федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«19» 09 2024 г.

ИНСТРУКЦИЯ

ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНА заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТА ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНА в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящая Инструкция пользователя информационных систем персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее, соответственно – ИС, Инструкция) определяет функциональные обязанности, права и ответственность пользователей ИС, в которых обрабатывается информация согласно утвержденному Перечню информации, обрабатываемой в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации).

1.2 Требования настоящей Инструкции обязательны для пользователей информационных систем ФГБОУ ВО ОмГМУ Минздрава России, в которых обрабатываются персональные данные согласно утвержденному Перечню информации.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящей Инструкции использованы ссылки на следующие документы:

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных».

3 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 В настоящей Инструкции используются следующие понятия и определения:

- Автоматизированное рабочее место (АРМ) - объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

- Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не

ограничиваясь) – несанкционированное сообщение пароля другому лицу; утеря бумажного или машинного носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется.

- Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.

- Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

- Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

- Средство защиты информации (СЗИ) – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в информационных системах.

- Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

- Утеря пароля – события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем.

- Электронная вычислительная машина (ЭВМ) – персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав информационной системы. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

4 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

4.1 Пользователь ИС обязан:

4.1.1 Знать и выполнять требования:

- настоящей инструкции;

- внутренних распорядительных документов по режиму обработки Информации, учету, хранению и пересылке носителей информации, обеспечению безопасности Информации;

- нормативных правовых актов действующего законодательства в области защиты Информации.

4.1.2 Хранить в тайне Информацию, ставшую ему известной во время работы или иным путем, и пресекать действия других лиц, которые могут привести к разглашению Информации. О таких фактах, а также о других причинах или условиях возможной утечки Информации немедленно информировать ответственного за обработку и защиту информации, администратора ИС и/или администратора информационной безопасности (далее – ИБ).

4.1.3 При определении информации, подлежащей защите, использовать Перечень информации, обрабатываемой в информационных системах персональных данных Организации, утвержденный руководителем Организации.

4.1.4 Знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с инструкциями, требованиями, регламентирующими функционирование установленных средств защиты.

4.1.5 Хранить в тайне свой пароль доступа в ИС, а также информацию о системе защиты, установленной в ИС.

4.1.6 Немедленно ставить в известность администратора ИС и/или администратора ИБ:

− в случае утери носителя с Информацией и/или при подозрении компрометации личных ключей и паролей;

− нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ИС;

− несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС.

4.1.7 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в ИС программно-аппаратных средств защиты информации ставить в известность администратора ИС и/или администратора ИБ.

4.1.8 Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций. Оперативно докладывать администратору ИС и администратору ИБ о случаях возникновения нештатных и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

4.2 Для получения консультаций по вопросам информационной безопасности и по использованию СЗИ пользователь обращается к администратору ИБ.

4.3 В случае увольнения пользователь обязан вернуть все документы и материалы, относящиеся к ИС. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ИС, полученные в течение срока работы.

4.4 Уборка помещений должна производиться под контролем пользователя, имеющего доступ в помещение и постоянно в нем работающего.

4.5 Вынос технических средств ИС, на которых проводилась обработка Информации, за пределы контролируемой зоны с целью их ремонта, замены и т.п. без согласования с администратором ИС, администратором ИБ и ответственным за обработку и защиту информации запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

4.6 Автоматизированные рабочие места, используемые для работы с Информацией, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра монитора (экрана).

4.7 Пользователю категорически запрещается:

- передавать кому бы то ни было, устно или письменно, Информацию, а также личные ключи и атрибуты доступа к ресурсам ИС, открыто осуществлять ввод персонального пароля в присутствии других лиц;

- использовать Информацию при подготовке открытых публикаций, докладов, научных работ и т.д.;

- выполнять работы с документами, содержащими Информацию, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за обработку и защиту информации;

- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие Информацию, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими Информацию;

- использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства (в том числе отключать (блокировать) СЗИ);

- осуществлять обработку Информации в присутствии посторонних (не допущенных к данной информации) лиц;

- подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;

- записывать и хранить Информацию на неучтенных носителях информации;

- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана);

- 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 – ставить в известность администратора ИС и/или администратора ИБ.

- обсуждать с посторонними лицами процедуры доступа к ИС и обрабатываемую Информацию.

4.8 Без согласования с администратором ИБ пользователю запрещается:

- производить установку программных средств;

- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение;

- изменять установленный алгоритм функционирования аттестованной ИС;

- запускать на рабочем месте файлы, не связанные с исполнением Пользователем служебных обязанностей;

- открывать общий доступ к папкам на своей рабочей станции;

- привлекать посторонних лиц для производства ремонта или настройки АРМ ИС.

5 ПРАВА ПОЛЬЗОВАТЕЛЯ

5.1 Пользователь имеет право:

5.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

5.1.2 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

6 ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

6.1 Пользователь несет ответственность за соблюдение требований настоящей Инструкции, а также нормативных документов в области защиты информации.

6.2 Пользователь несет ответственность за нарушения в работе аттестованной ИС, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей Инструкцией.

6.3 Пользователь отвечает за правильность включения и выключения АРМ ИС и всех действий при работе с ним.

6.4 За разглашение Информации, а также за нарушение порядка работы с документами или машинными носителями информации, работники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию
_____ А.С. Колчин
«12» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«09» 09 2024 г

СОГЛАСОВАНО
Начальник ОА и ИТ
_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«11» 09 2024 г.