МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Пензенский государственный университет»
(ФГБОУ ВО «ПГУ»)

ПРИКАЗ

13.06.2023 № 630/о

О создании органа криптографической защиты

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», утверждённой приказом ФАПСИ от 13 июня 2001 г. № 152,

ПРИКАЗЫВАЮ:

1. Создать орган криптографической защиты в ФГБОУ ВО «Пензенский государственный университет» и назначить ответственными за организацию работ со средствами криптографической защиты информации:

– начальника отдела информационной безопасности Коршунова Михаила Евгеньевича;

– инженера отдела информационной безопасности Смольянова Дмитрия Сергеевича.

2. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (далее – СКЗИ) (приложение № 1).

3. Утвердить Инструкцию пользователей средств криптографической защиты информации (приложение № 2).

4. Органу по криптографической защите ознакомить под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ и Инструкцией пользователей средств криптографической защиты информации.

5. Контроль за исполнением настоящего приказа возложить на проректора по цифровизации Антонова Александра Викторовича.

Ректор **А.Д. Гуляков**

Проект вносит:

Начальник ОИБ М.Е. Коршунов

Согласовано:

Первый проректор Д.В. Артамонов

Проректор по цифровизации А.В. Антонов

Начальник ПУ К.Б. Филиппов

Начальник ОДОУ Н.В. Шамарина

Приложение № 1
к приказу № 630/о от 13.06.2023

УТВЕРЖДЕНО
приказом «О создании органа
криптографической защиты информации»
от «13» 06 2023 года № 630/о

ИНСТРУКЦИЯ

по обращению со средствами криптографической защиты информации в ФГБОУ ВО «Пензенский государственный университет»

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) в ФГБОУ ВО «Пензенский государственный университет» (далее - Организация), которые осуществляют работы с применением 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 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. Порядок получения допуска пользователей к работе с СКЗИ

Основанием для допуска пользователя к работе с СКЗИ является внесение его в перечень пользователей СКЗИ, утверждаемый приказом по Организации.

4. Работа с СКЗИ

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.

5. Действия в случае компрометации ключей

О событиях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать в ОКЗ.

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;
2) утрата иных носителей ключа с последующим обнаружением;
3) возникновение подозрений на утечку ключевой информации или ее искажение;
4) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
5) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
7) доступ посторонних лиц к ключевой информации;
8) другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

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.

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).

Расследование инцидентов информационной безопасности, связанных с компрометацией ключевых носителей и ключевой документацией, осуществляет (обладатель скомпрометированной информации ограниченного доступа с привлечением отдела информационной безопасности).

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 № 2
к приказу № 630/0 от 13.06.2023

УТВЕРЖДЕНО
приказом «О создании органа
криптографической защиты информации»
от «___» _____ 20___ года № _____

ИНСТРУКЦИЯ

пользователей средств криптографической защиты информации в ФГБОУ ВО «Пензенский государственный университет»

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий работников, допущенных к работам с использованием средств криптографической защиты информации (далее - Пользователей), в ФГБОУ ВО «Пензенский государственный университет» (далее - Организация).

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, 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 (далее 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

Пользователи СКЗИ обязаны:

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

2) обеспечивать сохранность вверенных ключевых носителей и ключевой документации на них;

3) соблюдать требования безопасности информации ограниченного доступа при использовании СКЗИ;

4) незамедлительно сообщать Ответственному о ставших им известными попытках получения посторонними лицами доступа к сведениям об используемых СКЗИ, ключевым носителям и ключевой документации;

5) при увольнении или отстранении от исполнения обязанностей сдать Ответственному носители с ключевой документацией;

6) 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.

Пользователям СКЗИ запрещается:

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

2) оставлять ключевые носители с ключевой документацией без присмотра;

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

4) 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.

УТВЕРЖДЕНО
приказом «Об обращении со средствами
криптографической защиты информации»
от «___» _____ 20___ года № _____

ЖУРНАЛ
ознакомления с Инструкцией пользователей средств криптографической защиты информации

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

№ п/п	Ф.И.О.	Должность	Дата	Подпись

УТВЕРЖДЕНО
приказом «Об обращении со средствами криптографической защиты информации»
от «___» _____ 20___ года № _____

ЖУРНАЛ
ознакомления с Инструкцией по обращению со средствами криптографической защиты информации

Начат: «___» _____ 20__ г.

Окончен: «___» _____ 20__ г.

№ п/п	Ф.И.О.	Должность	Дата	Подпись