УТВЕРЖДЕНО
Приказом директора
НОЧУ ДПО «ВМШ»
№ 001/3-18 от 09 января 2018 г.

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НОЧУ ДПО «ВЫСШАЯ МЕДИЦИНСКАЯ ШКОЛА»

Москва, 2018 год

1. Общие положения

1. Настоящая инструкция разработана в целях обеспечения безопасности персональных данных, при их обработке в информационной системе персональных данных при работе на автоматизированном рабочем месте (далее – АРМ) в НОЧУ ДПО «Высшая медицинская школа» (далее – ВМШ).
2. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных АРМ (далее - ИСПД), необходим для выполнения трудовых обязанностей (далее – Пользователи), допускаются к соответствующим персональным данным на основании матрицы доступа и/или Перечня лиц, допущенных к обработке персональных данных.
3. Пользователи допускаются к работе на АРМ после ознакомления с настоящей инструкцией. Настоящая инструкция доводится до Пользователей под роспись.

2. Права и обязанности Пользователей по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

2.1. Каждый сотрудник ВМШ, участвующий, в процессах автоматизированной обработки персональных данных и имеющий доступ к средствам АРМ, несет персональную ответственность за свои действия и ОБЯЗАН:

- соблюдать правила обеспечения безопасности персональных данных, в том числе при доступе к сети" Интернет";
- использовать для доступа к ИСПД собственную уникальную учетную запись (логин) и пароль. Хранить пароли в тайне;
- обеспечить сохранность используемых отчуждаемых машинных носителей информации (далее - МНИ), если таковые используются;
- соблюдать правила и меры электробезопасности;
- по окончании работы за АРМ изъять съемный МНИ, на котором хранятся персональные данные и убрать его в запираемый на ключ шкаф (сейф, ящик офисной тумбы);
- в случае возникновения нештатных ситуаций в работе ИСПД, приостановить выполняемые работы и сообщить администратору ИСПД и своему руководителю о сбое (неисправности).

2.2. Пользователю ЗАПРЕЩАЕТСЯ:

- копировать персональные данные на МНИ без согласования со своим руководителем. Согласование может производиться следующими способами: отражаться в запросах и ответах по средствам корпоративной электронной почты, письменно или определено должностными обязанностями;
- записывать на МНИ программы, файлы, а также любые другие данные, не имеющие отношения к выполняемой работе;
- выносить за пределы ВМШ (занимаемых подразделениями помещений) МНИ;
- подключать к АРМ нештатные устройства, личные или другие не относящиеся к трудовой деятельности МНИ;
- вносить изменения в конфигурацию аппаратно-программных средств АРМ;
- оставлять включенным либо незаблокированным АРМ при его покидании;
- использовать АРМ при обнаружении нарушенных пломб узлов и блоков АРМ, в случае если оно было опломбировано (опечатано) или каких-либо других видимых неисправностей (повреждений);
- разглашать сведения о применяемых средствах защиты информации, пароли, а также другие реквизиты доступа;

- передавать МНИ посторонним лицам (посторонним признается любое лицо, которое по характеру выполняемой работы или трудовых обязанностей не имеет доступа к данным сведениям).

2.3. Пользователь имеет ПРАВО:

- получать помощь по вопросам эксплуатации ИСПД от администратора ИСПД;
- подавать заявки по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ, необходимыми для автоматизации деятельности в соответствии с возложенными на него обязанностями;
- подавать администраторам ИСПД предложения по совершенствованию функционирования АРМ.

3. Требования к размещению автоматизированных рабочих мест

1.1. Размещение и монтаж устройств, предназначенных для отображения и вывода персональных данных (дисплей, принтер и т.п.) необходимо проводить с учетом максимального затруднения визуального просмотра информации посторонними лицами, а также принимать дополнительные меры, исключающие подобный просмотр (использовать шторы на окнах, жалюзи, и т.п.).

1.2. Экраны мониторов во время работы необходимо располагать так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами.

4. Режим конфиденциальности персональных данных

4.1. Пользователем, получающим доступ к персональным данным, обрабатываемым в информационной системе, должна обеспечиваться конфиденциальность таких данных.

4.2 Персональную ответственность за обеспечение режима конфиденциальности при обработке персональных данных несет исполнитель, выполняющий такую обработку.

4.3. По фактам несоблюдения условий хранения носителей персональных данных, некорректного использования средств АРМ, средств защиты информации проводятся разбирательства и составляются соответствующие заключения. Для восстановления необходимого уровня защиты информации при необходимости могут применяться дополнительные меры, направленные на повышение уровня защиты информации.

5. Ответственность

5.1 Пользователь ИСПД несет ответственность за:

- не выполнение возложенных на него обязанностей;
- не обеспечение безопасности персональных данных при их обработке в ИСПД;
- несанкционированную передачу персональных данных третьим лицам;
- нарушение работоспособности или вывод из строя системы защиты ИСПД;
- преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПД, или несанкционированный доступ к персональным данным в ИСПД.

5.2. Работники Общества, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.