АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ УДМУРТСКОЙ РЕСПУБЛИКИ «РЕСПУБЛИКАНСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА Ф.А. ПУШИНОЙ МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ УДМУРТСКОЙ РЕСПУБЛИКИ»

УТВЕРЖДЕНО
Директором АПОУ УР «РМК МЗ УР»
Приказ № 17
от «22» 06. 2018 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ – ИНФОРМАЦИОННОЙ СИСТЕМЫ

2018

1. Общие положения

Настоящая Инструкция предназначена для сотрудников Автономного профессионального образовательного учреждения Удмуртской Республики «Республиканский медицинский колледж имени Героя Советского Союза Ф.А. Пушиной Министерства здравоохранения Удмуртской Республики» (АПОУ УР «РМК МЗ УР») и регулирует порядок допуска пользователей к работе в автоматизированной системе (АС), а также правила обращения с конфиденциальной информацией, обрабатываемой в АС.

Положения Инструкции обязательны для исполнения всеми пользователями АС.

Пользователем АС является сотрудник АПОУ УР «РМК МЗ УР», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки конфиденциальной информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным АС.

Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными правовыми документами Российской Федерации, общегосударственными и нормативно-методическими документами ФСТЭК и ФСБ России по вопросам защиты конфиденциальной информации в части его касающейся.

Положения инструкции обязательны для исполнения всеми пользователями. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

Доступ пользователей к работе в АС осуществляется в соответствии с утвержденным «Списком сотрудников, допущенных к обработке конфиденциальной информации автоматизированной системы…», с применением личного идентификатора (кода, логина) и пароля.

2. Требования по соблюдению мер безопасности при работе пользователя АС

2.1. Пользователь АС обязан:

2.1.1. Знать порядок подготовки к работе и порядок работы с программно-техническими средствами АС.

2.1.2. Строго соблюдать установленные правила обеспечения безопасности АС при работе с программными и техническими средствами, правила работы и порядок регистрации в системе, доступа к информационным ресурсам АС.

2.1.3. Знать и строго выполнять правила работы со средствами защиты информации, установленными на АС.

2.1.4. Хранить в тайне свои идентификационные данные (идентификатор (код, логин) и пароль).

2.1.5. Осуществлять вход в систему только под своими идентификационными данными.

2.1.6. лично создавать свой пароль, в присутствии администратора безопасности информации руководствуясь правилами:

а) пароль должен быть условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

б) при составлении пароля не использовать имена, даты и другие смысловые комбинации букв и цифр, бывшие в употреблении пароли;

в) вводить личный пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

г) не реже одного раза в год изменять пароль в присутствии администратора безопасности информации;

д) при компрометации пароля сообщить об этом администратору безопасности информации и произвести смену пароля немедленно.

2.1.7. Немедленно ставить в известность администратора безопасности информации при обнаружении нарушений целостности контрольных знаков на аппаратных средствах АС

или иных фактов совершения попыток несанкционированного доступа (НСД) к информации, несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АС, некорректного функционирования установленных средств защиты, непредусмотренных формуляром отводов кабелей и подключенных устройств.

2.1.8. При работе в АС выполнять только служебные задания.

2.1.9. Работать в АС только в разрешенный период времени.

2.1.10. Перед началом работы убедиться в исправности АС, отсутствии вредоносных программ.

2.1.11. При сообщениях антивирусных программ о появлении вредоносных программ немедленно прекратить работу в АС и поставить в известность администратора безопасности информации.

2.1.12. При необходимости использования съемных носителей информации (Flash-накопители) проводить проверку этих носителей на отсутствие вредоносных программ.

2.1.13. При решении задач с защищаемой информацией использовать только учтенные съемные носители информации.

2.1.14. Немедленно выполнять предписания администратора безопасности АС.

2.2. Пользователю АС запрещается:

2.2.1. Работать на АС с защищаемой информацией при обнаружении неисправностей.

2.2.2. Использовать компоненты программного и аппаратного обеспечения АС в неслужебных целях.

2.2.3. Самовольно вносить какие-либо изменения в конструкцию, размещение, конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства.

2.2.4. Осуществлять обработку конфиденциальной информации в присутствии третьих лиц, не допущенных к данной информации.

2.2.5. Записывать и хранить конфиденциальную информацию на неучтенных съемных носителях информации, в том числе для временного хранения.

2.2.6. Оставлять включенным без присмотра автоматизированное рабочее место (АРМ), не активизировав временную блокировку экрана и клавиатуры (средствами защиты от несанкционированного доступа) с помощью одновременного нажатия клавиш WinKey+L (флажок+L).

2.2.7. Оставлять без личного присмотра на рабочем месте или где бы то ни было съемные носители информации, распечатки и документы, содержащие конфиденциальную информацию.

2.2.8. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках АС (в том числе средств защиты информации), которые могут привести к несанкционированному доступу к информации. Об обнаружении такого рода ошибок – ставить в известность администратора безопасности информации.

2.2.9. Подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях.

2.2.10. Осуществлять попытки НСД к ресурсам АС и других пользователей.

2.2.11. Фиксировать и хранить свои идентификационные данные (идентификатор (код) и пароль) в доступных местах.

2.2.12. Вносить изменения в файлы, принадлежащие другим пользователям, без санкции последних или разработчика.

3. Ответственность пользователя АС

3.1. Пользователь несет персональную ответственность за ненадлежащее исполнение своих функциональных обязанностей, а также сохранность комплекта АС, съемных носителей информации и целостность установленного программного обеспечения.

3.2. Ответственность за нарушение функционирования АС, уничтожение,

под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается владельцем конфиденциальной информации (руководителем организации) по результатам служебного расследования, в соответствии с законодательством РФ.

3.3. Пользователи АС, виновные в нарушении законодательства Российской Федерации по обеспечению безопасности конфиденциальной информации, несут уголовную, административную или дисциплинарную ответственность в соответствии с действующими законами и организационно-распорядительными документами.

Разработал: программист Борисов Д.И.

С инструкцией ознакомлены:

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

_____/_____/
ФИО подпись, дата

ЭКСПЕРТИЗА ПРОВЕДЕНА
Юрисконсульт _____ \ О.Г. Кожевникова
22.06 2018 г.