Инструкция
пользователей средств криптографической защиты информации

1. Общие положения

1.1. Инструкция пользователей средств криптографической защиты информации определяет основные обязанности и ответственность сотрудников ФГБОУ ВО СамГМУ Минздрава России, допущенных к обработке конфиденциальной информации (в том числе персональных данных) с использованием средств криптографической защиты информации (далее – СКЗИ);

1.2. Доступ пользователей к работе с СКЗИ осуществляется в соответствии с внутренними локально-нормативными актами в ФГБОУ ВО СамГМУ Минздрава России» и действующим законодательством РФ;

1.3. При необходимости использования ключа электронной подписи, для выполнения должностных обязанностей сотрудника, не являющегося владельцем ключа ЭП, оформляется доверенность на право использования ключа электронной подписи, согласно приложению №5 Приказа «Об утверждении состава и содержания организационных мер, необходимых для выполнения требований по обеспечению безопасности персональных данных при их обработке в информационных системах с использованием средств криптографической защиты информации в ФГБОУ ВО СамГМУ Минздрава России»;

1.4. Пользователи при выполнении своих функциональных (должностных) обязанностей, выполняют требования, предъявляемые к работе с использованием средств криптографической защиты информации (далее - СКЗИ), обеспечивают безопасность конфиденциальной информации и несут персональную ответственность за соблюдение требований руководящих документов по защите информации;

1.5. Под работами с использованием СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия, согласно технической документации на СКЗИ;

1.6. В ФГБОУ ВО СамГМУ Минздрава России для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации используется СКЗИ, позволяющее реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные ключевые носители многократного (долговременного) использования со строгой двухфакторной аутентификацией и защищенного хранения ключей электронной подписи, имеющих сертификат соответствия ФСБ;

1.7. В Инструкции пользователей средств криптографической защиты информации (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;

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

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

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;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

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.

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

Пользователи СКЗИ – сотрудники ФГБОУ ВО СамГМУ Минздрава России, непосредственно допущенные к работе с СКЗИ.

Средства криптографической защиты информации (СКЗИ) – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

1.8. 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;
- Федерального закона от 06.04.2011г. №63-ФЗ «Об электронной подписи»;
- 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»

1.9. Требования Инструкции обязательны для выполнения всеми Пользователями СКЗИ ФГБОУ ВО СамГМУ Минздрава России.

2. Порядок работы со средствами криптографической защиты информации

2.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. В ФГБОУ ВО СамГМУ Минздрава России обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации;

2.2. Для получения доступа пользователям к работе с СКЗИ, сотруднику необходимо пройти инструктаж по информационной безопасности, ознакомиться с инструкцией пользователя СКЗИ и действующим законодательством Российской Федерации в сфере защиты персональных данных и конфиденциальной информации с использованием СКЗИ, с отметкой в «Журнале ознакомления сотрудников с инструкцией пользователя, допущенного к обработке конфиденциальной информации с использованием СКЗИ»;

2.3. Пользователь получает у ответственного сотрудника ЦИБ, на основании служебной записки от руководителя структурного подразделения на имя Директора института цифрового развития учетную запись для работы со специализированным программным обеспечением, с помощью которого будет подключен USB порт с защищенным носителем, на котором записан сертификат ключа проверки электронной подписи, с отметкой в Журнале выдачи парольной документации»;

2.4. В ФГБОУ ВО СамГМУ Минздрава России для организации и обеспечения безопасности хранения и эксплуатации электронной подписи, используются ключевые носители с двухфакторной аутентификацией. Защищенный носитель обеспечивает безопасное хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта. Пользователь при получении доступа к работе с электронной подписью, расписывается в «Журнале поэкземплярного учета СКЗИ» за эксплуатацию ключевого носителя и использование электронной подписи, оформляется акт установки СКЗИ;

2.5. Для начала работы с применением электронной подписи, пользователю необходимо запустить специализированное программное обеспечение, активировать определенный USB порт, зарегистрированный Ответственным сотрудником ЦИБ на его имя и ввести данные учетной записи, выданные Центром информационной безопасности. Персональные

идентификаторы (парольные карточки) держать в тайне, не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

2.6. По окончанию работы с применением электронной подписи, необходимо деактивировать USB порт и выйти из специализированного программного обеспечения.

3. Обязанности пользователей СКЗИ

3.1. Пользователи СКЗИ обязаны:

- осуществлять эксплуатацию СКЗИ в соответствии с документацией на СКЗИ, а также в соответствии с иными нормативными правовыми актами, регулирующими отношения в соответствующей области;

- не разглашать конфиденциальную информацию, к которой они, допущены, в том числе сведения о криптоключах;

- выполнять общие требования, предъявляемые к работе с использованием средств криптографической защиты информации и обеспечивать безопасность конфиденциальной информации, в соответствии с установленным законодательством РФ, внутренними организационно-распорядительными документами ФГБОУ ВО СамГМУ Минздрава России и настоящей Инструкцией;

- соблюдать правила работы с СКЗИ и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информации при ее обработке;

- обеспечивать сохранность вверенной ключевой документации на них;

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

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- хранить ключевую информацию в специальном месте, гарантирующем их сохранность (в запирающемся ящике стола или сейфе).

3.2. Пользователю СКЗИ запрещается:

- разглашать содержимое ключевых носителей лицам, к ним не допущенным. Пользователь несет персональную ответственность за эксплуатацию ключевых носителей;

- 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;

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

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

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

3.3. Действия при компрометации сертификат ключей проверки электронной подписи.

3.3.1. Если у Пользователя СКЗИ появилось подозрение, что его ключевая информация попала или могла попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу, незамедлительно сообщить об этом сотрудникам Центра информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru), написать служебную записку о факте компрометации персонального ключевого носителя на имя Директора Института цифрового развития.

3.3.2. В случае утери парольной карточки Пользователь СКЗИ обязан сообщить об этом в Центр информационной безопасности, написать объяснительную записку на имя Директора Института цифрового развития об утере.

4. Порядок прекращения работы пользователей с СКЗИ

4.1. В случае прекращения работы Пользователей с СКЗИ, необходимо оформить служебную записку на имя директора Института Цифрового развития для уничтожения средств криптографической защиты и оформления акта уничтожения СКЗИ;

4.2. В случае прекращения работы Пользователей с электронной подписью необходимо оформить служебную записку на имя директора Института Цифрового развития для аннулирования сертификата ключей проверки электронной подписи, прекращения доступа к информационным системам и

удаления учетной записи. После уничтожения ключевой информации оформляется акт уничтожения и делается соответствующая запись в «Журнале поэкземплярного учета СКЗИ». Пользователю необходимо сдать парольную карточку в Центр информационной безопасности под подпись в «Журнале выдачи парольной документации»;

5. Ответственность Пользователей

5.1. За нарушение установленных требований по эксплуатации криптосредств пользователь СКЗИ несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.