УТВЕРЖДЕНА
приказом ФГАОУ ВО «СПбПУ»
от 04.04.2024 № 823

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ СКЗИ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

Санкт-Петербург
2024 г.

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ, криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.

1.2. Настоящая Инструкция разработана в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 09.02.2005 № 66, приказом ФСБ России от 10.07.2014 № 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» и Инструкцией 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.

1.3. В ФГАОУ ВО «СПбПУ» используются только сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.4. В ФГАОУ ВО «СПбПУ» приказом руководителя назначается ответственный за хранение и эксплуатацию СКЗИ, именуемый также органом криптографической защиты информации (далее – ОКЗ).

1.5. Подписывая лист ознакомления с настоящей Инструкцией, ОКЗ подтверждает, что также ознакомлен с Инструкцией 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).

2. Обязанности органа криптографической защиты

2.1. Поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов.

2.2. Учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение руководителю списка пользователей СКЗИ.

2.3. Контроль за соблюдением условий использования СКЗИ.

2.4. Расследования и составление заключений по фактам нарушений условий использования СКЗИ.

2.5. Разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений.

2.6. Обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.

2.7. Список Пользователей СКЗИ утверждается приказом проректора по информационным технологиям ФГАОУ ВО «СПбПУ».

3. Обязанности пользователя

3.1. Не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты.

3.2. Соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ.

3.3. Хранить ключевую информацию в сейфах и помещениях, гарантирующую ее сохранность и конфиденциальность.

3.4. Сообщать ОКЗ о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним.

3.5. Незамедлительно уведомлять ОКЗ о фактах утраты или недостачи СКЗИ, криптографических ключей, 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.

3.6. Сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи ОКЗ, в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ (увольнении, перевода на другую должность и в иных подобных случаях).

3.7. К работе с СКЗИ Пользователи допускаются только после проведения соответствующего инструктажа.

4. Учет СКЗИ, хранение и передача криптографических ключей

4.1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ОКЗ в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал).

4.2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами. Если один и тот же носитель используется для записи другого криптографического ключа, его необходимо зарегистрировать снова.

4.3. Все полученные экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы выдаются Пользователям под роспись в Журнале. Пользователи несут персональную ответственность за сохранность СКЗИ и ключевых документов.

4.4. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к ним хранятся у ОКЗ.

4.5. Ключевые носители с криптографическими ключами хранятся у Пользователей.

4.6. Хранение осуществляется в ящиках, шкафах, сейфах (хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

4.7. В случае отсутствия у Пользователя индивидуального хранилища, ключевые носители с криптографическими ключами по окончании рабочего дня сдаются ОКЗ.

4.8. Ключевые носители с неработоспособными криптографическими ключами ОКЗ принимает от Пользователя и делает соответствующую запись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.

4.9. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

5. Использование СКЗИ

5.1. В ФГАОУ ВО «СПбПУ» СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика, а также с целью организации юридически значимого электронного документооборота с использованием средств электронной подписи.

5.2. Для шифрования электронного документа и/или сетевого трафика Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.

5.3. В ФГАОУ ВО «СПбПУ» используются только те СКЗИ, которые реализуют стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.

5.4. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.

5.5. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данному факту созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

5.6. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии ОКЗ.

6. При работе с СКЗИ пользователю запрещается

6.1. Оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ.

6.2. Самостоятельно вносить изменения в программную часть СКЗИ.

6.3. Разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства вывода информации.

6.4. Использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ.

6.5. Осуществлять несанкционированное копирование криптографических ключей.

6.6. Изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ОКЗ.

6.7. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации.

6.8. Осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

6.9. С целью обеспечения непрерывности работы ФГАОУ ВО «СПбПУ» плановая замена ключевой информации должна производиться заблаговременно.

7. Действия при компрометации криптографических ключей

7.1. Криптографические ключи считаются скомпрометированными в следующих случаях:

- потеря ключевых носителей (в том числе с последующим обнаружением);
- увольнение работников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в информационной системе;
- нарушение печати на хранилище с ключевыми носителями или на техническом средстве с СКЗИ;
- временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;
- иные случаи подозрения компрометации криптографических ключей.

7.2. В случае подозрения в компрометации криптографических ключей, Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.

7.3. Скомпрометированные криптографические ключи подлежат уничтожению.

8. Уничтожение криптографических ключей

8.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.

8.2. Уничтожение криптографических ключей на ключевых носителях производятся комиссией в составе председателя и членов комиссии, назначенной приказом руководителя ФГАОУ ВО «СПбПУ».

8.3. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

8.4. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. д.).

8.5. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:

- установить наличие оригинала и количество копий криптографических ключей;
- проверить внешнюю целостность каждого ключевого носителя;
- идентифицировать каждый ключевой носитель в соответствии с Журналом поэкземплярного учета средств криптографической защиты информации;
- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
- произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя;
- по факту уничтожения криптографических ключей составляется Акт уничтожения.

8.7. Акт подписывается председателем и членами комиссии по уничтожению.

8.8. В Журнале поэкземплярного учета средств криптографической защиты информации делается отметка об уничтожении криптографических ключей.

8.9. Акты уничтожения криптографических ключей хранятся у ОКЗ.

9. Требования к помещениям, в которых ведется работа с СКЗИ и/или хранятся криптографические ключи

9.1. Размещение, специально оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и/или хранятся криптографические ключи (далее – спецпомещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.

9.2. При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

9.3. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в спецпомещения. При этом, применение нераспахиваемых железных решеток на окнах запрещено, поскольку это противоречит правилам пожарной безопасности.

9.4. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам, либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.

9.5. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ в ОКЗ выделяется необходимое число надежных металлических хранилищ, у Пользователей выделяется необходимое число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от ящиков, шкафов, сейфов (хранилищах) хранятся у ОКЗ и у Пользователей.

9.6. По окончании рабочего дня спецпомещения и установленные в них хранилища должны быть закрыты на замок.

9.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ОКЗ. ОКЗ должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.