Государственное профессиональное образовательное учреждение
Тульской области «Алексинский химико-технологический техникум»

СОГЛАСОВАНО	УТВЕРЖДАЮ
на Совете техникума	Директор ГПОУ ТО «АХТТ»
протокол № 4 от 15.02.2022г.	Приказ № 7 - О от 15.02.2022г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00 bd 35 07 6f f6 ed 19 23
Владелец: Анохина Ольга Николаевна
Действителен с 22.03.2022 по 21.03.2027

ИНСТРУКЦИЯ
администратора, ответственного за эксплуатацию средств криптографической защиты информации в ГПОУ ТО «АХТТ»

1.1. Настоящая инструкция регламентирует обязанности и права ответственного пользователя средств криптографической защиты информации в работе по обеспечению безопасности средств криптографической защиты информации (далее СКЗИ) и эксплуатации СКЗИ в ГПОУ ТО «АХТТ».

1.2. Администратор, ответственный за эксплуатацию СКЗИ назначается из числа пользователей СКЗИ приказом директора и должен обладать необходимым уровнем квалификации по работе с СКЗИ. При необходимости (отсутствие необходимой квалификации у сотрудников) функция ответственного пользователя СКЗИ частично может быть возложена на основании договора на стороннюю организацию – лицензиата ФСБ России.

1.3. Администратор, ответственный за эксплуатацию СКЗИ обязан:

- проводить обучение лиц, использующих СКЗИ, правилам работы с ними;
- выполнять проверку готовности пользователей СКЗИ к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);
- вести поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;
- вести учет лиц, непосредственно допущенных к работе с СКЗИ (пользователей СКЗИ) и хранимых у них СКЗИ, эксплуатационной и технической документации к ним;
- осуществлять контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к СКЗИ;
- осуществлять подачу заявок на изготовление ключевых документов или исходной ключевой информации в удостоверяющий центр;
- проводить разбирательство и составление заключений по фактам нарушения условий хранения носителей конфиденциальной информации, использования СКЗИ, которые могут привести к нарушению или к снижению уровня защищенности информации.
- принимать меры для минимизации возможных последствий при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, сейфов

(металлических шкафов), личных печатей и т. п.;

- немедленно сообщать о фактах компрометации, утраты криптосредств, эксплуатационной документации и ключевых документов к ним, ключей от помещений, хранилищ, личных номерных печатей, нарушения печатей (наклеек), которыми опечатан системный блок ПЭВМ с установленными криптосредством, компрометации ключевой информации и о других фактах, которые могут привести к разглашению защищаемой информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации администратору, ответственному за эксплуатацию СКЗИ и в удостоверяющий центр, изготовивший криптографические ключи.
- проводить разбирательства по фактам нарушения условий хранения и использования СКЗИ;
- организовывать хранение криптоключей других пользователей СКЗИ в случае необходимости. Хранение должно осуществляться только в опечатанном виде;
- не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- не допускать снятия копий с ключевых документов, вывода ключевых документов на дисплей (монитор) ПЭВМ или принтер, записи на ключевой носитель посторонней информации, установки ключевых документов в другие ПЭВМ;
- соблюдать требования по обеспечению безопасности конфиденциальной информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним;
- немедленно уведомлять директора ГПОУ ТО «АХТТ» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к компрометации защищаемой конфиденциальной информации.

1.4. Администратор, ответственный за эксплуатацию СКЗИ имеет право:

- приостановить работу пользователя СКЗИ при возникновении подозрения на факт компрометации ключевой информации данного пользователя СКЗИ;
- приостановить работу пользователя и эксплуатацию ПЭВМ в случае возникновения факта нарушения эксплуатации СКЗИ;

– сообщить директору ГПОУ ТО «АХТТ» о факте компрометации ключевой информации, утраты СКЗИ, эксплуатационной и технической документации к ним, ключей от хранилищ, ключей от кабинетов, нарушения пломб, которыми опечатаны ПЭВМ с установленным СКЗИ и о других фактах, которые могут привести к разглашению информации конфиденциального характера с последующей инициацией расследования.

Ответственность

Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или дисциплинарной ответственности.

Утверждаю
Директор ГПОУ ТО «АХТТ»
_____О.Н.Анохина
29.12.2018 г.

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации в ГПОУ ТО «АХТТ»

Обеспечение безопасности применения криптографических средств (криптосредств) в ГПОУ ТО «АХТТ» организовано и проводится в соответствии с приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Порядок предоставления доступа к средствам криптографической защиты информации

Доступ к средствам криптографической защиты информации (СКЗИ) предоставляется только после соответствующего обучения пользователей работе с СКЗИ. Обучение работе заключается в ознакомлении с руководством пользователя СКЗИ и настоящей инструкцией.

Обязанности пользователя СКЗИ

- не разглашать информацию, к которой пользователи СКЗИ допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- не допускать снятия копий с ключевых документов, вывода ключевых документов на дисплей (монитор) ПЭВМ или принтер, записи на ключевой носитель посторонней информации, установки ключевых документов в другие ПЭВМ;
- соблюдать требования по обеспечению безопасности конфиденциальной информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним;
- немедленно уведомлять администратора, ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к защищаемой конфиденциальной информации;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы администратору, ответственному за эксплуатацию СКЗИ под запись в журналах учета при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

Администратор, ответственный за эксплуатацию СКЗИ обязан сдать директору ГПОУ ТО «АХТТ» находящиеся в его пользовании и относящиеся к деятельности техникума СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, журналы учета при увольнении (отстранении от исполнения обязанностей), расторжении (прекращении действия) договорных отношений.

Передача и хранение СКЗИ

СКЗИ, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются.

Хранение ключевых документов пользователями СКЗИ должно осуществляться в надежно запираемых шкафах (ящики, сейфы) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи СКЗИ обязаны сообщать администратору, ответственному за эксплуатацию СКЗИ.

События, квалифицируемые как явная компрометация ключей

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение работников, имевших доступ к ключевой информации;
- нарушение печати на сейфе с ключевыми носителями;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

К событиям, квалифицируемым как подозрение наличия факта компрометации криптографического ключа, требующим проведения расследования и принятия решения на предмет явной компрометации, относится возникновение подозрений в утечке информации в системе защищенной связи.

Ответственность

Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или дисциплинарной ответственности.