Инструкция пользователя криптосредств
ТГПУ им. Л.Н. Толстого

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя криптосредств ТГПУ им. Л.Н. Толстого (далее – Инструкция) определяет права и обязанности пользователей криптосредств, порядок обращения с криптосредствами, а также определяет порядок восстановления связи в случае компрометации действующих ключей к криптосредствам.

1.2. Пользователем криптосредств является сотрудник ТГПУ им. Л.Н. Толстого (далее – Университет), включенный в перечень сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, утвержденный локальным актом Университета.

1.3. Непосредственно к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с криптосредствами осуществляют сотрудники соответствующего органа криптографической защиты. Заключение о допуске или не допуске к работе с криптосредствами должно быть отмечено в Журнале обучения пользователей правилам работы с криптосредствами.

1.4. Пользователь криптосредств должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

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

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

2. ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ КРИПТОСРЕДСТВ

2.1. Пользователь криптосредств обязан:

– соблюдать требования по обеспечению безопасности функционирования криптосредств;

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

– сдать ответственному пользователю криптосредств ТГПУ им. Л.Н. Толстого (далее – Ответственный) носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

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

– немедленно уведомлять руководителя структурного подразделения или Ответственного 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.

2.2. Пользователю криптосредств запрещается:

– осуществлять несанкционированное и безучётное копирование ключевых данных;

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

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

– 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.

2.3. Пользователь имеет право:

– вносить предложения руководству Университета по вопросам использования криптосредств;

– повышать уровень квалификации по использованию криптосредств.

3. ПОРЯДОК ОБРАЩЕНИЯ С КРИПТОСРЕДСТВАМИ

3.1. Монтаж и установка криптосредства осуществляются органом криптографической защиты.

3.2. 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 (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.

3.3. Для хранения НКИ пользователь криптосредств должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня пользователь криптосредств обязан сдавать НКИ Ответственному под подпись в Журнале учета и выдачи носителей с ключевой информацией.

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

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

3.6. Все программное обеспечение ПЭВМ, предназначенное 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

4.1. 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 безучётное 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).

4.2. 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) Ответственному 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.

4.3. При подтверждении факта компрометации действующих ключей пользователь криптосредств обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь криптосредств получает у Ответственных новых ключей.