

**ПОЛОЖЕНИЕ**  
**по обеспечению безопасности информации с помощью**  
**средств криптографической защиты информации на объектах**  
**информатизации НГТУ**

**1. Общие положения**

Настоящее Положение по обеспечению безопасности информации с помощью средств криптографической защиты информации на объектах информатизации НГТУ (далее — Положение) разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Составы 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»;

К шифровальным (криптографическим) средствам защиты информации (далее — СКЗИ), включая документацию на эти средства, относятся:

- 1) средства шифрования — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;
- 2) средства электронной подписи — шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;
- 3) средства кодирования — средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

4) средства для изготовления ключевых документов — аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящих в состав этих шифровальных (криптографических) средств;

5) ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

6) средства имитозащиты — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

## **2. Организация и обеспечение функционирования СКЗИ**

Организация и обеспечение функционирования СКЗИ представляет следующий комплекс мероприятий:

- установка и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам;
- проверка готовности СКЗИ к использованию с составлением заключений о возможности их эксплуатации;
- разработка мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;
- создание исходной ключевой информации, создание из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;
- обучение работников, использующих СКЗИ, работе с ними;
- поэземплярный учет используемых СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- проведение служебной проверки и составление заключений по фактам нарушения условий криптографической защиты информации.

### **2.1. Структура ответственных лиц**

Структуру ответственных лиц по направлению организации и обеспечения криптографической защиты информации в НГТУ образуют:

- ответственный пользователь СКЗИ;
- пользователи СКЗИ.

Лица, осуществляющие работу с СКЗИ, должны быть ознакомлены с документами, регламентирующими организацию и обеспечение криптографической защитой информации, под подпись и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством РФ.

Контроль за организацией и обеспечением функционирования СКЗИ возлагается на ответственного пользователя СКЗИ в пределах его служебных полномочий.

Контроль за организацией, обеспечением функционирования и безопасности СКЗИ осуществляется в соответствии с законодательством РФ.

### **2.1.1. Ответственный пользователь СКЗИ**

Ответственный пользователь СКЗИ назначается в соответствии с документом, утвержденным ректором НГТУ.

На ответственного пользователя СКЗИ возлагаются функции органа криптографической защиты.

Организация и обеспечение функционирования СКЗИ возлагается на ответственного пользователя СКЗИ.

Перед допуском к работе ответственный пользователь СКЗИ обязан ознакомиться с нормативными правовыми документами, регулирующими организацию и обеспечение криптографической защиты информации, с настоящим Положением и локальными актами, определяющими порядок защиты информации с помощью СКЗИ в НГТУ.

Ответственный пользователь СКЗИ осуществляет:

- организацию безопасности обработки информации с использованием СКЗИ;
- обеспечение функционирования и безопасности СКЗИ;
- организацию и обеспечение эксплуатации СКЗИ;
- разработку и осуществление мероприятий по организации и обеспечению безопасности хранения, обработки и передачи информации с использованием СКЗИ;
- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей, ключевых документов;
- учет работников, являющихся пользователями СКЗИ;
- прием, выдачу, уничтожение ключевой информации, эксплуатационной и технической документации к ним;
- организацию плановой смены ключей, а также смены ключей в случае их компрометации;
- безопасное хранение резервных копий сертификатов и закрытых ключей пользователей, которые могут использоваться впоследствии только для перезаписи на новый ключевой носитель пользователя в случае неисправности старого.
- контроль за соблюдением пользователями СКЗИ условий использования СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- участие в комиссиях по расследованию фактов нарушений условий использования СКЗИ, которые могут привести (привели) к снижению уровня характеристик безопасности информации;
- участие в комиссиях по плановой проверке правильности учета и соблюдения правил обращения с СКЗИ и их хранением;
- уведомление руководства о фактах нарушения порядка эксплуатации СКЗИ.

Ответственный пользователь СКЗИ несет ответственность за соответствие проводимых им мероприятий по организации и обеспечению безопасности хранения, обработки с

использованием СКЗИ требованиям законодательства, эксплуатационной и технической документации к СКЗИ, настоящим Положением.

Ответственный пользователь СКЗИ обязан ознакомиться с требованиями настоящего Положения под подпись.

### **2.1.2. Пользователь СКЗИ**

Пользователи допускаются к работе с СКЗИ по распоряжению ректора НГТУ.

Пользователь СКЗИ обязан:

- не разглашать информацию, к которой он допущен, в том числе сведения об СКЗИ, ключевых документах к ним и других мерах защиты и не передавать сами носители лицам, к ним не допущенным;
- соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- обеспечивать безопасность хранения, обработки информации, ключевых документов к СКЗИ и парольной информации к ним;
- осуществлять эксплуатацию СКЗИ в соответствии с требованиями эксплуатационной документации;
- не допускать снятие копий с ключевых документов;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевой информации на объекты информатизации (далее — ОИ);
- хранить носители ключей, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;
- сообщать о ставших известными попытках получения сведений об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;
- немедленно уведомлять ответственного пользователя СКЗИ, руководство о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее — Помещения), хранилищ, личных печатей, предназначенных для опечатывания Помещений (хранилищ), и о других фактах, которые могут привести к снижению уровня характеристик безопасности информации;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- использовать СКЗИ только для целей, предусмотренных должностной инструкцией.

Все пользователи СКЗИ несут ответственность за действия с СКЗИ, нарушающие требования настоящего Положения и других организационных и правовых документов, определяющих меры по защите информации с помощью СКЗИ.

Пользователи СКЗИ обязаны ознакомиться с требованиями настоящего Положения под подпись.

## **2.2. Требования к обеспечению безопасности хранения и обработки информации с использованием СКЗИ**

Безопасность хранения и обработки с использованием СКЗИ информации достигается:

- соблюдением пользователями СКЗИ конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документов к ним;
- точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;
- надежным хранением эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации;
- своевременным выявлением работниками попыток получения сведений о защищаемой информации, об используемых СКЗИ или ключевых документах к ним лицами, не обладающими правом доступа к таким сведениям;
- немедленным принятием мер по предупреждению разглашения защищаемой информации, а также возможной ее утечки при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от Помещений, хранилищ, сейфов, личных печатей и т.п.

Техническое обслуживание СКЗИ и смена криптоключей осуществляется в отсутствие лиц, не допущенных к работе с данными СКЗИ

### **2.2.1. Требования к помещениям и хранилищам**

Размещение, специальное оборудование, охрана и организация режима в Помещениях, должны обеспечивать сохранность защищаемой информации, СКЗИ и ключевых документов к ним.

Помещения должны удовлетворять требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Размещение, специальное оборудование, охрана и организация режима в Помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Должен быть обеспечен режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих права доступа в Помещения, который достигается в том числе путем:

- оснащением Помещений входными дверьми с замками;
- обеспечением постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода;
- утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;
- утверждения перечня лиц, имеющих право доступа в Помещения.

Помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Помещений в нерабочее время. Для предотвращения просмотра Помещений извне их окна должны быть защищены.

Ответственный пользователь СКЗИ осуществляет учет хранилищ, ключей от них в журнале учета хранилищ и ключей от них, форма которого приведена в Приложении № 1 к настоящему Положению.

Помещения подлежат опечатыванию или должны быть оснащены охранной сигнализацией, связанной со службой охраны здания.

Личные печати работников, предназначенные для опечатывания хранилищ, должны находиться у пользователей СКЗИ, ответственных за эти хранилища. Выдачу личных печатей работникам осуществляет ответственный пользователь СКЗИ с отметкой в Журнале учета личных печатей, предназначенных для опечатывания хранилищ, форма которого приведена в Приложении № 2 к настоящему Положению.

По окончании рабочего дня хранилища должны быть закрыты и опечатаны, о чем производится запись в Журнале опечатывания (вскрытия) хранилищ, форма которого приведена в Приложении № 3 к настоящему Положению.

При утрате ключа от хранилища или от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь СКЗИ.

В обычных условиях опечатанные хранилища могут быть вскрыты только пользователями СКЗИ, имеющими право доступа к ним, или ответственным пользователем СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилище о случившемся должно быть немедленно сообщено ответственному пользователю СКЗИ или руководству. Прибывший ответственный пользователь СКЗИ должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации и к замене скомпрометированных криптоключей.

### **2.2.2. Требования к СКЗИ**

Для криптографической защиты конфиденциальной информации должны применяться только сертифицированные по требованиям Федеральной службы безопасности РФ СКЗИ.

### **2.2.3. Требования к объектам информатизации, на которые устанавливаются СКЗИ**

Технические характеристики и состав ПО должны соответствовать требованиям, предъявляемым эксплуатационной и технической документацией к СКЗИ.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ данные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

### **2.2.4. Требования к криптоключам**

По истечению срока действия, криптоключ подлежит смене в порядке, предусмотренном эксплуатационной и технической документацией к СКЗИ или регламентом удостоверяющего центра, от которого получен ключевой документ.

## **2.3. Эксплуатация СКЗИ**

### **2.3.1. Регистрация и учет СКЗИ, ключевых документов и эксплуатационной и технической документации к ним**

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярому учету в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, форма которого приведена в Приложении № 4 к настоящему Положению.

Единицей поэкземплярного учета криптоключей является ключевой носитель. Если один и тот же ключевой носитель многократно используется для записи криптоключей, то каждый раз он подлежит отдельной регистрации.

Журналы ведутся ответственным пользователем СКЗИ. С учетом особенности эксплуатации отдельных СКЗИ допускается добавление в журналы полей или их перестановка. При ведении журналов не допускается применение корректирующих средств.

Журналы ведутся до полного использования, после чего закрываются. Все числящиеся на момент закрытия журнала СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы берутся на учет во вновь заведенном журнале поэкземплярного учета.

Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в журнале поэкземплярного учета ключевых носителей, ключевых документов.

### **2.3.2. Выдача СКЗИ, ключевых документов, эксплуатационной и технической документации к ним**

Выдача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляется ответственным пользователем СКЗИ под подпись в соответствующем журнале учета.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается между пользователем СКЗИ и ответственным пользователем СКЗИ под подпись в соответствующем журнале поэкземплярного учета. Передача СКЗИ между пользователями запрещена.

Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно.

Изготовление (заказ) ключевой информации осуществляется на основе решения руководителя.

Ключи записываются только на машинные носители информации, учтенные в порядке, определенном в п.2.3.1.

Указание о вводе в действие очередных ключевых документов может быть дано ответственным пользователем СКЗИ только после поступления от всех заинтересованных пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю СКЗИ или по его указанию должны быть уничтожены на месте.

### **2.3.3. Установка СКЗИ**

Перед установкой СКЗИ проводится обследование Помещения на соответствие требованиям, предъявляемым к Помещениям технической и эксплуатационной документацией к СКЗИ.

Допуск пользователей СКЗИ к работе с СКЗИ осуществляется после прохождения ими инструктажа по работе с СКЗИ. Инструктаж проводит ответственный пользователь СКЗИ. Инструктаж включает ознакомление с требованиями нормативных правовых актов и локальных актов НГТУ, регламентирующих организацию криптографической защиты информации и предусматривающих порядок обращения с СКЗИ, эксплуатационной и технической документацией к СКЗИ, и настоящим Положением. О факте проведения инструктажа делается отметка в Журнале учёта и инструктажа пользователей средств криптографической защиты информации, форма которого приведена в Приложении № 5 к настоящему Положению.

Установка и настройка СКЗИ осуществляются системным администратором в соответствии с процедурой, предусмотренной эксплуатационной и технической документацией к СКЗИ.

По завершении установки составляется Акт ввода в эксплуатацию СКЗИ, форма которого приведена в Приложении № 6. Акт ввода в эксплуатацию СКЗИ подлежит хранению у ответственного пользователя СКЗИ. Сведения о пользователе СКЗИ заносятся в Журнале учета пользователей средств криптографической защиты информации.

### **2.3.4. Порядок эксплуатации СКЗИ**

Эксплуатация СКЗИ осуществляется в соответствии с технической и эксплуатационной документацией к нему.

Эксплуатационная и техническая документация для СКЗИ, ключевые документы хранятся в хранилищах в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Отдельно от ключей подлежат хранению резервные ключевые документы, предназначенные для применения в случае компрометации действующих.

Перед началом работы с ОИ контролируется наличие и целостность номерной наклейки (пломбы), которой опечатан системный блок. После входа в операционную систему контролируется запуск антивирусного программного обеспечения и актуальность антивирусных баз.

Во время эксплуатации СКЗИ осуществляется контроль целостности установленного СКЗИ с помощью механизма самого СКЗИ или с помощью программного обеспечения контроля целостности.

Во время эксплуатации СКЗИ пользователям СКЗИ запрещается:

- изменять настройки СКЗИ;
- осуществлять вскрытие системного блока ОИ с установленными СКЗИ;
- оставлять без контроля ключевые носители, а также ОИ с установленными СКЗИ при включенном питании и загруженном программном обеспечении СКЗИ;
- вносить какие-либо несанкционированные изменения в СКЗИ;
- выводить на монитор защищаемую информацию (в т.ч. информацию ключевых документов), обрабатываемых с использованием СКЗИ в присутствии лиц, не имеющих к такой информации права доступа;
- применять скомпрометированные ключи и пароли;

- осуществлять несанкционированное копирование ключевой информации;
- вставлять ключевой носитель в устройства, штатный порядок работы которых не предусматривает использование ключевого носителя.

### **2.3.5. Контроль за соблюдением правил эксплуатации СКЗИ**

Ежегодно комиссией, в которую входят работники НГТУ, проводятся плановые проверки:

- наличия, правильности учета и соблюдения правил обращения и хранения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- выявление установочных носителей СКЗИ, ключевых документов, экземпляров технической и эксплуатационной документации подлежащих уничтожению;
- соблюдения правил обращения, предусмотренных настоящим Положением пользователями СКЗИ.

Внеплановые проверки проводятся комиссией, в которую входят работники НГТУ, в случаях нарушения установленного в НГТУ порядка криптографической защиты информации.

Состав комиссии определяет ректор НГТУ.

По завершении проверки комиссией составляется Акт проверки, в котором указывается состав комиссии, основание проверки, проверочные мероприятия, недостатки, выявленные в ходе проверки, и рекомендации по их устранению, рекомендации по совершенствованию криптографической системы защиты информации. Акт проверки утверждается ректором НГТУ.

### **2.3.6. Порядок проведения служебной проверки по фактам нарушения правил эксплуатации СКЗИ**

В случае возникновения конфликтной ситуации и по фактам (подозрению) нарушения конфиденциальности информации, защищаемой с помощью СКЗИ, проводится служебная проверка.

Основаниями проведения служебной проверки являются докладная записка работника, информационные письма (претензии) сторонних организаций, непосредственное обнаружение руководством факта (подозрения) нарушения конфиденциальности защищаемой информации, безопасность которой обеспечивается применением СКЗИ.

Служебная проверка назначается руководителем не позднее трех дней с момента поступления информации о факте нарушения конфиденциальности защищаемой информации.

В ходе служебной проверки устанавливается:

- действительно ли имело место нарушение конфиденциальности защищаемой информации;
- лица виновные в нарушении, их вина и ее степень;
- причины и условия, способствовавшие нарушению;
- характер и размер причиненного ущерба;
- предложения по недопущению подобных случаев впредь;
- иные сведения, имеющие отношения к нарушению.

Служебная проверка осуществляется комиссией, состав которой утверждается ректором НГТУ. Состав комиссии должен представлять не менее трех человек.

Срок завершения служебной проверки указывается в документе о проведении служебной проверки. Если срок не указан, то служебная проверка завершается не позднее, чем через месяц со дня обнаружения нарушения.

На первом этапе служебной проверки комиссия устанавливает суть нарушения, его последствия, предполагает, что могло послужить причиной.

На втором этапе собирается вся необходимая интересующая информация о нарушении, объяснения с участников.

На третьем этапе на основании собранных в ходе первых двух этапов служебной проверки материалов оформляется письменное заключение (акт). В нем указываются основание и сроки проведения служебной проверки, состав комиссии, значимые обстоятельства, установленные в ходе служебной проверки. Акт подписывается всеми членами комиссии и направляется руководителю.

### **2.3.7. Порядок действий при компрометации ключа**

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Различают явную и неявную компрометацию ключей. Явной называется компрометация, факт которой становится известным на отрезке установленного времени действия данного ключа. Неявной называется компрометация ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа.

События, квалифицируемые как явная компрометация:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации.

К событиям, связанным с неявной компрометацией ключей и требующим их рассмотрения в каждом конкретном случае, относятся случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями, содержащими ключевую информацию, в том числе случаи, когда носитель (token и др.) вышел из строя и доказательно не опровергнуто, что данный факт произошел в результате несанкционированного доступа злоумышленника.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их чтения, копирования.

При наступлении компрометации ключа или подозрения в компрометации ключа пользователь СКЗИ обязан немедленно прекратить работу с СКЗИ и сообщить ответственному пользователю СКЗИ о факте компрометации (в том числе и предполагаемом).

По факту компрометации ключей (в том числе предполагаемому) проводится служебная проверка в соответствии с п. 2.3.6 настоящего Положения.

По завершению проверки оформляется письменное заключение (акт) о проведении служебной проверки.

Скомпрометированные ключи по завершению проверки подлежат уничтожению в порядке, определенном настоящим Положением.

Взамен скомпрометированных ключей ответственный пользователь СКЗИ производит замену ключей в порядке, предусмотренном технической и эксплуатационной документацией, или в соответствии с Регламентом удостоверяющего центра.

### **2.3.8. Деинсталляция средств криптографической защиты информации**

Деинсталляция СКЗИ с рабочих мест пользователей СКЗИ осуществляется при наступлении в том числе следующих условий: увольнение работника, отстранение от исполнения

обязанностей, отзыв доверенности и т.п., а также окончание срока действия лицензии или сертификата ключа ЭП (в случае, если не планируется продление срока действия сертификата на следующий период).

Деинсталляция СКЗИ осуществляется системным администратором в соответствии с процедурой, предусмотренной эксплуатационной и технической документацией к СКЗИ, с составлением Акта вывода из эксплуатации СКЗИ, форма которого приведена в Приложении № 6 к настоящему Положению. Акт вывода из эксплуатации СКЗИ подлежит хранению у ответственного пользователя СКЗИ.

Одновременно с деинсталляцией СКЗИ уничтожаются криптоключи, если не планируется их дальнейшее использование. В противном случае они возвращаются ответственному пользователю СКЗИ с отметкой в соответствующем журнале.

О факте деинсталляции СКЗИ делается отметка в журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

### **2.3.9. Уничтожение СКЗИ**

Основаниями для уничтожения инсталляционных носителей СКЗИ, эксплуатационной и технической документации к ним, ключевых документов являются утвержденные акты на списание и уничтожение материальных носителей и подлежащие хранению у ответственного пользователя СКЗИ.

Основанием для уничтожения ключей является истечение срока их действия, вывод из эксплуатации СКЗИ, увольнение работника, снятие с работника обязанностей, связанных с использованием СКЗИ и т.д.

Неиспользуемые или выведенные из действия ключевые носители подлежат возвращению ответственному пользователю СКЗИ, либо криптоключи, записанные на них, подлежат уничтожению на месте.

Уничтожение криптоключей производится путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей без повреждения ключевого носителя.

Криптоключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (компакт-дисков, токенов и т.п.). Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующему СКЗИ, а также указаниями организаций, производивших запись криптоключей.

Ключевые носители уничтожаются путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановление ключевой информации. Непосредственные действия по стиранию криптоключей, а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируется эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей.

Ключевые документы должны уничтожаться в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее десяти дней после вывода их из действия.

В эти же сроки с отметкой в соответствующем журнале подлежит уничтожению ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация,

соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключках.

Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под подпись в соответствующем журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо ответственным пользователем СКЗИ с указанием отметки о факте уничтожения в соответствующем журнале поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом ответственного пользователя СКЗИ.

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

Определенные к уничтожению СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятими из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к ним процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования должна быть надежно удалена.

Факт уничтожения носителей эксплуатационной и технической документации, установочных носителей СКЗИ, криптоключей, путем уничтожения ключевых носителей фиксируется в Акте уничтожения, форма которого приведена в Приложении № 7 к настоящему Положению. Акт уничтожения подлежит хранению у ответственного пользователя СКЗИ. О факте уничтожения делаются отметки в соответствующем журнале поэкземплярного учета.

# Журнал

## учёта хранилищ и ключей от них

Номер журнала \_\_\_\_\_

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал завершён « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал составлен на \_\_\_\_\_ листах



## Журнал

### учёта личных печатей, предназначенных для опечатывания хранилищ

Номер журнала \_\_\_\_\_

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал завершён « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал составлен на \_\_\_\_\_ листах

№ п/п	Отгиск (изображение) печати	Должность, ФИО получателя печати	Дата получения печати	Подпись работника в получении печати	Дата возврата печати	Подпись работника о возврате печати
<b>1</b>						
	Предприятие – изготовитель, номер и дата документа					
<b>2</b>						
	Предприятие – изготовитель, номер и дата документа					

## Журнал

### учёта опечатывания (вскрытия) хранилищ

Номер журнала \_\_\_\_\_

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/ \_\_\_\_\_/  
*подпись* *фамилия, имя, отчество*

Журнал завершён « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/ \_\_\_\_\_/  
*подпись* *фамилия, имя, отчество*

Журнал составлен на \_\_\_\_\_ листах



## Журнал

### поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Номер журнала \_\_\_\_\_

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал завершен « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/

*подпись*

*фамилия, имя, отчество*

Журнал составлен на \_\_\_\_\_ листах





# Журнал

## учёта и инструктажа пользователей СКЗИ

Номер журнала \_\_\_\_\_

Журнал начат « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
*подпись* *фамилия, имя, отчество*

Журнал завершён « \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

Должность \_\_\_\_\_

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
*подпись* *фамилия, имя, отчество*

Журнал составлен на \_\_\_\_\_ листах



**ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева»**

**АКТ  
ввода СКЗИ в эксплуатацию**

№ \_\_\_\_\_

от \_\_\_\_ . \_\_\_\_ . 202\_\_ г

Настоящий акт составлен о том, что

\_\_\_\_\_  
*(должность, место работы, Ф.И.О.)*

ввел(-а) в эксплуатацию СКЗИ:

\_\_\_\_\_  
*(модель СКЗИ и серийный (лицензионный) номер экземпляра)*

объект информационной инфраструктуры, на котором будет функционировать СКЗИ:

\_\_\_\_\_  
*(объект информационной инфраструктуры)*

\_\_\_\_\_  
*(подпись)*

\_\_\_\_\_  
*(Ф.И.О)*

**ФГБОУ ВО «Нижегородский государственный технический университет им. Р.Е. Алексеева»**

**АКТ  
вывода СКЗИ из эксплуатации**

№ \_\_\_\_\_

от \_\_\_\_ . \_\_\_\_ . 202\_\_ г

Настоящий акт составлен о том, что

\_\_\_\_\_  
*(должность, место работы, Ф.И.О.)*

вывел(-а) из эксплуатации СКЗИ:

\_\_\_\_\_  
*(модель СКЗИ и серийный (лицензионный) номер экземпляра)*

объект информационной инфраструктуры, на котором ранее функционировало СКЗИ:

\_\_\_\_\_  
*(объект информационной инфраструктуры)*

\_\_\_\_\_  
*(подпись)*

\_\_\_\_\_  
*(Ф.И.О)*

**АКТ**  
**уничтожения средств криптографической защиты информации**

Комиссия в составе председателя:

\_\_\_\_\_ (Должность, Фамилия И.О.)

и членов:

\_\_\_\_\_ (Должность, Фамилия И.О.)

\_\_\_\_\_ (Должность, Фамилия И.О.)

составила настоящий акт о том, что в

\_\_\_\_\_ **НГТУ** \_\_\_\_\_

(Наименование организации)

было произведено уничтожение следующих средств криптографической защиты информации:

Т а б л и ц а

№ п/п	Наименование	Заводской / регистрационный номер

Носитель информации, содержащий дистрибутив СКЗИ, эксплуатационная и техническая документация к СКЗИ уничтожены путем физического разрушения носителей.

Ключевые документы № \_\_\_\_\_, находящиеся на ключевом носителе № \_\_\_\_\_ уничтожены (при наличии ключевых документов).

Заключение комиссии: Восстановление и использование перечисленных в Таблице программных средств невозможно.

Председатель: / \_\_\_\_\_ / \_\_\_\_\_  
(подпись) (Фамилия И.О.)

Члены комиссии: / \_\_\_\_\_ / \_\_\_\_\_  
(подпись) (Фамилия И.О.)

/ \_\_\_\_\_ / \_\_\_\_\_  
(подпись) (Фамилия И.О.)