Частное профессиональное образовательное учреждение

**СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ**

Утвержден приказом

директора техникума

от «\_\_09\_\_\_» \_\_\_01\_\_ 2020 г.

№\_\_1-ИБ\_\_\_\_\_\_\_\_

Регистрационный № \_\_101\_\_\_

**Инструкция по обеспечению информационной безопасности руководителями и работниками ЧПОУ Социально-технологического техникума при использовании в работе персональных компьютеров, имеющих доступ к информационным ресурсам и Интернет**

**1. Общие положения**

1.1. Настоящая Инструкция разработана на основании:

* Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Гигиенических требований к персональным электронно-вычислительным машинам и организации работы (СанПиН 2.2.2/2.4.1340-03).

1.2. Инструкция определяет основные обязанности и ответственность руководителей и сотрудников образовательной организации – пользователей персональных компьютеров (далее – пользователи), имеющих доступ к информационным ресурсам локальной вычислительной сети образовательной организации (далее – ЛВС) и Интернет.

1.3. Основная цель обеспечения информационной безопасности – предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в ЛВС.

1.4. Методическое руководство работой пользователей, организацию антивирусного контроля, установку средств антивирусного контроля, настройку параметров ЛВС и персональных компьютеров осуществляет ответственное лицо из числа технических специалистов, назначенное руководителем образовательной организации. К перечисленным работам могут быть привлечены сторонние специалисты/организации на основании соответствующего договора.

1.5. Положения инструкции обязательны для исполнения всеми пользователями и доводятся под роспись. Пользователь должен быть предупрежден об ответственности за ее нарушение.

1.6. Контроль за выполнением требований настоящей Инструкции осуществляется руководителем образовательной организации

**2. Общие правила работы в ЛВС**

2.1. Работа в ЛВС производится сотрудниками образовательной организации с целью получения необходимой информации для выполнения возложенных на них должностных обязанностей на закрепленных за ними персональных компьютерах/автоматизированных рабочих местах (далее – АРМ).

2.2. Запрос на установку АРМ, его настройку и установку сетевого программного обеспечения осуществляется с санкции руководителя образовательной организации по предварительной заявке/служебной записке на имя руководителя образовательной организации.

2.3. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется техническими специалистами.

2.4. Несогласованное подключение внешних устройств и установка программного оборудования запрещены.

2.8. При нарушении нормальной работы сети и в случае обнаружения неисправности любого компьютерного и сетевого оборудования, а также при сбое или неправильной работе программного обеспечения пользователь обязан немедленно сообщить техническим специалистам.

## 3. Общие правила использования сети Интернет

3.1. Доступ к сети Интернет предоставляется сотрудникам образовательной организации в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

3.2. Предоставление доступа сотрудника к сети Интернет осуществляется с санкции руководителя образовательной организации по предварительной заявке/служебной записке на имя руководителя образовательной организации.

3.3. Подключение АРМ к сети Интернет выполняется техническими специалистами по распоряжению руководителя образовательной организации.

3.4. При использовании сети Интернет запрещено:

* использовать доступ в сеть Интернет в личных целях;
* публиковать, загружать и распространять:

- материалы, нарушающие действующее законодательство;

- материалы, несовместимые с этическими нормами поведения педагогического работника;

- конфиденциальную информацию;

- информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения правообладателя;

- угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.5. Информация о посещаемых Интернет-ресурсах протоколируется для последующего анализа и при необходимости может быть предоставлена руководителю образовательной организации для контроля и принятия соответствующего решения.

3.6. Организация в праве блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством.

3.7. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного программного обеспечения.

**4. Правила организации парольной защиты информационной системы**

4.1. Личные пароли выбираются пользователями самостоятельно с учетом следующих требований:

* длина пароля должна быть не менее 6 символов;
* среди символов пароля обязательно должны присутствовать буквы и цифры;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.);
* личный пароль пользователь не имеет права сообщать никому;
* смена паролей пользователей должна проводиться регулярно в соответствии с установленным порядком.

4.2. Внеплановая смена личного пароля или удаление учетной записи пользователя компьютерной сети в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) производится администратором после окончания последнего сеанса работы данного пользователя с ЛВС по распоряжению руководителя образовательной организации.

4.3. Хранение пользователями значений своих действующих паролей на бумажном носителе допускается только в местах, защищенных от несанкционированного доступа третьих лиц.

4.4. Повседневный контроль при работе пользователей информационной системы с паролями, соблюдением порядка их смены хранения и использования возлагается на администратора ЛВС.

**5. Правила организации антивирусной защиты**

5.1. К использованию в информационной системе образовательной организации допускаются только лицензионные антивирусные средства.

5.2. Установка средств антивирусного контроля на компьютерах, серверах ЛВС осуществляется техническими специалистами по распоряжению руководителя образовательной организации.

5.3. В начале работы при включении АРМ, а также при первом доступе к файлам в автоматическом режиме проводится их антивирусный контроль.

5.4. Не реже одного раза в неделю в автоматическом режиме производится полная проверка дисков персональных компьютеров, подключенных к ЛВС, на наличие вирусов.

5.5 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).

5.6. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщение о системных ошибках и т.п.), пользователь вместе с техническим специалистом должен провести внеочередной антивирусный контроль.

5.7. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов непосредственное руководство, владельца зараженных файлов, а также других пользователей, использующие эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* вместе с техническим специалистом провести лечение или уничтожение зараженных файлов.

**6. Обязанности пользователя – сотрудника образовательной организации**

Пользователь обязан:

6.1. Строго соблюдать изложенные выше:

* правила обеспечения информационной безопасности при работе с программными и техническими средствами ЛВС и доступа к Интернет;
* правила парольной защиты;
* правила антивирусной защиты.

6.2. Хранить в тайне свои идентификационные данные (имена, пароли и т.д.) и осуществлять вход в ЛВС только под своими идентификационными данными в разрешенный период времени.

6.3. Немедленно вызывать администратора ЛВС и ставить в известность руководителя образовательной организации при:

* подозрении о компрометации личных идентификаторов и паролей;
* обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа;
* обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
* обнаружении некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключенных устройств;
* выходе из строя или неустойчивом функционировании узлов АРМ или периферийных устройств, а также перебоях в системе электроснабжения.

6.4. Немедленно выполнять предписания администраторов безопасности ЛВС.

6.5.Предоставлять свое АРМ администратору безопасности для планового и внеочередного контроля.

6.6. Проводить полное или частичное резервное копирование служебной информации в соответствии с установленным порядком.

6.7. Осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера, с машинных носителей информации и из оперативной памяти АРМ.

6.8. Уважать права других пользователей на конфиденциальность и право пользования общими ресурсами.

Пользователям запрещается:

6.9. Самостоятельно переставлять и передвигать, а также подключать компьютерную технику в помещении (в том числе при проведении генеральных уборок, перестановке мебели и пр.).

6.10. Самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного или программного обеспечения.

**7. Обязанности пользователя – руководителя образовательной организации образовательной организации**

Руководительдля обеспечения информационной безопасности обязан:

7.1. Организовывать и контролировать вопросы информационной безопасности в образовательной организации в соответствии с действующим законодательством.

7.2. Издать соответствующий распорядительный документ, в котором предусмотрено:

* определение круга лиц, допущенных к работе в ЛВС и сети Интернет;
* назначение ответственного лица за обеспечение информационной безопасности;
* порядок осуществления антивирусного контроля;
* ознакомление под роспись лиц, допущенных к работе в ЛВС и сети Интернет, с перечисленными выше правилами и предупреждение об ответственности за их нарушение.

7.3. Контролировать работы по внесению изменений в аппаратно-программную конфигурацию компьютеров в образовательной организации

7.4. Контролировать соблюдение требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ ЛВС.

7.5. Осуществлять контроль за соблюдением пользователями требований настоящей Инструкции.

**8. Права пользователя – сотрудника образовательной организации**

Пользователь имеет право:

8.1. Осуществлять доступ к программным и аппаратным средствам информационной системы в пределах предоставленных полномочий и в соответствии с закрепленными за ним обязанностями.

8.2. Обращаться к техническим специалистам и руководству за необходимой технической и методической помощью.

8.3. Участвовать в анализе ситуаций, касающихся функционирования АРМ и рабочих программ.

8.4. Знакомиться с проектами решений руководства организации, касающимися его деятельности.

8.5. Вносить на рассмотрение руководства предложения по совершенствованию работы ЛВС и закрепленного за ним АРМ.

**9. Права пользователя – руководителя образовательной организации**

Руководитель имеет право на все перечисленные выше права пользователя – сотрудника образовательной организации и, в дополнение к ним:

9.1. Требовать от сотрудников образовательной организации выполнения положений действующего законодательства и локальных нормативных актов по обеспечению информационной безопасности.

9.2. Требовать от пользователей информационной системы своевременного информирования о возникновении сбоев в работе ЛВС и АРМ и/или инцидентов, связанных с нарушением правил эксплуатации оборудования, правил доступа к информационной системе.

9.3. Давать сотрудникам образовательной организации обязательные для выполнения указания по работе с информационной системой.

9.4. Инициировать и проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, модификации, порчи программных и аппаратных элементов ЛВС, правил эксплуатации технических средств.

9.5. Привлекать сотрудников образовательной организации к проведению плановых и внеочередных работ по обеспечению информационной безопасности, установке и модернизации программных и аппаратных средств.

9.6. Вести переписку со сторонними организациями по вопросам, входящим в его компетенцию.

# 10. Ответственность

Пользователи несут ответственность:

10.1. За неисполнение или ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, ‒ в пределах, определенных действующим трудовым законодательством Российской Федерации;

10.2. За причинение материального ущерба работодателю ‒ в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации;

10.3. За правонарушения, совершенные в процессе осуществления своей деятельности, ‒ в пределах, определенных действующим административным, уголовным, гражданским законодательством Российской Федерации.

10.4. За качество проводимых работ по контролю всех групп пользователей информационной системы в вопросах обеспечения безопасности персональных данных.

10.5. За обеспечение устойчивой работоспособности информационной системы.

С инструкцией ознакомлен:

|  |  |  |  |
| --- | --- | --- | --- |
| ФИО | должность | подпись | дата |
| Макарова Любовь Германовна | Директор |  |  |
| Садыриева Ирина Николаевна | секретарь |  |  |
| Углов Евгений Сергеевич | преподаватель |  |  |
| Садыриев Руслан Маратович | преподаватель |  |  |
| Иконникова Юлия Владимировна | преподаватель |  |  |
| Лучникова Татьяна Анатольевна | преподаватель |  |  |
| Саранчук Андрей Николаевич | преподаватель |  |  |
| Дрозд Ольга Витальевна | преподаватель |  |  |
| Тихонова Людмила Валерьевна | преподаватель |  |  |