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
«10» 09 2024 г.

ИНСТРУКЦИЯ

ПО ВОССТАНОВЛЕНИЮ СВЯЗИ В СЛУЧАЕ КОМПРОМЕТАЦИИ ДЕЙСТВУЮЩИХ КЛЮЧЕЙ К КРИПТОСРЕДСТВАМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ 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 Целью Инструкции является предотвращение ключевой информации и незаконного использования криптографического ключа, в том числе электронной подписи, в ФГБОУ ВО ОмГМУ Минздрава России.

1.2 Действие настоящей Инструкции распространяется на пользователей (далее - Пользователи) и оператора (далее - Оператор) автоматизированных рабочих мест (далее - АРМ) ФГБОУ ВО ОмГМУ Минздрава России.

1.3 Настоящая Инструкция является локальным нормативным актом Университета, выполнение требований которого обязательно для всех структурных подразделений Университета, должностных лиц и сотрудников, участвующих в работе с АРМ.

2 НОРМАТИВНЫЕ ССЫЛКИ

2.1 Настоящая Инструкция разработана с учетом следующих положений, законодательных и нормативно-правовых актов:

– Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;

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

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) носителей ключевой информации (далее – НКИ), в том числе – с последующим их обнаружением;

- увольнение (переназначение) работников, имевших доступ к ключевой информации;

- передача секретных ключей по линии связи в открытом виде;

- нарушение правил хранения криптоключей;

- вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

- отрицательный результат при проверке наложенной электронной подписи;

- несанкционированное или безучётное копирование ключевой информации;

- все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

3.2 События 1-5 пункта 1 должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.

3.3 При наступлении любого из перечисленных выше событий владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному за эксплуатацию криптографических средств защиты информации лично, по телефону, электронной почте или другим доступным способом. В любом случае владелец ключа обязан убедиться, что его сообщение получено и прочтено адресатом.

3.4 При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей в течение трёх рабочих дней.

3.5 Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает новые ключи.

ЛИСТ СОГЛАСОВАНИЯ

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

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«11» 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.