Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по обращению со средствами криптографической защиты информации

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНА
Приказом ректора
(чем) (должность)
от «20» июля 2021 г. № 393-О
(дата)

И Н С Т Р У К Ц И Я О Р Г А Н И З А Ц И И
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Инструкция по обращению со средствами криптографической защиты информации — Введена впервые

1 Область применения

1.1 Настоящая инструкция по обращению со средствами криптографической защиты информации, разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в ФГБОУ ВО «ИРНИТУ», которые осуществляют работы с применением СКЗИ.

1.2 Требования данной инструкции распространяются на работников ФГБОУ ВО «ИРНИТУ», эксплуатирующих СКЗИ.

2 Нормативные ссылки

Настоящая инструкция разработана в соответствии и содержит ссылки на следующие нормативные документы:

Конституция Российской Федерации;

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Указ Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;

Приказ 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»;

Приказ Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)»;

Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 г. №378 «Об утверждении 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»;

Устав Иркутского национального исследовательского технического университета;

СТО 002-2018 Порядок управления документированной информацией (документами) СМК.

3 Термины, определения и сокращения

3.1 В настоящей инструкции применены следующие термины с соответствующими определениями:

Информация ограниченного доступа – информация, доступ к которой ограничен законодательством: персональные данные, информация, составляющая профессиональную (адвокатскую, банковскую, аудиторскую и пр.), коммерческую и служебную тайну.

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

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем 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 – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Пользователи СКЗИ – работники ФГБОУ ВО «ИРНИТУ», допущенные к работе с СКЗИ.

Система менеджмента качества – часть системы менеджмента применительно к качеству.

Средство криптографической защиты информации – аппаратные и/или программные компоненты, предназначенные для подписания электронных документов и/или 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.

Стандарт организации – нормативный документ по стандартизации, разработанный, как правило, на основе согласия, характеризующегося отсутствием возражений по существенным вопросам у большинства заинтересованных сторон, устанавливающий комплекс норм, правил, требований к различным видам деятельности университета или их результатам и утвержденный приказом руководства университета.

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

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.

3.2 В настоящей инструкции используются следующие сокращения:

Криптоключ – криптографический ключ;

СКЗИ – средство криптографической защиты информации;

СМК – система менеджмента качества;

СТО – стандарт организации;

ФГБОУ ВО «ИРНИТУ» – Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет».

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данную инструкцию возложена на начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ».

4.2 Разработчик настоящей инструкции осуществляет периодическую проверку (пересмотр) данного документа в установленном порядке согласно СТО 002-2018 Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований данной инструкции возлагается на все должностные лица и подразделения ФГБОУ ВО «ИРНИТУ», эксплуатирующие СКЗИ в ФГБОУ ВО «ИРНИТУ».

5 Общие положения

5.1 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.

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

5.3 Структурные подразделения ФГБОУ ВО «ИРНИТУ», в случаях приобретения ими СКЗИ, обязаны согласовать сводную заявку на приобретении СКЗИ с отделом информационной безопасности и документооборота. Подразделение, приобретшее СКЗИ, обязано передать рабочие копии СКЗИ в отдел информационной безопасности и документооборота.

6 Порядок получения допуска пользователей к работе с СКЗИ

6.1 Для получения допуска к работе с СКЗИ, работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний. Обучение проводится работниками отдела информационной безопасности и документооборота в форме инструктажа с соответствующей записью в журнал об инструктаже. Проверка знаний проводится в форме устного опроса по окончанию инструктажа. Программа инструктажа составляется отделом информационной безопасности и документооборота и утверждается ректором. При внесении значимых изменений в программу инструктажа, работнику необходимо прийти повторный инструктаж.

6.2 Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый ректором. Перечень пользователей составляется работниками отдела информационной безопасности и документооборота, в перечень включаются работники ФГБОУ ВО «ИРНИТУ», прошедшие обучение и проверку знаний о работе с СКЗИ.

6.3 Контроль над реализацией данных мероприятий возлагается на отдел информационной безопасности и документооборота.

7 Работа с СКЗИ

7.1 Размещение и установка 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 запрещены. В ФГБОУ ВО «ИРНИТУ» должны быть обеспечены условия

хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированное использование или копирование ключевой информации.

7.2 Для исключения утраты ключевой информации вследствие дефектов носителей необходимо, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в отделе информационной безопасности и документооборота.

7.3 Каждый ключевой носитель, а также другие СКЗИ должны быть зарегистрированы в журнале учёта СКЗИ (Приложение 1). Ответственным за ведение и хранение журнала учета СКЗИ является отдел информационной безопасности и документооборота.

7.4 Передача СКЗИ, эксплуатационной и технической документации к ним допускается только с разрешения ректора. Соответствующая пометка проставляется в журнале учета СКЗИ.

7.5 При обнаружении на рабочей станции с установленным СКЗИ, программного обеспечения, не применимого для решения рабочих задач, а также вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности.

8 Обязанности пользователей СКЗИ

8.1 Пользователи СКЗИ обязаны:

8.1.1 соблюдать конфиденциальность информации ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;

8.1.2 обеспечивать сохранность вверенных ключевых носителей и ключевой информации на них;

8.1.3 соблюдать требования безопасности информации ограниченного доступа при использовании СКЗИ;

8.1.4 незамедлительно сообщать Начальнику отдела информационной безопасности и документооборота о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;

8.1.5 при увольнении или отстранении от исполнения обязанностей сдать в отдел информационной безопасности и документооборота ключевые носители;

8.1.6 при подозрении на компрометацию ключевой информации, а также при обнаружении факта утраты или недостачи СКЗИ, ключевых носителей, незамедлительно уведомлять Начальника отдела информационной безопасности и документооборота.

8.2 Пользователям СКЗИ запрещается:

8.2.1 выводить ключевую информацию на средства отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.);

8.2.2 оставлять ключевые носители без присмотра;

8.2.3 записывать на ключевой носитель информацию, не связанную с работой СКЗИ (текстовые и мультимедиа файлы, служебные файлы и т.п.);

8.2.4 вносить любые изменения в программное обеспечение СКЗИ.

9 Действия в случае компрометации ключей

9.1 О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Начальнику отдела информационной безопасности и документооборота.

9.2 К компрометации ключей относятся следующие события:

а) утрата носителей ключа;

b) утрата носителей ключа с последующим обнаружением;

c) возникновение подозрений на утечку ключевой информации или ее искажение;

d) нарушение целостности печатей на местах хранения носителей ключевой информации, если используется процедура опечатывания таких мест;

e) утрата ключей от мест хранения носителей ключевой информации в момент нахождения в них носителей ключевой информации;

f) утрата ключей от мест хранения носителей ключевой информации в момент нахождения в них носителей ключевой информации с последующим обнаружением;

g) доступ посторонних лиц к ключевой информации;

h) другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

9.3 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.

9.4 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).

9.5 Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет отдел информационной безопасности и документооборота. При необходимости, привлекается внешний орган криптографической защиты, с соответствующей лицензией.

10 Ответственность лиц, допущенных к работе с СКЗИ

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

Приложение 1 Форма журнала учета СКЗИ

(обязательное)

ЖУРНАЛ
учета средств криптографической защиты информации
в ФГБОУ ВО «ИРНИТУ»

Дата начала: «___» _____ 20__ г.
Дата окончания: «___» _____ 20__ г.

№ п/п	Наименование	Регистрационный номер	Сведения о сертификате	Сведения об установке СКЗИ			Отметка о выдаче СКЗИ			Отметка об изъятии СКЗИ			Примечание
				Место установки (использования)	Ф.И.О. производившего установку	Подпись	Ф.И.О. пользователя СКЗИ	Дата	Подпись	Ф.И.О. производившего изъятие	Дата	Подпись	

Приложение 2 Лист согласования Инструкции по обращению со средствами криптографической защиты информации

(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по молодежной политике и работе с выпускниками	С.С. Аносов	05.07.21	
Проректор по административно-хозяйственной деятельности	И.А. Горбунов	12.07.21г	
Проректор по научной работе	А.М. Кононов	06.07.21	
Советник ректора	Е.Г. Можаева	16.07.21	
Проректор по международной деятельности	Д.А. Савкин	02.07.21	
Проректор по инновационной деятельности	Е.Ю. Семёнов	07.07.21	
Проректор по учебной работе	В.В. Смирнов	07.07.2021	
Советник ректора по безопасности и международным связям	С.К. Филиппов	25.06.2021	
Начальник управления по работе с персоналом и обучающимися	Т.Ю. Гуруленко	18.06.2021	
Начальник управления планирования, бухгалтерского учета и аудита	Н.Б. Максимова	08.07.2021	
Начальник управления по дополнительному образованию и социальной работе	Б.Б. Пономарев	07.07.21г	
Начальник управления информатизации	В.В. Шмелев	18.06.2021	
Руководитель юридической службы	О.Л. Пенизева	10.06.2021	
Заместитель начальника отдела мониторинга и качества образовательных услуг	О.С. Артемова	13.07.2021	

РАЗРАБОТАНО:

Начальник отдела информационной безопасности и документооборота	Л.В. Бархатова	18.06.21	

Приложение 3 Лист регистрации изменений Инструкции по обращению со средствами криптографической защиты информации

(обязательное)

Порядковый номер изменения	Основание (№ приказа, дата)	Дата введения изменения	Изменения внёс	
			Фамилия, инициалы	Подпись вносившего изменения, дата внесения
1	2	3	4	5

Приложение 4 Лист ознакомления с Инструкцией по обращению со средствами криптографической защиты информации

(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись