Государственное казенное учреждение здравоохранения
Детский санаторий «ТОПОЛЁК»
Министерства Здравоохранения Краснодарского края

УТВЕРЖДАЮ
Главный врач
ГКУЗ «Детский санаторий «Тополек»
_____ / М. А. Мугу /
«24» 12 2021 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

1. Общие положения

Настоящая Инструкция пользователя криптосредств (далее–Инструкция) ГКУЗ «Детский санаторий «Тополек» определяет права и обязанности пользователей криптосредств, порядок обращения с криптосредствами, а также определяет порядок восстановления связи в случае компрометации действующих ключей к криптосредствам.

Пользователем криптосредств является сотрудник ГКУЗ «Детский санаторий «Тополек», включенный в перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных.

Пользователь криптосредств должен знать законодательные и иные нормативные правовые акты Российской Федерации в сфере обработки персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

В своей деятельности, связанной с обработкой персональных данных, пользователь криптосредств руководствуется настоящей Инструкцией.

Пользователи криптосредств несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту криптосредств от несанкционированного использования.

2. Обязанности и права пользователя криптосредств

Пользователь криптосредств обязан:

– соблюдать требования по обеспечению безопасности функционирования криптосредств;

– обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

– сдать администратору безопасности носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

– сдать администратору безопасности НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

– немедленно уведомлять руководителя структурного подразделения и администратора безопасности о компрометации НКИ, о фактах утраты или недостачи криптосредств;

– в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования криптосредств.

Пользователю криптосредств запрещается:

– осуществлять несанкционированное и неучтенное копирование ключевых данных;

– хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать НКИ каким бы то ни было лицам, кроме администратора безопасности;

– во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– хранить на НКИ какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются криптосредства, личные технические средства, позволяющие осуществлять копирование ключевой информации;

– использовать НКИ, выведенные из действия.

Пользователь имеет право:

– вносить предложения руководству ГКУЗ «Детский санаторий «Тополек», и администратору безопасности по вопросам использования криптосредств;

– повышать уровень квалификации по использованию криптосредств.

3. Порядок обращения с криптосредствами

Служебные помещения, в которых размещаются криптосредства, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (личными ящиками с замком), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, и сдаются под охрану.

Для хранения НКИ пользователь криптосредств должен быть обеспечен личным ящиком, запираемым на замок. В случае отсутствия индивидуального ящика по окончании рабочего дня пользователь криптосредств обязан сдавать НКИ администратору безопасности.

Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей криптосредств должны храниться в сейфе руководителя структурного подразделения или администратора безопасности. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

К эксплуатации криптосредств допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным криптосредством.

Все программное обеспечение ПЭВМ, предназначенной для установки криптосредств, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую криптосредства, не допускается.

4. Восстановление связи в случае компрометации действующих ключей к криптосредствам

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

– утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– увольнение (переназначение) сотрудников, имевших доступ к НКИ;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения НКИ;

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

– ошибки при совершении криптографических операций;

– несанкционированное или неучтенное копирование ключевой информации;

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

При наступлении любого из перечисленных выше событий пользователь криптосредств или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору безопасности лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь криптосредств или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

При подтверждении факта компрометации действующих ключей пользователь криптосредств обязан обеспечить немедленное изъятие из обращения

скомпрометированных криптографических ключей и сдачу администратору безопасности в течение 1 рабочего дня.

Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь криптосредств получает у администратора безопасности новые ключи.