МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)

ПРИКАЗ

26.08.2019 № 588-о

Казань

Об организации работ со средствами криптографической защиты информации в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет»

В целях исполнения требований приказа ФСБ России от 10.07.2014 № 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 ФАПСИ от 13 июня 2001 г. N 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» п р и к а з ы в а ю:

1. Создать группу обеспечения функционирования и безопасности средств криптографической защиты информации в составе начальника Центра компьютерной безопасности (далее – ЦКБ) Управления информатизации Филюкова В.Ю. (начальник группы) и специалиста по защите информации автоматизированных систем ЦКБ.

2. Утвердить Положение о группе обеспечения функционирования и безопасности средств криптографической защиты информации (Приложение №1).

3. Утвердить Инструкцию по обеспечению функционирования и безопасности криптографических средств в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (Приложение № 2).

4. Начальнику ЦКБ Филюкову В.Ю. руководствоваться в своей деятельности Инструкцией по обеспечению функционирования и безопасности криптографических средств в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет». Данную инструкцию довести под роспись сотрудникам ЦКБ.

5. Утвердить Инструкцию по обращению со средствами криптографической защиты информации в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (Приложение № 3).

6. Утвердить Инструкцию пользователей средств криптографической защиты информации в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (Приложение № 4).

7. Начальнику ЦКБ Филюкову В.Ю. ознакомить под роспись пользователей СКЗИ с вышеперечисленными инструкциями

8. Помещение № И-1-104 определить как спецпомещение органа криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации и инсталлирующих СКЗИ носителей. Охрану спецпомещения организовать в соответствии с требованиями раздела IV Инструкции об организации и обеспечения безопасности хранения,

обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (приказ ФАПСИ РФ от 13 июня 2001 года № 152). Ответственным за помещение № И-1-104 назначить ведущего инженера-программиста ЦКБ Тупаева А.С.

9. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти инструктаж в ЦКБ по правилам работы с СКЗИ.

10. Контроль за исполнением настоящего приказа возложить на директора по развитию Артемьева А.В.

Ректор С.В. Юшко

Приложение № 1
к приказу ФГБОУ ВО «КНИТУ»
от 26.08.2019 № 588-О

Положение
о группе обеспечения функционирования и безопасности криптографических средств защиты информации

1 Общие положения

Настоящее Положение о группе обеспечения функционирования и безопасности криптографических средств защиты информации (далее – группа) разработано в целях обеспечения криптографическими средствами безопасность информации, не составляющей государственную тайну, циркулирующей в информационных системах ФГБОУ ВО «КНИТУ»

Группа является нештатным подразделением. Руководство группой осуществляет начальник Центра компьютерной безопасности.

Группа в своей деятельности руководствуется требованиями Закона РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи», приказа ФСБ России от 10.07.2014 № 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 ФАПСИ от 13.06.2001 № 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», указаниями начальника Управления информатизации, а также указаниями и рекомендациями органа криптографической защиты – лицензиата ФСБ, оказывающего услуги КНИТУ по криптографической защите информации.

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.

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

Пользователи СКЗИ – работники КНИТУ, 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.

3. Функции группы:

- осуществление взаимодействия с органом криптографической защиты – лицензиатом ФСБ, оказывающим услуги КНИТУ по криптографической защите информации;
- обеспечение функционирования и безопасности криптографических средств.
- организация допуска пользователей к работе на СКЗИ;

4. Задачи группы:

- ведение «Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов» и иной документации;
- организация хранения носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;
- организация обучения и инструктаж пользователей при допуске к работе с СКЗИ;
- ведение учета лиц, допущенных к работе с криптосредствами (в том числе и с электронной подписью);
- организация передачи СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ под роспись в соответствующих журналах поэкземплярного учета;

- 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 мероприятий по розыску и локализации последствий при компрометации криптоключей, а также информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ (осуществляется совместно с подразделением КНИТУ - обладателем скомпрометированной информации ограниченного доступа);

- осуществление периодической проверки (не реже одно раза в полгода) журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов;

- осуществление контроля целостности печатей (пломб) на технических средствах с установленными СКЗИ;

- организация и контроль использования средств электронной подписи в подразделениях КНИТУ.

5. Обязанности работников группы:

– не разглашать информацию ограниченного доступа, к которой работники 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 информации ограниченного доступа;

– немедленно уведомлять начальника Управления информатизации и проректора по режиму и безопасности 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;

– 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.

6. Права работников группы:

– требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;

– обращаться к руководителю подразделения КНИТУ с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

– инициировать проведение служебных расследований по фактам нарушения порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Приложение № 2
к приказу ФГБОУ ВО «КНИТУ»
от 26.08.2019 № 588-о

Инструкция
по обеспечению функционирования и безопасности криптографических средств в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет»

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за обеспечение функционирования и безопасности криптографических средств в информационных системах ФГБОУ ВО «КНИТУ».

Ответственность за обеспечение функционирования и безопасность криптографических средств в информационных системах ФГБОУ ВО «КНИТУ» (далее – КНИТУ) возлагается на начальника Центра компьютерной безопасности Управления информатизации КНИТУ (далее – ЦКБ).

СКЗИ должны использоваться 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 13.06.2001 №152 (далее – Инструкция ФАПСИ от 13.06.2001 № 152).

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.

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

Пользователи СКЗИ – работники Университета, 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.

3 Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ необходимо реализовать ряд мероприятий:

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

– учёт лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения защиты информации в ирнформационных системах Университета, осуществлять в Журнале учета лиц, допущенных к работе на СКЗИ;

– контроль над реализацией данных мероприятий возлагается на ЦКБ.

4 Задачи ЦКБ в вопросах обеспечения функционирования и безопасности криптографических средств

При решении всех вопросов, связанных с обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, начальник ЦКБ должен руководствоваться Инструкцией по обращению с СКЗИ в ФГБОУ ВО «КНИТУ».

На ЦКБ возлагается проведение следующих мероприятий:

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

– 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 (не реже одно раза в полгода) журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов.

Работники ЦКБ обязаны:

– не разглашать информацию ограниченного доступа, 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 информации ограниченного доступа;

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

– немедленно уведомлять начальника Управления информатизации, курирующего проректора и проректора по режиму и безопасности, 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;

– 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 ЦКБ в вопросах обеспечения функционирования и безопасности криптографических средств

В рамках исполнения возложенных на ЦКБ обязанностей, работники ЦКБ имеют право:

– требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;

– ставить вопрос перед руководством о прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

– инициировать проведение служебных расследований по фактам нарушения порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

Приложение № 3
к приказу ФГБОУ ВО «КНИТУ»
от 26.08.2019 № 588-о

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет»

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) в информационных системах государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее – КНИТУ). 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, в т.ч. ПДн.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

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 ФСБ РФ 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, утвержденной приказом ФАПСИ РФ от 13 июня 2001 г. № 152.

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;

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

Пользователи СКЗИ – работники Университета, 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.

3 Работа с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с 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 подразделениях КНИТУ 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 и об этом факте информируется Центр компьютерной безопасности (далее – ЦКБ), который 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 информации ограниченного доступа, пользователи СКЗИ обязаны сообщать в ЦКБ.

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 информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет подразделение КНИТУ (обладатель скомпрометированной информации ограниченного доступа).

5 Обязанности и ответственность лиц, допущенных к работе с СКЗИ

Лица, допущенные к работе с СКЗИ, обязаны:

– не разглашать информацию ограниченного доступа, 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 информации ограниченного доступа;

– сообщать в ЦКБ 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 ЦКБ 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 с СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала им известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями, а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

Приложение № 4
к приказу ФГБОУ ВО «КНИТУ»
от 26.08.2019 № 588-о

ИНСТРУКЦИЯ
пользователей средств криптографической защиты информации в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет»

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) в информационных системах Федерального государственного бюджетного образовательного учреждения высшего образования «Казанский национальный исследовательский технологический университет» (далее – КНИТУ)

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 т.д.

СКЗИ должны использоваться 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) и «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.

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;

Пользователи СКЗИ – работники организации или учреждения, 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

Для работы с СКЗИ привлекаются сотрудники, включенные в перечень пользователей СКЗИ, утвержденного соответствующим приказом ректора КНИТУ. Основанием для включения в перечень является Заключение о допуске к самостоятельной работе с СКЗИ. Решение о готовности пользователя к самостоятельной работе с СКЗИ принимает начальник Центра компьютерной безопасности (далее – ЦКБ) на основании результатов принятого у пользователя зачета.

Для того чтобы получить Заключение о допуске к самостоятельной работе с СКЗИ, пользователю необходимо выполнить следующее:

1) Самостоятельно ознакомиться с положениями:

- Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011;
- Приказа ФАПСИ N 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 средствами криптографической защиты информации;
- Эксплуатационной документацией на СКЗИ;

2) Пройти зачет на знание правил работы с СКЗИ.

3) При успешном прохождении тестирования ЦКБ оформляет Заключение о допуске пользователя к самостоятельной работе с СКЗИ, которое утверждается ректором КНИТУ.

4 Обязанности пользователей СКЗИ

Пользователи СКЗИ обязаны:

1) не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;

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

3) соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;

4) сообщать в ЦКБ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

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

6) немедленно уведомлять ЦКБ 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 с СКЗИ на данном рабочем месте должна быть прекращена и ЦКБ организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Все полученные обладателем информации ограниченного доступа 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:

1) разглашать информацию ограниченного доступа, к которой был допущен пользователь СКЗИ;

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

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

4) вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других ПК;

5) записывать на ключевом носителе постороннюю информацию;

6) вносить какие-либо изменения в программное обеспечение СКЗИ;

7) 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 информации ограниченного доступа, пользователи СКЗИ обязаны сообщать в ЦКБ.

5 Ответственность пользователей СКЗИ

Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей. Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями, а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.