Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

ПРИКАЗ

от «18» апреля 2024 г. г. Королёв № 01-04-01-05/375

Об утверждении Положения о порядке обеспечения безопасности информации с использованием средств криптографической защиты информации федерального государственного бюджетного образовательного учреждения высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова».

На основании решения ученого совета федерального государственного бюджетного образовательного учреждения высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» от 08.04.2024г., протокол №9.

ПРИКАЗЫВАЮ:

1. Ввести в действие Положение о порядке обеспечения безопасности информации с использованием средств криптографической защиты информации федерального государственного бюджетного образовательного учреждения высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» (далее – Положение) согласно Приложению №1 к настоящему приказу.
2. Начальнику общего отдела (Проняева Н.А.) или лицу, его замещающему в установленном порядке в течении трех рабочих дней с момента издания приказа обеспечить рассылку настоящего приказа руководителям всех структурных подразделений Университета.
3. Начальнику управления информационных технологий (Хвостов П.М.) или лицо, его замещающее в установленном порядке, в течении трех рабочих дней с момента издания приказа обеспечить размещение документа, указанного в пункте 1 настоящего приказа, на образовательном портале Университета, в формате .pdf, в разделе «Приказы по основной деятельности».
4. Настоящий приказ вступает в силу с момента его подписания.
5. Контроль за исполнением настоящего приказа возложить на исполняющего обязанности проректора Троицкого А.В.

И.о. ректора **Н.В. Фролова**

Приложение № 1
к приказу от «18» апреля 2024г.
№ 01-04-01-05/375

Положение
о порядке обеспечения безопасности информации с использованием средств криптографической защиты информации

1. Общие положения

1.1. Настоящее положение определяет порядок обеспечения безопасности информации, а так же учета, хранения и использования средств криптографической защиты информации (далее – Положение), криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации средств криптографической защиты информации (далее – СКЗИ) в Федеральном государственном бюджетном образовательном учреждении высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» (далее – Университет).

1.2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:

- 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 (утв. приказом ФСБ России от 10.07.2014 № 378);
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);
- Инструкция 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).

1.3. В Университете используются только сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

1.4. В Университете приказом ректора 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).

1.6. ОКЗ осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов;
- учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение ректору Университета списка пользователей СКЗИ;
- контроль за соблюдением условий использования СКЗИ;
- расследования и составление заключений по фактам нарушений условий использования СКЗИ;
- разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;
- обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.

1.7. Список Пользователей утверждается приказом ректора Университета.

1.8. Пользователь обязан:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;
- хранить ключевую информацию в сейфах и помещениях, гарантирующую ее сохранность и конфиденциальность;
- сообщать ОКЗ о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;
- 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;
- 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).

1.9. К работе с СКЗИ Пользователи допускаются только после соответствующего инструктажа.

1.10. При использовании СКЗИ требования настоящего Положения имеют преимущество перед требованиями организационно – распорядительной документации по управлению обработкой и защитой ПДн в ИС в отношении аналогичных объектов или процессов защиты.

1.11. Настоящее Положение вступает в силу после его утверждения ректором Университета и действует бессрочно, до момента его замены новым.

2. Термины и определения

В данном Положении используются следующие термины и их определения:

- Администратор безопасности - пользователь, уполномоченный выполнять действия (имеющий полномочия) по администрированию (управлению) системы защиты информации информационной системы персональных данных.
- Средство криптографической защиты информации - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну (далее - СКЗИ).
- Пользователь СКЗИ - лицо, участвующее в эксплуатации СКЗИ или использующее результаты его функционирования.
- Ответственный за организацию обработки персональных данных (далее - ПД) – сотрудник Университета, эксплуатирующий информационную систему персональных данных (далее - ИСПД), отвечающий за организацию обработки ПД.
- Криптоключ - секретная информация, используемая криптографическим алгоритмом при шифровании/расшифровке сообщений.

3. Управление СКЗИ

3.1 Управление СКЗИ осуществляется в Университете с целью обеспечения безопасности обработки ПДн, с использованием криптосредств (Приказ ФСБ Российской Федерации №378 Часть 1, п.3).

3.2 Настоящее Положение регламентирует порядок управления СКЗИ на стадии эксплуатации СКЗИ в составе системы защиты информации ИС.

3.3 К управлению СКЗИ на этапе эксплуатации отнесены процедуры:

- учет СКЗИ;
- учет пользователей СКЗИ;
- контроль соблюдения условий использования СКЗИ;
- хранение, выдача, замена и уничтожение СКЗИ;
- действия при утере и компрометации СКЗИ;
- защита СКЗИ.

4. Учет и хранение СКЗИ

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

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

4.4 Ключевые носители с криптографическими ключами хранятся у Пользователей.

4.5 Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи, ответственный пользователь СКЗИ должен немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

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

4.7 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 Университете 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 закрытый криптографический ключ и открытый криптографический ключ.

5.3. В Университете 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 их целостность.

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 (далее – ГРИИБ), 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.

5.7. При работе с СКЗИ запрещается:

- оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;
- самостоятельно вносить изменения в программную часть СКЗИ;
- 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;
- использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;
- осуществлять несанкционированное копирование криптографических ключей;
- изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ОКЗ;
- использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;
- осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.

5.8. С целью обеспечения непрерывности работы Университета плановая замена ключевой информации должна производиться заблаговременно.

6. Действия при компрометации криптографических ключей

6.1. Криптографические ключи считаются скомпрометированными в следующих случаях:

- потеря ключевых носителей (в том числе с последующим обнаружением);
- увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение в информационной системе;
- нарушение печати на хранилище с ключевыми носителями ли на техническом средстве с СКЗИ;

- временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;
- иные случаи подозрения компрометации криптографических ключей.

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

6.3. Скомпрометированные криптографические ключи подлежат уничтожению.

7. Правила выдачи СКЗИ

7.1. Все экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственный пользователь криптосредств выдает пользователям криптосредств под расписку в журнале поэкземплярного учета.

7.2. Ответственный пользователь криптосредств заводит и ведет журнал пользователей криптосредств, в котором регистрирует числящиеся за пользователми криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

7.3. Передачу криптосредств, эксплуатационной и технической документации к ним, ключевых документов пользователю криптосредств может производить только ответственный пользователь криптосредств под расписку в журнале поэкземплярного учета.

7.4. Передача криптосредств между пользователями криптосредств запрещена.

8. Правила уничтожения СКЗИ

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 ректором Университета.

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. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств, и они полностью отсоединены от аппаратных средств.

8.6. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для

аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

8.7. 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.

8.8. По факту уничтожения криптографических ключей составляется Акт уничтожения (Приложение № 1).

8.9. Акт подписывается председателем и членами комиссии по уничтожению.

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

8.11. 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. Размер помещений для установки и хранения СКЗИ должен быть выбран с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией на СКЗИ.

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

9.4. 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.

9.5. 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.

9.6. По окончании рабочего дня спецпомещения должны быть закрыты на замок.

9.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения 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.

10. Размещение и монтаж СКЗИ

10.1. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с криптосредствами, в соответствующих помещениях должны сводить к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

10.2. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

Приложение № 1

АКТ

уничтожения СКЗИ

№

г. _____ «_____»_____20_____г.

Комиссия из числа сотрудников органа криптографической защиты в составе:

1. _____

(ФИО, должность)

2. _____

(ФИО, должность)

назначенных приказом от_____г. №_____в ФГОУ ВО «Технологический университет» составила настоящий акт о том, что перечисленные в нем СКЗИ, указанные в таблице №1, уничтожены путем _____

№ п/п	Наименование СКЗИ	Уч. №АРМ	Серийный номер сертификата ключа проверки электронной подписи / номер лицензии	ФИО пользователя СКЗИ

Уничтожено в количестве_____(цифрами и прописью) наименований и экземпляров ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации.

Члены комиссии:

_____/_____

(подпись) (Ф.И.О)

_____/_____