П-105/2019

Министерство образования и науки Самарской области
ГБПОУ «ТК им. Н.Д. Кузнецова»

Протокол заседания Совета Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета обучающихся Учреждения
от 29.10.2019г. № 20

Протокол заседания Совета родителей Учреждения
от 29.10.2019г. № 20

УТВЕРЖДАЮ
Директор
ГБПОУ «ТК им. Н.Д. Кузнецова»
_____А.Н. Сакеев
«29» октября 2019г.

Приказ № 522 о/д от 29.10.2019

Инструкция
по обеспечению информационной безопасности руководителями и работниками структурных подразделений при использовании в работе персональных компьютеров, имеющих доступ к информационным ресурсам и Интернет

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция разработана в соответствии с «Положением о порядке обработки персональных данных в ГБПОУ «ТК им. Н.Д. Кузнецова»», «Политикой ГБПОУ «ТК им. Н.Д. Кузнецова» в отношении обработки персональных данных сотрудников учреждения, а также обучающихся и (или) родителей (законных представителей)», утверждённых приказом директора ГБПОУ «ТК им. Н.Д. Кузнецова» № 294 о/д от 18.07.2018., и определяет основные права, обязанности и ответственность работников ГБПОУ «ТК им. Н.Д. Кузнецова» (далее - Учреждение) - пользователей персональных компьютеров (далее - ПК), имеющих доступ к информационным ресурсам локальной сети Учреждения и сети «Интернет».

1.2. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах Учреждения.

2. Обязанности работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет»

2.1. Работники Учреждения - пользователи ПК, имеющие доступ к информационным ресурсам локальной сети Учреждения и сети «Интернет» обязаны:

2.1.1. Знать и соблюдать требования настоящей Инструкции и других документов по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам локальной сети Учреждения и сети «Интернет»;

2.1.2. Знать и уметь правильно использовать то аппаратно - программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них;

2.1.3. Хранить в тайне свой пароль (пароли);

2.1.4. Выполнять следующие требования по антивирусному контролю:

а) Антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;

б) К использованию в структурных подразделениях Учреждения допускаются только лицензионные антивирусные средства.

в) Обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных

средств.

г) В процессе работы 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 (flesh-дисках, CD-, DVD- и т.п.). Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема.

Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель).

д) Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц;

е) Устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК должна быть выполнена антивирусная проверка;

ж) При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник колледжа должен провести внеочередной антивирусный контроль своего ПК;

з) В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов инженера по защите информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, немедленно приостановить работу и сообщить о данном факте инженеру по защите информации;
- по факту обнаружения зараженных вирусом файлов составить служебную записку инженеру по защите информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

2.1.5. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК.

2.1.6. Немедленно вызывать ответственного за защиту информации при подозрении компрометации личных паролей или их утери, а также при обнаружении:

а) Нарушений целостности пломб, наклеек на аппаратных средствах ПК или иных фактов совершения в его отсутствие попыток несанкционированного доступа к ПК;

б) Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПК;

в) Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПК, выхода из строя или неустойчивого функционирования узлов ПК или периферийных устройств (дисководов, принтера и т.п.);

г) Непредусмотренных формуляром ПК отводов кабелей и подключенных устройств

2.1.7. Хранить значение своих паролей на бумажном или другом носителе информации только в сейфе у ответственного по защите информации или руководителя

подразделения в опечатанном конверте.

2.1.8. Работникам ГБПОУ «ПГК» категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства,
- не предусмотренные формулярами ПК;
- осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию (персональные данные) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;
- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок немедленно ставить в известность инженера по защите информации.

3. Права работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет»

3.1. Работники Учреждения, пользователи ПК имеют право:

3.1.1. Давать ответственному за защиту информации предложения по совершенствованию мер информационной безопасности в подразделении;

3.1.2. Обращаться к ответственному за защиту информации для оказания необходимой технической и методологической помощи в своей работе.

3.2. Ответственный за защиту информации имеет право:

3.2.1. Требовать от работников Учреждения - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;

3.2.2. Обращаться к руководителю с требованием прекращения работы сотрудников - пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;

3.2.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

4. Ответственность

4.1. Ответственный за защиту информации обеспечивает контроль за соблюдением работниками требований настоящей Инструкции.

4.2. Работники Учреждения, пользователи ПК, имеющие доступ к информационным ресурсам локальной сети Учреждения и сети «Интернет», несут персональную ответственность за обеспечение информационной безопасности при их использовании, и

соблюдение требований настоящей Инструкции.

Разработчик:
заместителя директора по общим вопросам

_____/ Ю.Ю. Алексеев /