МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

ПРИКАЗ

«02» 08 2018 г. № 1269

Об обращении со средствами
криптографической защиты информации

В целях исполнения требований «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию работ по криптографической защите информации начальника ОИБ Супонина А.В.
2. Ввести в действие Инструкцию по обращению со редствами криптографической защиты информации (СКЗИ) (Приложение 1).
3. Ввести в действие Инструкцию ответственного за организацию работ по криптографической защите информации (Приложение 2).
4. Ввести в действие Инструкцию пользователей средств криптографической защиты информации (Приложение 3).
5. Ответственному за организацию работ по криптографической защите информации ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией по обращению со средствами криптографической защиты информации и Инструкцией ответственного за организацию работ по криптографической защите информации.
6. Ответственному за организацию работ по криптографической защите информации ознакомить под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ и Инструкцией пользователей средств криптографической защиты информации.
7. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти обучение и проверку знаний по правилам работы с СКЗИ.
8. Ввести в действие форму Перечня пользователей СКЗИ (Приложение 4).
9. Ввести в действие форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение 5).

10. Ввести в действие форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов (Приложение 6).

11. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор М.В. Грязев

Лист согласования

Проекта приказа от **01.08.2018 (1249)**

Об обращении со средствами криптографической защиты информации

Исполнитель: **Супонин А.В.;**

ФИО	Должность	Дата	Виза/Форма согласования
Супонин А.В.	Начальник ОИБ	01.08.2018	Проект внесен / Электронно
Савельев А.В.	Начальник УИТиА	01.08.2018	Согласен / Электронно
Величко Т.А.	Документовед общего отдела	01.08.2018	Принят к согласованию общим отделом / Электронно
Маликов А.А.	Проректор по финансовой деятельности	01.08.2018	Согласен

УТВЕРЖДАЮ

Ректор ТулГУ

М.В. Грязев

2018 Г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЕЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Проректор по ФД	А.А. Маликов
Проректор по НР	В.Д. Кухарь
Проректор по УВР	Э.С. Темнов
Начальник ПЭУ	С.И. Триденская
Начальник ОМКОД	Е.А. Саввина
Начальник УИТиА	А.В. Савельев
Начальник УПР	А.С. Никифоров
Начальник УАК	М.В. Метелищенкова
Начальник ЮУ	Н.Я. Матвеева
Начальник ОИБ	А. В. Супонин

Предисловие

1 РАЗРАБОТАНА начальником ОИБ Супониным А.В.
2 ВНЕСЕНА отделом информационной безопасности ТулГУ.
3 УТВЕРЖДЕНА приказом ректора от «02» 08 2018 г.
4 ИЗДАНИЕ первое.
5 Дата размещения документа на сайте университета «02» 08 2018г.

СОДЕРЖАНИЕ

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий работников, допущенных к работам с использованием средств криптографической защиты информации (далее - Пользователей), в федеральном государственном бюджетном образовательном учреждении высшего образования «Тульский государственный университет» (далее - Организация).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия согласно технической документации на СКЗИ.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66, а также «Состава 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», утвержденных приказом ФСБ от 10.07.2014 № 378.

2 Термины и определения

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.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Орган криптографической защиты (ОКЗ) – структурное подразделение Организации, работник Организации или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Ответственный за организацию работ по криптографической защите информации (Ответственный) – сотрудник Организации, отвечающий за реализацию мероприятий, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ –работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - 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.

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.

3 Обязанности пользователей СКЗИ

1.1 Пользователи СКЗИ обязаны:

- соблюдать конфиденциальность информации ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
- обеспечивать сохранность вверенных ключевых носителей и ключевой документации на них;
- соблюдать требования безопасности информации ограниченного доступа при использовании СКЗИ;
- незамедлительно сообщать Ответственному о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;
- при увольнении или отстранении от исполнения обязанностей сдать Ответственному носители с ключевой документацией;
- при подозрении на компрометацию ключевой документации, а также при обнаружении факта утраты или недостачи СКЗИ, ключевых носителей, ключевой документации, хранилищ, личных печатей незамедлительно уведомлять Ответственного.

1.2 Пользователям СКЗИ запрещается:

- выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.);
- оставлять ключевые носители с ключевой документацией без присмотра;
- записывать на ключевой носитель информацию, не связанную с работой СКЗИ (текстовые и мультимедиа файлы, служебные файлы и т.п.);
- вносить любые изменения в программное обеспечение СКЗИ.

4 Ответственность пользователей СКЗИ

За нарушение установленных требований по эксплуатации криптосредств пользователь СКЗИ несет ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1

Лист ознакомления

с Инструкцией пользователей средств криптографической защиты информации

№ п/п	ФИО	Должность	Подпись, дата

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер листа				Всего листов в документе	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, ответственного за внесение изменений
	измененного	заменённого	нового	изъятого				

УТВЕРЖДАЮ

Ректор ТулГУ

М.В. Грязев

_____ 2018 Г.

ИНСТРУКЦИЯ ПО ОБРАЩЕНИЮ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Проректор по ФД	А.А. Маликов
Проректор по НР	В.Д. Кухарь
Проректор по УВР	Э.С. Темнов
Начальник ПЭУ	С.И. Триденская
Начальник ОМКОД	Е.А. Саввина
Начальник УИТиА	А.В. Савельев
Начальник УПР	А.С. Никифоров
Начальник УАК	М.В. Метелищенкова
Начальник ЮУ	Н.Я. Матвеева
Начальник ОИБ	А. В. Супонин

Предисловие

1 РАЗРАБОТАНА начальником ОИБ Супониным А.В.
2 ВНЕСЕНА отделом информационной безопасности ТулГУ.
3 УТВЕРЖДЕНА приказом ректора от «02» 08 2018 г.
4 ИЗДАНИЕ первое.
5 Дата размещения документа на сайте университета «02» 08 2018г.

СОДЕРЖАНИЕ

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в федеральном государственном бюджетном образовательном учреждении высшего образования «Тульский государственный университет» (ТулГУ), которые осуществляют работы с применением СКЗИ.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов другие действия согласно технической документации на СКЗИ.

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66, а также «Состава 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», утвержденных приказом ФСБ от 10.07.2014 № 378.

2 Термины и определения

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.

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

Орган криптографической защиты (ОКЗ) – структурное подразделение ТулГУ, работник Тулгу или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Ответственный за организацию работ по криптографической защите информации (Ответственный) – сотрудник ТулГУ, отвечающий за реализацию мероприятий, связанных с обеспечением в ТулГУ безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, средство автоматизации, предназначенное для эксплуатации работником ТулГУ в рамках исполнения должностных обязанностей.

Пользователи СКЗИ - работники ТулГУ, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - 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.

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.

3 Порядок получения допуска пользователей к работе с СКЗИ

3.1 Для получения допуска к работе с СКЗИ, работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний.

3.2 Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый руководителем ТулГУ.

3.3 Контроль над реализацией данных мероприятий возлагается на Ответственного.

4 Работа с СКЗИ

4.1 Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей в присутствии посторонних лиц запрещено. В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

4.2 Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в общем порядке. Все копии учитываются за отдельным номером.

4.3 Каждый ключевой документ должен быть зарегистрирован в Журнале поэкземплярного учёта СКЗИ.

4.4 Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только с разрешения руководителя организации с соответствующей пометкой в

журнале поэкземплярного учета.

4.5 При обнаружении на рабочей станции с установленным СКЗИ программного обеспечения, не соответствующего решаемым на данном рабочем месте задачам и должностным обязанностям работника, а также вирусных программ, отделом информационной безопасности ТулГУ должны быть незамедлительно организованы работы по расследованию инцидента информационной безопасности.

5 Действия в случае компрометации ключей

5.1 О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

5.2 К компрометации ключей относятся следующие события:

- утрата носителей ключа;
- утрата иных носителей ключа с последующим обнаружением;
- возникновение подозрений на утечку ключевой 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 информации, согласно технической документации на СКЗИ.

5.3 В случае компрометации ключа пользователя незамедлительно должны быть приняты меры по отзыву ключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

5.4 Визуальный осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

5.5 Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет отдел информационной безопасности ТулГУ.

При необходимости, привлекается лицензированный орган криптографической защиты.

6 Ответственность лиц, допущенных к работе с СКЗИ

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1

Лист ознакомления
с Инструкцией по обращению со средствами
криптографической защиты информации

№ п/п	ФИО	Должность	Подпись, дата

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер листа				Всего листов в документе	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, ответственного за внесение изменений
	измененного	замененного	нового	изъятого				

УТВЕРЖДАЮ
ректор ТулГУ
_____ М.В. Грязев
_____ 2018 Г.

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ РАБОТ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Проректор по ФД	А.А. Маликов
Проректор по НР	В.Д. Кухарь
Проректор по УВР	Э.С. Темнов
Начальник ПЭУ	С.И. Триденская
Начальник ОМКОД	Е.А. Саввина
Начальник УИТиА	А.В. Савельев
Начальник УПР	А.С. Никифоров
Начальник УАК	М.В. Метелищенкова
Начальник ЮУ	Н.Я. Матвеева
Начальник ОИБ	А. В. Супонин

Предисловие

1 РАЗРАБОТАНА начальником ОИБ Супониным А.В.
2 ВНЕСЕНА отделом информационной безопасности ТулГУ.
3 УТВЕРЖДЕНА приказом ректора от «02» 08 2018 г
4 ИЗДАНИЕ первое.
5 Дата размещения документа на сайте университета «02» 08 2018г.

СОДЕРЖАНИЕ

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее – Ответственный) в Федеральном государственном бюджетном образовательном учреждении высшего образования «Тульский государственный университет» (далее – Организация), которые осуществляют работы с применением средств криптографической защиты информации (далее – СКЗИ).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и другие действия согласно технической документации на СКЗИ.

Ответственный назначается приказом руководителя Организации из числа её работников.

Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее - Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. № 66, а также «Состава 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», утвержденных приказом ФСБ от 10.07.2014 № 378.

2 Термины и определения

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.

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

Орган криптографической защиты (ОКЗ) – структурное подразделение Организации, работник Организации или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – работники Организации, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) - 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.

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.

3 Обязанности Ответственного

3.1 При реализации мероприятий, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться действующим законодательством Российской Федерации, Инструкцией по обращению с СКЗИ, а также настоящей инструкцией.

3.2 На Ответственного возлагается проведение следующих мероприятий:

- ведение журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
- хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним;
- принятие ключевых документов к СКЗИ от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- своевременная актуализация перечня пользователей СКЗИ;
- ежегодная проверка наличия СКЗИ, эксплуатационной и технической документации к ним, согласно Журналу поэкземплярного учета СКЗИ.

3.3 Ответственный обязан:

- не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;
- обеспечивать сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;
- обеспечить соблюдение требований к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;
- немедленно уведомлять непосредственного руководителя 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 информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

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

4 Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

- требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;
- обращаться к непосредственному руководителю с предложением прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;
- инициировать проведение служебных расследований по фактам нарушения в Организации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

5 Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

6 Ответственность за невыполнение настоящей инструкции

За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1

Лист ознакомления
с Инструкцией ответственного за организацию работ
по криптографической защите информации

№ п/п	Фамилия, Имя, Отчество	Должность	Подпись, дата

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер листа				Всего листов в документе	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, ответственного за внесение изменений
	измененного	замененного	нового	изъятого				

УТВЕРЖДАЮ

Ректор ТулГУ

_____ М.В. Грязев

_____ 2018 Г.

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

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		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи 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	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

УТВЕРЖДАЮ

Ректор ТулГУ

_____ М.В. Грязев

«___» _____ 2018 Г.

Перечень пользователей, допущенных к работе с СКЗИ

№	ФИО работника	Должность

Сухонин /Сухонин А.В./

УТВЕРЖДАЮ

Ректор ТулГУ

_____ М.В. Грязев

_____2018 Г.

Форма типового акта № _____ «__» _____ 20__ г. (форма) об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов

Комиссия _____в составе:

(название организации)

_____

_____

_____

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 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**:

Председатель комиссии

_____/_____

Члены комиссии:

_____/_____

_____/_____

_____/_____

Сушин/Сушкин А.В./