МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ТОЛЬЯТТИНСКИЙ ХИМИКО-ТЕХНОЛОГИЧЕСКИЙ ТЕХНИКУМ»

УТВЕРЖДАЮ
и. о. директора ГБПОУ «Тольяттинский химико-технологический техникум»
_____ Т. А. Михайленко
Приказ от «23» января 2019 г. № 6/1-од

Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей ГБПОУ «Тольяттинский химико-технологический техникум»

СОГЛАСОВАНО
Советом Учреждения
протокол от 22.01.2019 г. № 1

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных (далее - ИСПДн), необходим для выполнения ими служебных (трудовых) обязанностей ГБПОУ «Тольяттинский химико-технологический техникум» (далее – Учреждение) разработан с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе в защите прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей в Учреждении (далее – Правила), обязателен для всех работников Учреждения, осуществляющих обработку и допущенных к персональным данным, устанавливает требования по обеспечению получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности Учреждения.

1.3. Правила разработаны на основании Трудового кодекса РФ, Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федерального закона от 26.07.2006 г. № 149-ФЗ «Об информации, информатизации и защите информации», приказа Федеральной службы по техническому и экспортному контролю России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», постановлений Правительства РФ.

1.4. Пользователем является работник Учреждения, участвующих в рамках своих функциональных обязанностях в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты (далее – Пользователь). Персональный состав пользователей утверждается приказом директора.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

2.1. Пользователь обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации, приказов, регламентирующих порядок действий по защите информации в Учреждении.

2.2. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

2.3. Осуществлять обработку персональных данных (далее – ПДн) исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля и качества выполняемой работы и обеспечения сохранности имущества.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Во время работы экран монитора располагать так, чтобы исключать возможность несанкционированного ознакомления с отображаемой на них информацией посторонним лицам.

2.7. Получать необходимые ПДн непосредственно у субъекта персональных данных.

2.8. Если ПДн возможно получить только у третьей стороны, то Пользователь обязан уведомить субъекта ПДн об этом заранее, получить от него письменное согласие, сообщить о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение.

2.9. Обо всех выявленных нарушениях, связанных с информационной безопасностью необходимо обратиться к ответственному за информационную безопасность в Учреждении.

2.10. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

2.11. Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

2.12. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

2.13. Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;

– Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;

– Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

– Выполнять требования инструкции по организации антивирусной защиты в полном объеме;

– Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

– Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

– Некорректного функционирования установленных на АРМ технических средств защиты;

– Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

– Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

– Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

– Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);

– Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

– Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

– Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;

- Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.