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 № 01-04-01-05/379

Об утверждении Положения о работе с электронной подписью 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 15.04.2024г., протокол №10.

ПРИКАЗЫВАЮ:

1. Ввести в действие Положение о работе с электронной подписью 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.
№ 01-04-01-05/379

Положение
о работе с электронной подписью

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ "Об электронной подписи", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ГОСТ Р 34.10-2012 "Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. и введен в действие Приказом Росстандарта от 07.08.2012 N 215-ст), "Р 1323565.1.033-2020. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML" (утв. и введены в действие Приказом Росстандарта от 17.11.2020 N 1112-ст), иными нормативно-правовыми актами российского законодательства в сфере применения электронных подписей.

1.2. Положение устанавливает порядок использования электронных подписей сотрудниками Федерального государственного бюджетного образовательного учреждения высшего образования «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» (далее - Университет) при общении в электронном виде внутри Университета и с третьими лицами, в том числе с государственными и муниципальными органами, государственными корпорациями, органами государственных внебюджетных фондов, иностранными контрагентами.

1.3. Требования настоящего Положения не распространяются на документы, для которых установлен собственный регламент подписания и обмена.

1.4. Право электронной подписи документов предоставляется сотруднику Университета при наличии у него соответствующих полномочий по должности или по доверенности.

1.5. Доверенность оформляется на бумаге и заверяется в соответствии с внутренними документами Организации или нотариально.

1.6. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи".

1.7. Электронная подпись используется в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью.

1.8. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

1.9. Электронные документы, подписанные электронной подписью, равнозначны документам на бумажных носителях, подписанным собственноручной подписью, если:

1) не опорочена сама подпись;

2) нет сомнений в определении лица, подписывающего электронный документ, по его электронной подписи;

3) подписантом соблюдена конфиденциальность при создании и/или использовании ключа электронной подписи.

2. Термины и определения

В данном Положении используются следующие термины и их определения:

1) Электронная подпись (далее –ЭП) - 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;

2) Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

4) Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) 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 настоящим Федеральным законом;

8) Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

9) Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

10) Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

3. Порядок генерации ЭП

3.1. Порядок генерации ЭП регламентируется соответствующим Регламентом Удостоверяющего центра.

3.2. Владельцы ЭП и ответственные исполнители ЭП (далее - Пользователь ЭП) назначаются распоряжением Ректора Университета.

3.3. Получение ЭП осуществляется на основании заявление сотрудника (Приложение 1), которое подается в управление информационных технологий, посредством электронного документооборота.

3.4. Пользователь, обладающий правом ЭП (ответственный исполнитель ЭП), вырабатывает самостоятельно или в сопровождении администратора информационной безопасности личный открытый ключ подписи, а также запрос на получение сертификата открытого ключа (в электронном виде и на бумажном носителе)

3.5.Хранить ЭП на носителях, используемых (флэшки, жесткие диски) совместно с рабочими файлами запрещается.

3.6. Не позднее, чем за 30 рабочих дней до окончания срока действия закрытого ключа, его пользователь обязан выполнить мероприятия по формированию новых закрытых ключей, соответствующего запроса на издание сертификата и оформить заявку на получение нового сертификата.

4. Порядок хранения и использования ЭП

4.1. Право доступа к рабочим местам с установленным программным обеспечением средств ЭП предоставляется только тем лицам, которые по приказу руководителя Университета назначены ответственными исполнителями ЭП и им предоставлены полномочия на эксплуатацию этих средств.

4.2. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками.

4.3. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним.

4.4. Владелец ЭП несет персональную ответственность за ключевой носитель своей ЭП и определяет режим ее хранения и транспортирования.

4.5. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

4.6. На технических средствах, оснащенных средствами ЭП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

4.7. Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства ЭП.

4.8. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется ЭП после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

4.9. Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

4.10. Носители ключевой информации относятся к материальным носителям, содержащим информацию ограниченного распространения и должны быть учтены по соответствующим учетным.

4.11. Формирование закрытых ключей подписи и шифрования производится на учтенные съемные носители информации.

4.12. Ни при каких обстоятельствах нельзя хранить ключи ЭП на жестких дисках АРМ.

4.13. В нерабочее время ключевые носители должны находиться в хранилище.

4.14. При необходимости временно покинуть помещение, в котором проводятся работы с использованием ЭП, ключевой носитель должен быть извлечен из компьютера.

4.15. Категорически не допускается:

• осуществлять несанкционированное копирование ключевых носителей;

• разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;

• использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭП, либо использовать ключевые носители на посторонних ПЭВМ;

• записывать на ключевые носители постороннюю информацию.

5. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

5.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним. Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство квалифицированной электронной подписи. Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

5.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий Злоумышленниками. Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам. Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами квалифицированной электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами. На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

5.3. Обеспечение безопасности АРМ с установленными средствами квалифицированной электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа

программными или аппаратными средствами межсетевого экранирования. На технических средствах, используемых для работы в информационных системах:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям безопасности ИС;
- должно быть установлено только лицензионное программное обеспечение;
- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;
- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);
- должны регулярно устанавливаться обновления операционной системы;
- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;
- должна быть активирована регистрация событий информационной безопасности;
- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства квалифицированной электронной подписи, журналы работы систем обмена электронными документами и так далее.

6. Порядок уничтожения ключей на ключевых носителях

6.1. Приказом ректора Университета должна быть создана комиссия по уничтожению ключевой информации.

6.2. Ключи должны быть выведены из действия и уничтожены в следующих случаях:

- плановая смена ключей;
- изменение реквизитов ответственного исполнителя (владельца) ЭП;
- компрометация ключей;
- выход из строя (износ, порча) ключевых носителей;
- прекращение полномочий пользователя ЭП.

6.3. Уничтожение ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) ключей без повреждения ключевого носителя. Ключи стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, Touch Memory, Rutoken и т.п.). Непосредственные действия по стиранию ключевой информации регламентируются эксплуатационной и технической документацией.

6.4 Ключи должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется актом (Приложение № 2) и отражается в соответствующих учетных формах.

7. Действия при компрометации ключей

7.1. Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

7.2. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

• потеря ключевых носителей;

• потеря ключевых носителей с последующим обнаружением;

• нарушение правил хранения и уничтожения (после окончания срока действия ключа);

• возникновение подозрений на утечку информации или ее искажение;

• нарушение печати на контейнере с ключевыми носителями;

• случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в т.ч. случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

7.3. При компрометации ключа пользователь немедленно прекращает обмен электронными документами с другими пользователями и извещает о факте компрометации.

7.4. По факту компрометации ключей должно быть проведено служебное расследование с оформлением уведомления о компрометации.

7.5. Факт компрометации закрытых ключей подписи должен быть подтвержден официальным уведомлением института в адрес Удостоверяющего центра о компрометации в письменном виде. Уведомление должно содержать идентификационные параметры сертификата, дату и время компрометации, характер компрометации, подпись владельца ключа подписи, подпись руководителя и печать института или его филиала.

7.6. Выведенные из действия скомпрометированные ключи уничтожаются, о чем составляется акт.

8. Права и обязанности Пользователя

8.1. Пользователь обязан:

а) хранить в тайне Ключ ЭП и Ключ проверки ЭП, ПИН-коды, принимать все возможные меры, предотвращающие нарушение их конфиденциальности;

б) использовать ЭП только в интересах Университета;

в) в случае нарушения конфиденциальности ЭП (Ключа проверки ЭП, PIN-кода) или ее утери незамедлительно уведомить об этом Администратора информационной безопасности;

г) при наличии оснований полагать, что конфиденциальность ЭП или Ключа проверки ЭП нарушена или такой Ключ и/или PIN-код скомпрометирован иным образом (утерян, похищен, отобран, передан третьему лицу), немедленно прекратить использование такого Ключа, самостоятельно или через

Администратора обратиться в выдавший его удостоверяющий центр для прекращения его действия;

д) не использовать ключи ЭП, если они используются или использовались ранее другими владельцами сертификатов ключей подписи;

е) строго соблюдать установленный порядок обращения с ключевой документацией;

ж) немедленно докладывать непосредственному начальнику и в подразделение безопасности об утрате средств ЭП, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о ставших ему известными попытках третьих лиц получить сведения о закрытых ключах, других фактах, которые могут привести к компрометации ключа ЭП, а также о причинах и условиях возможной утечки таких сведений.

8.2. Пользователь ЭП при работе с ключевыми документами обязаны руководствоваться положениями соответствующего Регламента Удостоверяющего центра и настоящим Положением.

8.3. В случае каких-либо изменений реквизитов ЭП (плановая смена ключей, изменение реквизитов владельцев или Ответственных исполнителей, генерация новой ЭП, и др.) в течении 3 суток Пользователь ЭП обязаны предоставить Администратору информационной безопасности уточненную информацию.

8.4. Ответственные исполнители ЭП обязаны выполнять требования Администратора информационной безопасности в части, касающейся обеспечения информационной безопасности Университета, его подразделений и филиалов.

9. Обязанности Администратора информационной безопасности.

9.1. Администратор информационной безопасности инструктирует пользователей по правилам обращения с ЭП.

9.2. Администратор информационной безопасности контролирует аппаратные средства и программные продукты, используемых для систем, в которых используются ЭП.

9.3. Администратор информационной безопасности осуществляет контроль за правильностью и своевременностью выполнения работ с ЭП.

9.4. При обнаружении фактов компрометации ключей или нарушений требований информационной безопасности при работе с ЭП администратор информационной безопасности письменно извещает руководителя организации.

Приложение 1

В Управление ИТ

Заявление

Я, _____

_____

(Фамилия, Имя, Отчество)

_____

_____

(должность, наименование подразделение)

прошу выпустить корпоративную электронную подпись на мое имя. Подтверждаю свое согласие на регистрацию сертификата ключа проверки корпоративной электронной подписи в системе электронного документа оборота «Технологический университет».

С положением о работе с электронной подписью «Технологического университета» ознакомлен.

«____»_____20___ _____ _____

(Дата) (Подпись) (Фамилия, И.О.)

Подтверждаю получение ключа корпоративной электронной подписи и сертификата ключа проверки корпоративной электронной подписи, выпущенных на мое имя Управлением ИТ , а так же отсутствие компрометации этого ключа.

«____»_____20___ _____ _____

(Дата) (Подпись) (Фамилия, И.О.)

Приложение 2

АКТ № _____ от «__» _____ 20__ г.
об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов

Комиссия _____ в составе:
(название организации)

_____
_

произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие средства криптографической защиты информации (СКЗИ).

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

Председатель комиссии

_____/_____