц, имеющих право получать доступ к общим ресурсам, определяется приказом директора Учреждения.

2.2. Приказ о допуске издается в начале учебного года. Проект приказа подготавливается руководителем отдела ИТ.

2.3. Сотрудники включаются в приказ по письменной заявке руководителя подразделения. Заявка подается в свободной форме в отдел ИТ до 10 сентября. В заявке должны быть указаны ФОИ сотрудников, перечень ресурсов, к которым им необходим доступ, инвентарные номера компьютеров, с которых следует организовать доступ, дата подачи заявки, ФИО и подпись руководителя подразделения.

2.4. Действующий приказ размещается на общем сетевом ресурсе «Информация» в папке «Отдел ИТ информирует».

2.5. Доступ к общим ресурсам возможен только с компьютера Учреждения с установленным на нем лицензионным программным обеспечением, в том числе антивирусным.

2.6. Максимальное количество пользователей ЛВС определяется количеством имеющихся у Учреждения лицензий на доступ к серверам под управлением операционной системы Microsoft Windows Server 2008 R2, к базам данных 1С: Предприятие, на антивирусное программное обеспечение и с учетом технических возможностей используемого в ЛВС оборудования.

2.7. Подключение выполняется сотрудниками отдела ИТ при наличии технической возможности подключения рабочего места сотрудника к ЛВС.

2.8. При приеме на работу нового сотрудника, либо при возникновении производственной необходимости в каком-либо подразделении, подключение к общим ресурсам производится сотрудниками отдела ИТ в течение трех рабочих дней по письменной заявке руководителя подразделения. Заявка подается в свободной форме в отдел ИТ. В заявке должны быть указаны ФИО сотрудников, перечень ресурсов, к которым им необходим доступ, инвентарные номера компьютеров, с которых следует организовать доступ, дата подачи заявки, ФИО и подпись руководителя подразделения. При выполнении подключения учитываются п.п.2.5 – 2.7. настоящей Инструкции.

2.9. Для доступа к общим ресурсам сотрудник вводит свои учетные данные (имя пользователя и пароль).

2.10. Учетные данные выдаются сотруднику руководителем отдела ИТ единожды (при первом подключении). При первом входе сотрудника в ЛВС Учреждения система попросит изменить пароль доступа. Новый пароль должен отвечать требованиям, указанным в разделе 4 настоящей Инструкции.

2.11. В случае утери пароля сотрудник обязан обратиться к руководителю отдела ИТ.

2.12. Действия на серверах Учреждения, выполненные под учетной записью сотрудника, передавшего свои учетные данные другому сотруднику или потерявшего свой пароль, расценивается как выполненные данным сотрудником.

3. Общие ресурсы на сервере.

3.1. Пользователю ЛВС могут быть доступны следующие общие ресурсы:

3.1.1. «Почта» - ресурс с полным доступом для всех зарегистрированных пользователей ЛВС – используется для оперативного обмена информацией:

- ресурс автоматически подключается при входе пользователя в ЛВС под своими именем и паролем;
- папки на ресурсе создаются самими пользователями;
- за удаление информации на нем отдел ИТ ответственности не несет.

3.1.2. «Информация» - ресурс с общей информацией, необходимой в работе подразделения Учреждения, а также для информирования сотрудников. Доступ на запись определяется приказом директора Учреждения.

- ресурс автоматически подключается при входе пользователя в ЛВС под своим именем и паролем.

3.1.3. «Методработа», «Бухгалтерия» - ресурсы для хранения документов учебной части, методической службы и бухгалтерии соответственно, ресурсы созданы по заявке подразделений:

- ресурс доступен только сотрудникам конкретного подразделения;
- ресурс автоматически подключается при входе пользователя в ЛВС под своими именем и паролем, в зависимости от того, в каком подразделении зарегистрирован пользователь, будет доступен тот или иной сетевой ресурс.

3.1.4. «Контингент» - ресурс с персональными данными обучающихся. Доступ к ресурсу определяется приказом директора Учреждения.

- ресурс монтируется вручную сотрудниками отдела ИТ;
- в системе ресурс не отображается;
- запрещается копирование информации с сервера на любые электронные носители.

3.1.5. «Студенту» - ресурс для размещения материалов к урокам для студентов, созданный по заявке преподавателей, работающих в компьютерных классах. Доступ на запись предоставлен только пед.работникам, остальным – доступ только для чтения:

- папки на ресурсе создаются и удаляются пед.работниками самостоятельно.

3.2. Удаление личных папок уволенных сотрудников выполняется сотрудниками отдела ИТ в течение 10 дней после издания приказа об увольнении. В течение этого времени руководитель подразделения может запросить данные сотрудника в отделе ИТ.

4. Политика паролей.

4.1. При создании пароля пользователи должны учитывать следующее:

- длина пароля – не менее 8 символов;
- пароль включает в себя прописные и строчные буквы, цифры;
- пароль может включать специальные символы;
- максимальный срок действия пароля ограничен двумя месяцами;
- новый пароль не совпадает как минимум с тремя предыдущими паролями;
- пароль не совпадает с именем учетной записи пользователя.

4.2. При создании паролей не серверах сотрудники отдела ИТ учитывают следующее:

- длина пароля – не менее 14 символов;
- пароль обязательно включает прописные и строчные буквы, цифры, специальные символы;
- максимальный срок действия пароля ограничен одним месяцем;
- новый пароль не совпадает как минимум с тремя предыдущими паролями;
- пароль не совпадает с именем учетной записи пользователя.

4.3. Для предотвращения попыток подбора пароля после 5 неудачных попыток авторизации учетная запись пользователя блокируется на 30 минут, после чего блокировка автоматически снимается. Сообщение о многократно неудавшихся попытках авторизации пользователя заносится в журнал системных событий. Для сервера в журнал событий заносится каждая неудавшаяся авторизация.

4.4. Недопустимо хранение пароля в открытом виде на любых видах носителей информации.

4.5. Каждый пользователь в индивидуальном порядке отвечает за понимание и правильное отношение к правилам безопасности систем, которые он использует. В программах, установленных на его компьютере, использующих парольную защиту, пользователь обязан выбирать качественный пароль и периодически самостоятельно менять его.

4.6. Каждый пользователь обязан:

- не разглашать учетные данные;
- использовать пароли, отвечающие требованиям политики паролей, действующих в Учреждении;
- изменять временный пароль при первом входе в систему;
- не использовать автоматический вход в систему;
- осуществлять выход из системы (завершение сеанса) при завершении своей работы за компьютером.

5. Безопасность и устойчивость ЛВС.

5.1. Составляющие безопасности ЛВС:

- конфиденциальность – защита от несанкционированного получения информации;
- целостность – защита от несанкционированного изменения информации.

Прямое или косвенное нарушение одной из составляющих является нарушением безопасности ЛВС.

5.2. Пользователь, использующий носители информации, несет ответственность за антивирусную чистоту содержащихся на них данных.

5.3. В случае получения носителя информации из сомнительного источника пользователь обязан проверить его на «вирусы».

5.4. На компьютерах, участвующих в обработке персональных данных, использование посторонних (не принадлежащих Учреждению) носителей информации запрещается. Перед началом каждого использования носителя пользователь обязан выполнить его полную проверку на «вирусы».

5.5. Пользователю категорически запрещается открывать подозрительные почтовые сообщения и вложенные в них файлы.

5.6. В случае подозрения на заражение компьютера «вирусом» пользователь обязан немедленно выключить компьютер и обратиться в отдел ИТ.

5.7. При обнаружении неисправности компьютерного или сетевого оборудования пользователь обязан незамедлительно подать заявку в отдел ИТ.

5.8. Пользователям запрещается самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного и программного обеспечения, а также подключать компьютерную технику к ЛВС Учреждения.

5.9. Пользователям запрещается предпринимать какие-либо действия прямо или косвенно направленные на нарушение нормальной работы сетевого оборудования и разрушение общих информационных ресурсов.

5.10. В ЛВС Учреждения ведется мониторинг сетевых событий. Перечень событий, подлежащих протоколированию, определяется отделом ИТ. Полученные при мониторинге электронные журналы событий используются для анализа работы ЛВС, а также могут служить доказательством неправомерных действий пользователей.

5.11. Для надежной и безопасной работы основных сервисов, функционирующих в ЛВС, а также для обеспечения сохранности информации пользователей на сервере выполняется автоматическое резервное копирование.

5.12. На общих ресурсах, а также на компьютерах Учреждения запрещается размещать личные данные, данные, не связанные с исполнением должностных обязанностей.

5.13. На общих ресурсах (кроме папки «Контингент») категорически запрещается размещать конфиденциальную информацию, в том числе персональные данные. За размещение на общем ресурсе конфиденциальной информации ответственность несет пользователь, разместивший её.

5.14. При работе с персональными данными сотрудники обязаны соблюдать требования законодательства о защите персональных данных и действующие в Учреждении локальные нормативные акты, касаемые персональных данных.

5.15. Пользователи, чьи действия привели к нарушению нормального (безопасного) функционирования ЛВС Учреждения и повлекшие за собой материальный и моральный ущерб Учреждению, должностным лицам или другим пользователям, несут ответственность. Ответственность определяется действующим законодательством и административными мерами.

РАЗРАБОТАНО:

И.о.руководителя отдела информационных технологий «20» 06 2022 г. А.Д.Березин

СОГЛАСОВАНО:

Инспектор по кадрам «23» 06 2022 г. Т.О.Медяшкина

Юрисконсульт «21» 06 2022 г. Э.Н.Зайкова