Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Самарский государственный экономический университет»

ПРИКАЗ

Самара

№ 333 - ОВ «25» мая 2020 года

Об обращении со средствами криптографической защиты информации

В целях исполнения требований приказа Федеральной службы безопасности России от 10 июля 2014 г. № 378 «Состав и содержание 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», приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации 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»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Инструкцию ответственного за обеспечение функционирования и безопасности криптографических средств;

1.2. Инструкцию по обращению со средствами криптографической защиты информации;

1.3. Инструкцию пользователей средств криптографической защиты информации;

1.4. Форму Журнала проведения инструктажа пользователям средств криптографической защиты информации;

1.5. Форму Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный экономический университет»;

1.6. Форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов;

2. Начальнику отдела информационной безопасности ознакомить ответственного за обеспечение функционирования и безопасности криптографических средств (далее – Ответственный за СКЗИ) под роспись с Инструкцией ответственного за обеспечение функционирования и безопасности криптографических средств, в своей в своей деятельности Ответственный за СКЗИ должен руководствоваться данной инструкцией.

3. Ответственному за СКЗИ провести инструктаж пользователей средств криптографической защиты информации (далее – Пользователи СКЗИ), факт проведения инструктажа и ознакомления Пользователей СКЗИ с Инструкцией по обращению со средствами криптографической защиты информации и Инструкцией пользователей средств криптографической защиты информации зафиксировать в Журнале проведения инструктажа пользователям средств криптографической защиты информации.

4. Пользователям, которым необходимо получить доступ к работе со средствами криптографической защиты информации, пройти инструктаж по правилам работы со средствами криптографической защиты информации.

5. Считать утратившим силу Приказ от 19.03.2018 года № 178-ОВ;

6. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор С.И. Ашмарина

Разработчик:
Начальник ОИБ
Черемисин А.А.
(846)933-86-96 (вн. 528)

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

Инструкция ответственного за обеспечение функционирования и безопасности криптографических средств

1. Термины и определения

АС – автоматизированная система.

ИОД (информация ограниченного доступа) – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптоключ (криптографический ключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Ответственный за СКЗИ – ответственный за обеспечение функционирования и безопасности криптографических средств.

ПДн – персональные данные.

Пользователи СКЗИ – работники Университета, непосредственно допущенные к работе со СКЗИ.

СКЗИ (средство криптографической защиты информации) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

2. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, Ответственных за СКЗИ.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152.

Ответственный за СКЗИ назначается приказом ректора Университета из числа Пользователей СКЗИ, или возлагается на структурное подразделение или должностное лицо (работника), ответственных за защиту информации (обеспечение безопасности информации, в том числе ПДн).

СКЗИ должны использоваться для защиты ИОД (включая ПДн), не содержащей сведений, составляющих государственную тайну.

3. Порядок получения допуска пользователей к работе со СКЗИ

Для работы пользователей со СКЗИ необходимо реализовать ряд

мероприятий:

– пользователи, которым необходимо получить доступ к работе со СКЗИ, должны быть проинструктированы и обучены правилам работы со СКЗИ;

– учёт лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения защиты информации в АС, осуществлять в Перечне Пользователей СКЗИ, утвержденного приказом ректора Университета;

– контроль над реализацией данных мероприятий возлагается на Ответственного за СКЗИ.

4. Обязанности Ответственного за СКЗИ

При решении всех вопросов, связанных с обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ ИОД, Ответственный за СКЗИ должен руководствоваться Инструкцией по обращению со СКЗИ.

На Ответственного за СКЗИ возлагается проведение следующих мероприятий:

– ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– ведение Журнала проведения инструктажа пользователям СКЗИ;

– принятие СКЗИ, эксплуатационной и технической документации к ним, ключевых документов от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– осуществление периодической проверки журнала учета СКЗИ, перечня Пользователей СКЗИ и иных документов.

Ответственный за СКЗИ обязан:

– не разглашать ИОД, к которой он допущен, в том числе сведения о криптоключах;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности ИОД;

– контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

– немедленно уведомлять ректора Университета о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению ИОД, а также о причинах и условиях возможной утечки такой информации;

– незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

– не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

5. Права Ответственного за СКЗИ

В рамках исполнения возложенных на него обязанностей Ответственный за СКЗИ имеет право:

– требовать от Пользователей СКЗИ соблюдения положений Инструкции по обращению со СКЗИ и Инструкции Пользователя СКЗИ;

– проводить тестирование пользователей на знание правил работы со СКЗИ и оформлять Заключение о допуске пользователя к самостоятельной работе со СКЗИ;

– обращаться к ректору Университета с требованием прекращения работы Пользователя СКЗИ при невыполнении им установленных требований по обращению со СКЗИ;

– инициировать проведение служебных расследований по фактам нарушения в Университете порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ ИОД.

6. Порядок передачи обязанностей при смене Ответственного за СКЗИ

При смене Ответственного за СКЗИ должны быть внесены соответствующие изменения в приказ «О назначении ответственных за защиту информации».

Вновь назначенный Ответственный за СКЗИ должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

Лист ознакомления
с Инструкцией ответственного за обеспечение функционирования и безопасности криптографических средств
(утверждена приказом № 333-ОВ от «25» мая 2020 г.)

Ф.И.О.	Должность	Дата	Подпись
Мишуров Дмитрий Александрович	Ведущий инженер отдела технического администрирования УИСиТ	25.05 2020	

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации

1. Термины и определения

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

ИОД (информация ограниченного доступа) – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Криптоключ (криптографический ключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Ответственный за СКЗИ – ответственный за обеспечение функционирования и

безопасности криптографических средств.

ПДн – персональные данные.

Пользователи СКЗИ – работники Университета, непосредственно допущенные к работе со СКЗИ.

СКЗИ (средство криптографической защиты информации) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

2. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со СКЗИ.

Настоящая Инструкция в своем составе, терминах и определениях основывается на Положении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005), утвержденного приказом Федеральной службы безопасности России от 9 февраля 2005 г. № 66; «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», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152.

Под обращением со СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ ИОД, в том числе ПДн.

СКЗИ должны использоваться для защиты ИОД (включая ПДн), не

содержащей сведений, составляющих государственную тайну.

3. Работа со СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего со СКЗИ, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия Пользователей СКЗИ указанное оборудование при наличии технической возможности должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае в Университете должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется после получения ключевых носителей создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же как оригиналы.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между Пользователями СКЗИ под роспись в соответствующих журналах поэкземплярного учета.

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена, организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

4. Действия в случае компрометации ключей

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием ИОД Пользователи СКЗИ обязаны сообщать Ответственному за СКЗИ.

К компрометации ключей относятся следующие события:

– утрата носителей ключа;

– утрата иных носителей ключа с последующим обнаружением;

– увольнение сотрудников, имевших доступ к ключевой информации;

– возникновение подозрений на утечку информации или ее искажение;

– нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

– утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

– утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

– доступ посторонних лиц к ключевой информации;

– другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации ИОД, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет в Университете Ответственный за СКЗИ.

5. Обязанности и ответственность лиц, допущенных к работе со СКЗИ

Лица, допущенные к работе со СКЗИ, обязаны:

– не разглашать ИОД, к которой они допущены;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности ИОД;

– сообщать Ответственному за СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– не вводить номера лицензий на СКЗИ уже вводимые на других АРМ;

– немедленно уведомлять Ответственного за 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 разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Лица, допущенные к работе со СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность ИОД, которая стала им известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе со СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция Ответственного за СКЗИ, Инструкция Пользователя СКЗИ), а также за разглашение ИОД, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

ИНСТРУКЦИЯ
пользователей средств криптографической защиты информации

1. Термины и определения

АС – автоматизированная система.

ИОД (информация ограниченного доступа) – информация, доступ к которой ограничен федеральными законами.

Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

криптоключ (криптографический ключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Ответственный за СКЗИ – ответственный за обеспечение функционирования и безопасности криптографических средств.

ПДн – персональные данные.

Пользователи СКЗИ – работники Университета, непосредственно допущенные к работе со СКЗИ.

СКЗИ (средство криптографической защиты информации) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Университет – федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет».

ЭП (электронная подпись) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Общие положения

Настоящая Инструкция разработана в целях регламентации действий Пользователей СКЗИ.

Настоящая Инструкция в своем составе, терминах и определениях основывается на Положении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005), утвержденного приказом Федеральной службы безопасности России от 9 февраля 2005 г. № 66; «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», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. №152.

Под работами с применением СКЗИ в настоящей Инструкции понимаются

защищенное подключение к информационным системам, подписание электронных документов ЭП и проверка подписи, шифрование файлов и так далее.

СКЗИ должны использоваться для защиты ИОД (включая ПДн), не содержащей сведений, составляющих государственную тайну.

3. Порядок получения допуска пользователей к работе со СКЗИ

3.1. Для работы со СКЗИ привлекаются физические лица, включенные в перечень Пользователей СКЗИ, утвержденного соответствующим приказом ректора Университета. Основанием для включения в перечень является Заключение о допуске к самостоятельной работе со СКЗИ. Решение о готовности пользователя к самостоятельной работе со СКЗИ принимает Ответственный за СКЗИ на основании результатов принятого у пользователя зачета.

3.2. Для того чтобы получить Заключение о допуске к самостоятельной работе со СКЗИ пользователю необходимо выполнить следующее:

3.2.1. Самостоятельно ознакомиться с положениями:

– Федерального закона от 06.04.2011 № 63–ФЗ «Об электронной подписи»;

– Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 152 от 13.06.2001 «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»;

– Настоящей инструкцией;

– Инструкцией по обращению со СКЗИ;

– Эксплуатационной документацией на СКЗИ.

3.2.2. Пройти зачет на знание правил работы со СКЗИ.

3.2.3. При успешном прохождении тестирования Ответственным за СКЗИ оформляется Заключение о допуске пользователя к самостоятельной работе со СКЗИ (Приложение 1), которое утверждается ректором Университета.

4. Обязанности Пользователей СКЗИ

Пользователи СКЗИ обязаны:

– не разглашать ИОД, к которой они допущены, в том числе сведения о криптоключах;

– сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;

– соблюдать требования к обеспечению с использованием СКЗИ безопасности ИОД;

– сообщать Ответственному за СКЗИ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять Ответственного за 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 разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Пользователь несет ответственность за то, чтобы на ПК, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы–вирусы), которые могут нарушить функционирование СКЗИ.

На ПК, оборудованном СКЗИ, программное обеспечение должно быть лицензионным. При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, работа со СКЗИ на данном рабочем месте должна быть прекращена и организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Все полученные обладателем ИОД экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям

СКЗИ, несущим персональную ответственность за их сохранность.

Не допускается:

– разглашать ИОД, к которой был допущен пользователь СКЗИ;

– разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;

– выводить ключевую информацию на дисплей и(или) принтер;

– вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка ЭП и так далее), а также в порты других ПК;

– записывать на ключевом носителе постороннюю информацию;

– вносить какие–либо изменения в программное обеспечение СКЗИ;

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием ИОД, Пользователи СКЗИ обязаны сообщать Ответственному за СКЗИ.

5. Ответственность пользователей СКЗИ

Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность ИОД, которая стала им известной вследствие исполнения ими своих служебных обязанностей. Ответственность лиц, допущенных к работе со СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция по обращению со СКЗИ, Инструкция пользователя СКЗИ), а также за разглашение ИОД, ставшей им известной вследствие исполнения ими своих служебных обязанностей, определяется действующим законодательством Российской Федерации.

Приложение 1
к Инструкции пользователей средств криптографической защиты информации

Заключение о допуске к самостоятельной работе со СКЗИ (форма)

УТВЕРЖДАЮ
ректор ФГБОУ ВО «СГЭУ»

_____ Ашмарина С.И.
м.п.
«___» _____ 20 ___ г.

Заключение
о допуске к самостоятельной работе со СКЗИ

Должность: _____
Фамилия, имя, отчество: _____
_____
в соответствии с Инструкцией пользователя средств криптографической защиты информации (далее – СКЗИ), утвержденной приказом ректора ФГБОУ ВО «СГЭУ» №____-ОВ от «___» _____ 2020 г. самостоятельно ознакомился(лась) с положениями: Федерального закона от 06.04.2011 № 63–ФЗ «Об электронной подписи»; Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 152 от 13.06.2001 «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»; Инструкцией по обращению со СКЗИ, утвержденной приказом ректора ФГБОУ ВО «СГЭУ» №____-ОВ от «___» _____ 2020 г. и прошел(ла) зачет на знание правил работы со СКЗИ, не содержащей сведений, составляющих государственную тайну, результат по итогам тестирования – _____.
зачет / не зачет

По решению ответственного за обеспечение функционирования и безопасности криптографических средств (далее – Ответственный за СКЗИ) к самостоятельной работе со средствами криптографической защиты информации _____. Дата прохождения зачета: «___» _____ 20___ г.
допущен(а) / не допущен(а)

Тестируемый _____ / _____ /
подпись Фамилия И.О.

Ответственный за СКЗИ _____ / _____ /
подпись Фамилия И.О.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

ЖУРНАЛ
проведения инструктажа пользователей средств криптографической защиты информации
(форма)

Журнал начат «____» _____ 20___ г.

_____
должность
_____ /_____/
подпись Фамилия ИО

Журнал завершен «____» _____ 20___г.

_____
должность
_____ /_____/
подпись Фамилия ИО

На _____ листах

20__ год

При проведении инструктажа я ознакомлен(а) с:	1) Инструкцией по обращению со средствами криптографической защиты информации; 2) Инструкцией пользователей средств криптографической защиты информации.						
№ п/п	Фамилия И.О.	Должность	Подпись	Инструктаж провел (ФИО)	Подпись	Дата	СКЗИ к работе с которым допущен работник
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							
12.							

В настоящем журнале прошнуровано,
пронумеровано и скреплено
___ листов
Ответственный за ведение журнала

_____

_____

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный экономический университет»
(форма)

Журнал начат «____» _____ 20___ г.

_____
должность
_____ /_____/
подпись Фамилия ИО

Журнал завершен «____» _____ 20___г.

_____
должность
_____ /_____/
подпись Фамилия ИО

На _____ листах

20___ год

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата/ подпись лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

В настоящем журнале прошнуровано,
пронумеровано и скреплено
___ листов
Ответственный за ведение журнала

_____

_____

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный экономический университет»

УТВЕРЖДЕНО
приказом ректора
ФГБОУ ВО «СГЭУ»
№ 333-ОВ от «25» мая 2020 г.

АКТ № _____ от «___» _____ 20___ г.
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов
(форма)

Комиссия ФГБОУ ВО «СГЭУ» в составе:_____
_____
_____
произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

Ответственный за обеспечение функционирования и безопасности криптосредств _____/_____

Члены комиссии:

_____/_____
_____/_____
_____/_____
_____/_____