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

ПРИКАЗ

27.12.2021 № 396

Самара

Об утверждении Инструкции
по организации криптографической защиты информации

В целях исполнения требований Федерального закона «О персональных данных» от 27.07.2006 N 152-ФЗ; Приказа ФСБ России от 10 июля 2014 г. № 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. № 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»

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по организации криптографической защиты информации 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, руководителей структурных подразделений и заведующих кафедр.

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

Приложение 1 к приказу
от «27» 12 2021 г. № 296

ИНСТРУКЦИЯ
по организации криптографической защиты информации в ФГБОУ ВО СамГМУ Минздрава России

1. Термины и определения

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

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 многократного использования - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации), сертифицированный ФСБ.

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.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Ответственный за организацию работ по криптографической защите информации (Ответственный) – сотрудник ФГБОУ ВО СамГМУ Минздрава России, отвечающий за реализацию мероприятий, связанных с обеспечением в ФГБОУ ВО СамГМУ Минздрава России безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем ФГБОУ ВО СамГМУ Минздрава России в рамках исполнения должностных обязанностей;

Пользователи СКЗИ - сотрудники ФГБОУ ВО СамГМУ Минздрава России, непосредственно допущенные к работе с СКЗИ;

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

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;

Доверенность на право использование ключа электронной подписи - письменное уполномочие, выдаваемое одним физическим или юридическим лицом (доверителем) другому лицу (поверенному) для использования ключа электронной подписи владельца от его имени;

Управляемый USB over IP концентратор (USB концентратор) - предназначен для подключения USB электронных ключей защиты, например, серии ruToken и других аналогов, ключей для программных продуктов, к компьютерной сети и позволяет авторизованным пользователям, допущенным к обработке конфиденциальной информации (в том числе персональных данных) с использованием средств криптографической защиты информации сети удаленно подключать USB устройства к своему компьютеру, ноутбуку, пользоваться ими, и удаленно управлять подключенными USB-устройствами;

Система контроля и управления доступом, СКУД (англ. Physical Access Control System) — совокупность программно-аппаратных технических средств контроля и средств управления, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода».

2. Общие положения

2.1. Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к организации работ со средствами криптографической защиты информации (далее - СКЗИ) в Федеральном государственном бюджетном образовательном учреждении высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ВО СамГМУ Минздрава России), которые осуществляют работы с применением СКЗИ, для защиты информации

ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну;

2.2. Под работами с применением СКЗИ в настоящей Инструкции понимаются формирование запроса на изготовление сертификата; установка программ для генерации электронной подписи; установка средств криптографической защиты, предназначенные для обеспечения целостности программных приложений при помощи методов шифрования; учет выданных защищенных носителей СКЗИ; настройка рабочего места пользователя для работы с СКЗИ; настройка защищенного подключения к информационным системам; подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия, согласно технической документации на СКЗИ; аннулирование сертификата электронной подписи, уничтожение СКЗИ на рабочем месте пользователя, а также уничтожение криптоключей с защищенного ключевого носителя многократного использования;

2.3. Под организацией криптографической защиты информации в ФГБОУ ВО СамГМУ Минздрава России понимается проведение мероприятий по обеспечению безопасности создания, хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа;

2.4. В ФГБОУ ВО СамГМУ Минздрава России для организации и обеспечения безопасности создания, 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 использования со строгой двухфакторной аутентификацией и защищенного хранения ключей электронной подписи, имеющих сертификат соответствия ФСБ. Защищенный носитель обеспечивает безопасное хранение ключей электронной подписи во встроенной защищенной памяти без возможности их экспорта;

2.5. Для обеспечения безопасности хранения ключевых носителей используется Управляемый USB over IP концентратор (далее Концентратор). Возможность управления USB портами позволяет отключать и включать USB устройства физически. Концентратор поддерживает управление из внутренней локальной сети;

2.6. Концентраторы установлены в серверных помещениях по адресу: ул. Чапаевская д. 89, кабинет №8 и проспект Карла Маркса д. 165 «б» Доступ в серверное помещение осуществляется на основании перечня лиц, утвержденного приказом № 63п от 27.04.2021 «Об утверждении перечня лиц, имеющих доступ в помещения, содержащие серверное и телекоммуникационное оборудование».

Вход в кабинет и вход в серверное помещение оснащен системой контроля управления доступом (СКУД), препятствующее возможности неконтролируемого проникновения или пребывания в помещении;

2.7. Ответственные за организацию работ по криптографической защите информации назначаются приказом ректора ФГБОУ ВО СамГМУ Минздрава России.

2.8. Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66, а также «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», утвержденных приказом ФСБ от 10.07.2014 № 378.

3. Порядок получения доступа пользователей к работе с СКЗИ

3.1. Для получения доступа пользователям к работе с СКЗИ, сотруднику необходимо пройти инструктаж по информационной безопасности, ознакомиться с инструкцией пользователя СКЗИ;

3.2. Доступ пользователей к работе с СКЗИ осуществляется в соответствии с внутренними локально-нормативными актами в ФГБОУ ВО СамГМУ Минздрава России;

3.3. Для возможности работы пользователя со средствами криптографической защиты информации, ответственный сотрудник центра информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России создает учетную запись и разрешает доступ к определенному USB порту, на котором находится Ключевой носитель многократного использования, с записанным на нем сертификатом ключа проверки электронной подписи;

3.4. Для корректной эксплуатации электронной подписи, ответственный сотрудник центра информационной безопасности в ФГБОУ ВО СамГМУ Минздрава России устанавливает специализированное программное

обеспечение на рабочее место Пользователя. Пользователю выдается парольная карточка с логином и паролем для подключения к USB порту, с отметкой в «Журнале выдачи парольной документации»;

3.5. При необходимости использования ключа электронной подписи, для выполнения должностных обязанностей сотрудника, не являющегося владельцем ключа ЭП, оформляется доверенность на право использования, согласно утвержденной типовой форме.

4. Порядок прекращения доступа пользователей к работе с СКЗИ

В случае изменения должностных обязанностей, увольнения или прекращения использования СКЗИ, сотрудник уведомляет Центр информационной безопасности.

4.1. В случае прекращения доступа пользователей к работе с СКЗИ, ответственный сотрудник ЦИБ производит уничтожение средств криптографической защиты стандартными средствами удаления программ Windows, с отметкой в «Журнале поэкземплярного учёта СКЗИ» и оформлением акта уничтожения;

4.2. В случае прекращения работы пользователя с электронной подписью, Ответственный сотрудник ЦИБ оформляет заявление на аннулирование сертификата, отправляет в удостоверяющий центр, который выдавал данную электронную подпись и закрывает доступ в информационных системах, в которых данная электронная подпись использовалась. Ответственный сотрудник ЦИБ удаляет учетную запись и форматирует ключевой носитель многократного использования. После уничтожения ключевой информации оформляется акт уничтожения и делается соответствующая запись в «Журнале поэкземплярного учета СКЗИ».

Специализированное программное обеспечение деинсталлируется с рабочего места пользователя стандартными средствами удаления программ Windows. Парольная карточка подлежит уничтожению.

5. Работа с СКЗИ

5.1. При установке СКЗИ в помещениях, в которых будет осуществляться эксплуатация средств криптографической защиты информации, необходимо исключить возможность доступа посторонних лиц к указанным средствам. Техническое обслуживание и смена криптоключей в присутствии посторонних лиц запрещено;

5.2. Ключевые носители многократного использования подключены в Концентратор, предназначенный для подключения USB ключей электронной защиты и позволяет авторизованным пользователям, допущенным к обработке конфиденциальной информации (в том числе персональных данных) с использованием средств криптографической защиты информации подключить USB устройство к своему компьютеру, тем самым обеспечивая условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации;

5.3. Концентратор обеспечивает двухступенчатую защиту USB устройств и авторизацию для подключения USB устройств по логину, паролю. В электронном журнале Концентратора хранится вся информация о подключениях и отключениях как USB входов (портов), так и любого из USB устройств, а также попытках не правильного ввода пароля;

5.4. Каждый ключевой носитель должен быть зарегистрирован в Журнале поэкземплярного учёта СКЗИ;

5.5. При обнаружении на рабочей станции с установленным СКЗИ вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности и дальнейшему удалению вирусных программ.

6. Действия в случае компрометации ключей

6.1. О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать в Центр информационной безопасности (телефон: 8 (846) 374-00-66 (вн.: 4729, 4732, 4745), эл. почта: cib@samsmu.ru).

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;
2) утрата иных носителей ключа с последующим обнаружением;
3) возникновение подозрений на утечку ключевой информации или ее искажение;
4) доступ посторонних лиц к ключевой информации;
5) другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ;

6.2. В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных

сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации;

6.3. Выявление причин возникновения инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет Центр информационной безопасности ФГБОУ ВО СамГМУ Минздрава России. О результатах своей работы и выявленных причинах возникновения инцидента Центр информационной безопасности информирует руководителя Института цифрового развития и соответствующего подразделение университета.

7. Требования к помещениям, в которых производятся работы с СКЗИ

Осуществление безопасности и ограничение неконтролируемого доступа в помещения для хранения и использования СКЗИ осуществляется средствами специального программно-аппаратного комплекса и силами подразделения общей безопасности университета.

Ответственные за организацию работ по криптографической защите информации хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение или сейфах (хранилищах).

Доступ лиц в защищаемые помещения должен быть ограничен в соответствии исходя из утвержденных списков сотрудников подразделений, имеющих право доступа в данное помещение.

Помещения должны быть оборудованы прочными входными дверями, препятствующими свободному доступу. Окна помещений должны быть оборудованы средствами, препятствующими неконтролируемому проникновению в помещения. В помещении должна быть установлена система охранной и пожарной сигнализации. В случае отсутствия охранной сигнализации, помещение должно опечатываться, а ключ сдаваться на охрану.

8. Ответственность лиц, допущенных к работе с СКЗИ

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

За утерю, компрометацию ключевой информации и ключевых носителей многократного использования пользователь несет персональную ответственность.