КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «РУБЦОВСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»

Подписано цифровой подписью: Кравцова Виктория Викторовна
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Казначейство России
Причина: Я утвердил этот документ
Дата: 22 Февраль 2023 г. 13:46:01

УТВЕРЖДАЮ:
Директор КГБПОУ
«Рубцовский медицинский колледж»
_____ В.В. Кравцова
«17» февраля 2023 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОСТУПАЮЩИХ НА ОБЪЕКТАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В КГБПОУ «РУБЦОВСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»

Введена
приказом № 66 от 17.02.2023

г. Рубцовск
2023 год

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных поступающих и иной конфиденциальной информации на объектах вычислительной техники в КГБПОУ «Рубцовский медицинский колледж» (далее - пользователь, ПЭВМ).

1.2. Пользователь должен быть допущен к обработке соответствующих категорий персональных данных поступающих и иметь навыки работы на ПЭВМ.

1.3. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных поступающих, обрабатываемых и хранимых в ПЭВМ, и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Права пользователя

Пользователь имеет право:

2.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.

2.2. Обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

3. Обязанности пользователя

Пользователь обязан:

3.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции.

3.2. При работе с персональными данными поступающих не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами.

3.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке.

3.4. После окончания обработки персональных данных поступающих в рамках выполнения одного задания произвести стирание остаточной информации с жесткого диска ПЭВМ.

3.5. Оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ.

3.6. Не допускать "загрязнение" ПЭВМ посторонними программными средствами.

3.7. Знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий.

3.8. Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

3.9. Помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе.

3.10. Знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов.

3.11. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3.12. 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.) провести внеочередной антивирусный контроль своей рабочей станции.

3.13. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4. Ограничения в деятельности пользователя

Пользователю запрещается:

4.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации.

4.2. Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности (при их наличии).

4.3. Самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ.

4.4. Самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей.

4.5. Осуществлять обработку персональных данных поступающих в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ.

4.6. Сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ.

4.7. Отключать (блокировать) средства защиты информации.

4.8. Производить какие-либо изменения в подключении и размещении технических средств.

4.9. Производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.

4.10. Оставлять бесконтрольно ПЭВМ с загруженными персональными данными поступающих, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

5. Ответственность пользователя

Пользователь несет ответственность

5.1. За надлежащее выполнение требований настоящей инструкции.

5.2. За соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов.

5.3. За сохранность и работоспособное состояние средств вычислительной техники ПЭВМ.

5.4. За сохранность и неразглашение персональных данных.