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

# ПО ПОРЯДКУ ОБРАЩЕНИЯ С СЕРТИФИЦИРОВАННЫМИ СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ПРЕДНАЗНАЧЕННЫМИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, ОБРАБАТЫВАЕМОЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ, И КРИПТОКЛЮЧАМИ К НИМ

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 по порядку обращения с сертифицированными средствами криптографической защиты информации (далее – СКЗИ), предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – Информация), обрабатываемой в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – ИСПДн), и криптографическим ключами (далее - криптоключ) к ним регламентирует порядок обращения с криптосредствами в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты Информации.

1.2 Требования настоящей Инструкции обязательны для сотрудников ФГБОУ ВО ОмГМУ Минздрава России, обрабатывающих информацию в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России.

## 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 закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

## 3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Под криптосредством в настоящей Инструкции понимается шифровальное средство, предназначенное для защиты информации.

3.2 К криптосредствам относятся:

3.2.1 Средства шифрования – 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.

3.2.2 Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

3.2.3 Средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи.

3.2.4 Средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

3.2.5 Средства изготовления ключевых документов (независимо от вида носителя ключевой информации).

3.2.6 Ключевые документы (независимо от вида носителя ключевой информации).

3.3 В настоящей Инструкции используются следующие понятия и определения:

3.3.1 Доступ к информации – возможность получения информации и ее использования.

3.3.2 Закрытый ключ – криптоключ, который хранится пользователем системы в тайне.

3.3.3 Ключевой документ – физический носитель определенной структуры, содержащий криптоключи.

3.3.4 Компрометация криптоключа – утрата доверия к тому, что используемые криптоключи обеспечивают безопасность информации.

3.3.5 Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

3.3.6 Криптоключ – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

3.3.7 Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

3.3.8 Модель угроз – перечень возможных угроз.

3.3.9 Пользователь криптосредства – лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

3.3.10 Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3.4 Для обеспечения безопасности Информации при её обработке в ИСПДн должны использоваться сертифицированные в системе сертификации Федеральной службы безопасности Российской Федерации криптосредства

(имеющие положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

3.5 Класс криптосредства определяется в соответствии с Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 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».

## 4 ОРГАНИЗАЦИОННАЯ СТРУКТУРА

4.1 Безопасность обработки Информации в ИСПДн с использованием криптосредств организует и обеспечивает Ответственный за эксплуатацию СКЗИ в ИСПДн.

## 5 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЙ КРИПТОСРЕДСТВ

5.1 Пользователи криптосредств допускаются к работе с ними только после получения заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и ознакомления под роспись с настоящей Инструкцией, другими документами, регламентирующими организацию и обеспечение безопасности Информации при ее обработке в ИСПДн.

5.2 При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

5.3 Пользователи криптосредств обязаны:

5.3.1 Не нарушать конфиденциальность закрытых ключей.

5.3.2 Не допускать снятие копий с ключевых документов, содержащих закрытые ключи.

5.3.3 Не допускать вывод закрытых ключей на дисплей (монитор) автоматизированного рабочего места (далее – АРМ) или принтер.

5.3.4 Не допускать записи на ключевой документ посторонней информации.

5.3.5 Не допускать установки ключевых документов на другие АРМ.

5.3.6 Обеспечить конфиденциальность информации о криптосредствах, других мерах защиты.

5.3.7 Точно соблюдать требования к обеспечению безопасности Информации, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

5.3.8 Хранить ключевые документы к криптосредствам в защищаемых хранилищах.

5.3.9 Сдавать ключевые документы к криптосредствам при увольнении или отстранении от исполнения обязанностей.

5.3.10 Своевременно выявлять и сообщать Ответственному за эксплуатацию СКЗИ в ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации) о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним.

5.3.11 Немедленно уведомлять Ответственного за эксплуатацию СКЗИ в Организации и принимать меры по предупреждению нарушения конфиденциальности Информации при утрате или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей, удостоверений, пропусков, при других фактах, которые могут привести к компрометации закрытых ключей, снижению уровня защищенности обрабатываемой Информации.

# 6 УЧЕТ КЛЮЧЕВЫХ ДОКУМЕНТОВ

6.1 Ключевые документы подлежат поэкземплярному учету. Единицей поэкземплярного учета ключевых документов считается ключевой носитель информации.

6.2 Все экземпляры ключевых документов выдаются пользователям криптосредств под роспись в соответствующем журнале поэкземплярного учета.

6.3 Передача ключевых документов допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись в соответствующем Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов. Аналогичная передача между пользователями криптосредств осуществляется с письменного разрешения Ответственного за эксплуатацию СКЗИ.

6.4 Для исключения компрометации ключевых документов на период отсутствия пользователя и в нерабочее время, ключевые документы убираются в защищенные хранилища, ящики или шкафы) индивидуального пользования, которые, в свою очередь, закрываются на ключ и опечатываются.

6.5 Учет эксплуатационной и технической документации к криптосредствам:

6.5.1 Эксплуатационная и техническая документация к криптосредствам подлежит поэкземплярному учету.

6.5.2 Все экземпляры эксплуатационной и технической документации к криптосредствам выдаются пользователям криптосредств под роспись.

6.5.3 Передача эксплуатационной и технической документации к криптосредствам допускается только между пользователями криптосредств и Ответственным за эксплуатацию СКЗИ под роспись. Аналогичная передача между пользователями криптосредств осуществляется с санкции Ответственного за эксплуатацию СКЗИ.

6.6 Плановая смена ключевых документов:

6.6.1 Заказ на изготовление очередных ключевых документов, их изготовление и получение пользователем производится заблаговременно для своевременной замены действующих ключевых документов.

6.7 Внеплановая смена ключевых документов:

6.7.1 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

6.8 Уничтожение ключевых документов:

6.8.1 Ключевые документы с неиспользованными или выведенными из действия криптоключами (исходной ключевой информацией) возвращаются Ответственному за эксплуатацию СКЗИ, или по его указанию уничтожаются на месте пользователями криптосредств.

6.8.2 Уничтожение ключевых документов производится путем стирания (разрушения) криптоключей без повреждения ключевого документа.

6.8.3 Бумажные и прочие сгораемые ключевые документы уничтожаются путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

6.8.4 Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы уничтожаются не позднее 10 (десяти) суток после вывода их из действия (окончания срока действия).

6.8.5 Пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) ключевые документы. После уничтожения пользователи криптосредств уведомляют об этом Ответственного за эксплуатацию СКЗИ.

6.9 Уничтожение эксплуатационной и технической документации к криптосредствам:

4.9.1 Эксплуатационная и техническая документация к криптосредствам уничтожается путем сжигания или с помощью любых бумагорезательных машин с составлением соответствующего акта.

## 7 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ КРИПТОСРЕДСТВ

7.1 Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

7.2 На время отсутствия пользователей криптосредства, а также другое оборудование, функционирующее с криптосредствами, при наличии технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

## 8 ОПЕЧАТЫВАНИЕ АППАРАТНЫХ СРЕДСТВ

8.1 Системные блоки АРМ, на которых установлены криптосредства, должны оборудоваться средствами контроля за их вскрытием (опечатываются, опломбируются). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

## 9 ПОРЯДОК ДОСТУПА К ХРАНИЛИЩАМ

9.1 Эксплуатация хранилищ:

9.1.1 Пользователи криптосредств хранят эксплуатационную и техническую документацию к криптосредствам, ключевые документы в

хранилищах (ящиках, шкафах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

9.1.2 Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

9.2 При необходимости доступа к содержимому хранилища работник, ответственный за данное хранилище, проверяет целостность хранилища, открывает механический замок хранилища с использованием ключа.

9.3 По окончании работы работник закрывает и опечатывает хранилище, за которое он ответственен.

9.4 Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за данные хранилища.

## 10 КОНТРОЛЬ БЕЗОПАСНОСТИ КРИПТОСРЕДСТВ

10.1 Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на Ответственного за эксплуатацию СКЗИ в пределах его полномочий.

## 11 ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ

11.1 Пользователи криптосредств несут персональную ответственность за сохранность полученных криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов, за соблюдение положений настоящей Инструкции.

11.2 Ответственный за эксплуатацию СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности обработки Информации с использованием криптосредств

лицензионным требованиям и условиям эксплуатационной и технической документации к криптосредствам, а также настоящей Инструкции.

# 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
«12» 09 2024 г.