федеральное государственное бюджетное
образовательное учреждение высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации
(ФГБОУ ВО СамГМУ Минздрава России)

ПРИКАЗ

31.03.2021 № 80

Самара

Об утверждении Инструкции
по обеспечению информационной безопасности

В целях исполнения требований Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ; Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по обеспечению информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России согласно Приложению 1 к настоящему приказу.
2. Контроль за исполнением настоящего Приказа возложить на директора Института цифрового развития Одобеску С.В.
3. Отделу документационного обеспечения довести данный Приказ до проректоров и руководителей структурных подразделений.

Ректор,
профессор РАН **А.В. Колсанов**

Приложение 1 к приказу

от «31» 03 2021 г. № 80

Инструкция
по обеспечению информационной безопасности

1. Общие положения

1.1. Инструкция по обеспечению информационной безопасности определяет основные обязанности и ответственность сотрудников ФГБОУ ВО СамГМУ Минздрава России, допущенных к обработке конфиденциальной информации и персональных данных.

1.2. Сотрудники при выполнении своих функциональных (должностных) обязанностей, обеспечивают безопасность конфиденциальной информации и персональных данных и несут персональную ответственность за соблюдение требований руководящих документов по защите информации.

1.3. В Инструкции по обеспечению информационной безопасности (далее – Инструкция) использованы следующие термины и определения:

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Несанкционированный доступ (НСД) — доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Пользователь - сотрудник ФГБОУ ВО СамГМУ Минздрава России, участвующий в рамках своих функциональных обязанностей в процессах

автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ПДн.

Средство криптографической защиты информации (СКЗИ) - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи.

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронно-вычислительная машина (ЭВМ) – комплекс технических, аппаратных и программных средств, предназначенных для автоматической обработки информации, вычислений, автоматического управления.

1.4. Настоящая Инструкция разработана в целях исполнения:

- Федерального закона Российской Федерации от 27.07.2006г. №152-ФЗ «О персональных данных»;
- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;
- Постановления Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- Приказа ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

1.5. Требования Инструкции обязательны для выполнения всеми сотрудниками ФГБОУ ВО СамГМУ Минздрава России.

2. Основные обязанности Пользователя

2.1. Выполнять общие требования по обеспечению безопасности конфиденциальной информации и персональных данных, установленные законодательством РФ, внутренними организационно-распорядительными документами ФГБОУ ВО СамГМУ Минздрава России и настоящей Инструкцией.

2.2. При работе с конфиденциальной информацией и персональными данными располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами.

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информации и персональных данных при их обработке.

2.4. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к информации, обрабатываемой в ЭВМ или без использования средств автоматизации) немедленно сообщить об этом в Центр информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru).

2.5. Не вносить самовольно какие-либо изменения в конфигурацию аппаратно-программных средств ЭВМ, не устанавливать дополнительно любые программные и аппаратные средства.

2.6. Знать штатные режимы работы программного обеспечения, основные пути проникновения и распространения компьютерных вирусов.

2.7. Помнить личные пароли и персональные идентификаторы, хранить их в тайне, не оставлять без присмотра носители, их содержащие, и хранить в запирающемся ящике стола или сейфе. С установленной периодичностью менять свой пароль (пароли).

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

2.9. Знать и строго выполнять правила работы с установленными на его ЭВМ средствами защиты информации (антивирус, средства криптографической защиты и т.п.).

2.10. Немедленно ставить в известность Центр информационной безопасности при обнаружении:

- фактов совершения в его отсутствие попыток несанкционированного доступа к закрепленной за ним защищенной ЭВМ;
- некорректного функционирования установленных на ЭВМ технических средств защиты;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ЭВМ.

2.11. По завершении работ по изменению аппаратно-программной конфигурации, закрепленной за ним ЭВМ проверять ее работоспособность.

3. Обеспечение антивирусной безопасности

3.1. Основными путями проникновения вирусов в информационно-вычислительную сеть являются: съемные носители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные ЭВМ.

3.2. В случае подозрения на наличие компьютерного вируса (сообщение антивирусной программы, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь **ОБЯЗАН:**

- прекратить (приостановить) работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Центр информационной безопасности;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости, для выполнения требований данного пункта следует обратиться за помощью к сотрудникам Центра информационной безопасности).

3.4. Пользователю **ЗАПРЕЩАЕТСЯ:**

- отключать средства антивирусной защиты информации;

- устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4. Обеспечение безопасности персональных данных

4.1. Каждый сотрудник, участвующий в процессах обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и базам данных ФГБОУ ВО СамГМУ Минздрава России является Пользователем и несет персональную ответственность за свои действия.

4.2. Допуск к обработке персональных данных осуществляется в соответствии с внутренними локально-нормативными актами в ФГБОУ ВО СамГМУ Минздрава России.

4.3. Пользователь **ОБЯЗАН**:

- знать требования руководящих документов по защите персональных данных;

- производить обработку персональных данных в строгом соответствии с законодательством РФ;

- строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами.

4.4. Пользователю **ЗАПРЕЩАЕТСЯ**:

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

- записывать и хранить персональные данные на неучтенных съемных носителях информации (жестких дисках, флэш - накопителях и т.п.), осуществлять несанкционированную распечатку персональных данных;

- оставлять включенной без присмотра свою ЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана;

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители и распечатки, содержащие персональные данные;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям безопасности персональных данных (об обнаружении такого рода ошибок необходимо ставить в известность Центр информационной безопасности).

4.5. Особенности обработки персональных данных без использования средств автоматизации.

4.5.1. Обработка персональных данных считается неавтоматизированной, если она осуществляется без использования средств вычислительной техники.

4.5.2. Персональные данные при их неавтоматизированной обработке и хранении должны обособляться от иной информации путем фиксации их на отдельных материальных носителях в специальных разделах.

4.5.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4.5.4. Для каждой категории персональных данных используется отдельный материальный носитель.

4.5.5. Хранение материальных носителей персональных данных должно осуществляться в специальных запирающихся шкафах (ящиках, сейфах и т.д.), обеспечивающих сохранность материальных носителей и исключающих несанкционированный к ним доступ.

5. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

5.1. Ресурсы сети Интернет могут использоваться для осуществления информационно-аналитической работы в интересах ФГБОУ ВО СамГМУ Минздрава России, обмена почтовыми сообщениями, ведения хозяйственной деятельности, дистанционного обслуживания, получения и распространения информации, связанной с деятельностью ФГБОУ ВО СамГМУ Минздрава России.

5.2. При осуществлении дистанционного обслуживания и электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет ФГБОУ ВО СамГМУ Минздрава России применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

5.3. При пользовании ресурсами сети Интернет Пользователю **ЗАПРЕЩАЕТСЯ:**

- использовать на рабочем месте иные каналы доступа ЭВМ к сети Интернет, кроме установленного;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения ЭВМ, подключенной к сети Интернет;
- использовать иные, кроме служебных, почтовые ящики для электронной переписки;
- открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;
- осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;
- скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п.;
- скачивать из сети Интернет нелицензионное программное обеспечение (с нарушением авторских прав) и прочие файлы (программы, игры и т.п.), в том числе посредством торрент-трекеров, а также с использованием VPN-сервисов;
- использовать сеть Интернет вне служебных задач, посещать интернет–сайты, не связанные с выполнением должностных обязанностей (развлекательные сайты, игровые сайты, сайты знакомств, сайты порнографического содержания, социальные сети, а также прочие сайты, которые не относятся к направлению деятельности сотрудника). В случае необходимости - исключительно в рамках выполнения должностных обязанностей, допускается посещение сотрудниками ФГБОУ ВО СамГМУ Минздрава России социальных сетей и прочих интернет-порталов.

6. Порядок работы с СКЗИ (включая средства ЭП)

6.1. В некоторых информационных системах для обеспечения контроля за целостностью передаваемых по технологическим каналам электронных документов, а также для подтверждения их подлинности и авторства могут использоваться СКЗИ (включая средства ЭП).

6.2. Сотруднику ФГБОУ ВО СамГМУ Минздрава России, которому в соответствии с внутренними локально-нормативными актами предоставлено право использования СКЗИ и возможности постановки на электронный документ его ЭП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭП), относящаяся к категории сведений ограниченного распространения.

6.3. Владелец ключа ЭП **ОБЯЗАН:**

- получать ключевые носители под роспись в журнале поэкземплярного учёта СКЗИ;

- хранить персональные ключевые носители в специальном месте, гарантирующем их сохранность (в запирающемся ящике стола или сейфе);

- в своей работе руководствоваться законодательством Российской Федерации в области информационной безопасности и внутренними локально-нормативными актами ФГБОУ ВО СамГМУ Минздрава России по обеспечению информационной безопасности.

6.4. Владельцу ключа ЭП **ЗАПРЕЩАЕТСЯ**:

- оставлять ключевой носитель без личного присмотра;

- передавать свой ключевой носитель другим лицам (исключение: передача ключевого носителя сотрудникам Центра информационной безопасности для осуществления настройки средств ЭП на рабочем месте Пользователя);

- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск ЭВМ), вносить изменения в файлы, находящиеся на ключевом носителе;

- использовать ключевой носитель на заведомо неисправном дисководе и/или ЭВМ;

- сообщать третьим лицам информацию о владении ключом ЭП для какого-либо технологического процесса.

6.5. Действия при компрометации ключей.

6.5.1. Если у владельца ключа ЭП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом в Центр информационной безопасности, сдать скомпрометированный ключевой носитель с пометкой в журнале поэкземплярного учёта СКЗИ о причине компрометации, написать служебную записку о факте компрометации персонального ключевого носителя.

6.5.2. В случае утери ключевого носителя владелец ключа ЭП обязан немедленно сообщить об этом в Центр информационной безопасности, написать объяснительную записку об утере ключевого носителя и принять участие в служебной проверке по факту утери ключевого носителя.

6.5.3. По решению ректора ФГБОУ ВО СамГМУ Минздрава России установленным порядком владелец ключа ЭП может получить новый комплект персональных ключевых носителей взамен скомпрометированных.

6.5.4. В случае перевода владельца ключа ЭП на другую работу, увольнения или прекращения трудовых отношений иным образом он обязан сдать (сразу по окончании последнего сеанса работы) свой ключевой носитель в Центр информационной безопасности под роспись в журнале поэкземплярного учёта СКЗИ.

7. Организация парольной защиты

7.1. В целях обеспечения информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России, для доступа в домен Active Directory и прочие автоматизированные информационные системы, сотрудникам предоставляются учетные записи, защищенные паролем. Не допускается использование учетных записей, не защищенных паролем.

Пароль для своей учетной записи Windows Пользователь получает после регистрации его учетной записи в домене Active Directory сотрудниками Управления информационных технологий. Пароль учетной записи Пользователя состоит не менее чем из 8 символов, а в числе символов пароля обязательно используются буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

7.2. Запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке ЭВМ) для входа в иные автоматизированные информационные системы.

7.3. Длина пароля, вводимого Пользователем в автоматизированных информационных системах, также должна быть не менее 8 символов, а в числе символов пароля необходимо использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

7.4. Пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, USER, PASSWORD и т.п.).

7.5. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

7.6. Пользователь обязан хранить в тайне свои личные пароли.

7.7. Пользователю запрещается передавать любые пароли и доступы третьим лицам, ставшие ему известными в рамках выполнения должностных обязанностей.

8. Ответственность Пользователей

8.1. Сотрудники ФГБОУ ВО СамГМУ Минздрава России несут ответственность за нарушения требований законодательства Российской Федерации, а также локальных нормативных актов по обеспечению информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России.