МИНОБРНАУКИ РОССИИ

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

ПРИКАЗ

17.07.2023 № 648-о

Об организации работ с электронной подписью

В целях приведения порядка пользования электронной подписью (далее – ЭП), в соответствии с требованиями Федерального Закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» п р и к а з ы в а ю:

1. Утвердить Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в ФГБОУ ВО «КНИТУ» (Приложение №1).

2. Утвердить Инструкцию пользователю средствами электронной подписи (Приложение №2).

3. Утвердить Регламент получения сертификата электронной подписи (Приложение №3).

4. Признать утратившим силу приказ от 21.08.2019 № 583-о «Об организации работ с электронной подписью».

5. Начальнику ЦКБ Филюкову В.Ю. организовать взятие на учет носителей ключевой информации, доведение указанных в настоящем приказе нормативных документов до пользователей ЭП и обучение работе со средствами криптографической защиты информации (при необходимости).

6. Назначить ведущего инженера-программиста ЦКБ Тупаева А.С. ответственным за учет и выдачу сертификатов и ключевых носителей ЭП, полученных в корпоративном центре регистрации (КЦР).

7. Назначить ведущего программиста ПФУ Рахамова С.А. ответственным за учет и выдачу сертификатов и ключевых носителей ЭП, полученных в удостоверяющем центре территориального отделения федерального казначейства.

8. Контроль за исполнением настоящего приказа возложить на проректора по РБ Муратова А.Х.

И.о. ректора Ю.М. Казаков

Приложение № 1
к приказу ФГБОУ ВО «КНИТУ»
от 17.07.2023 № 648-О

Руководство
по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи в ФБГОУ ВО «КНИТУ»

1. Общие положения

1.1. Настоящее руководство разработано в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи».

1.2. Руководство является средством официального информирования об условиях, рисках и порядке использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее - средства ЭП), а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи (далее – ЭП) в подразделениях ФГБОУ ВО «КНИТУ» (далее – КНИТУ).

1.3. Применение ЭП в государственных и иных информационных системах, а также в системах юридически значимого электронного документооборота, сопровождаются в том числе следующими рисками:

1) финансовые убытки (в том числе штрафы и т.п.);
2) репутационные риски;
3) нарушение сроков оказания государственных и муниципальных услуг;
4) нарушение правильного функционирования информационных систем.

Риски, связанные с применением ЭП, возникают вследствие возможности признания недействительности сделок, совершенных с использованием ЭП, недействительности документов, подписанных ЭП при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка ЭП.

1.4. В целях снижения рисков необходимо выполнение приведенных в настоящем руководстве организационно-технических и административных мер по обеспечению безопасного функционирования средств обработки и передачи информации. В соответствии с правилами функционирования информационных систем и систем обмена электронными документами, а также требованиями по эксплуатации средств ЭП могут быть установлены дополнительные требования по обеспечению их безопасной эксплуатации.

1.5. Ответственность за организацию безопасного использования средств ЭП и ЭП, выпущенные через корпоративный центр регистрации (далее – КЦР) удостоверяющего центра, возлагается на центр компьютерной безопасности (далее – ЦКБ).

1.6. Ответственность за организацию безопасного использования средств ЭП и ЭП, выпущенные через удостоверяющий центр территориального органа федерального казначейства (далее – УЦ ТОФК), возлагается на планово-финансовое управление (далее – ПФУ).

1.7. Ответственность за выполнение правил использования ЭП и средств ЭП возлагается на руководителей подразделений и исполнителей, допущенных к работе с ЭП.

2. Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями:

2.1. **Владелец сертификата ключа проверки электронной подписи** – лицо, которому в установленном Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ порядке выдан сертификат ключа проверки электронной подписи.

2.2. **Квалифицированная электронная подпись** – усиленная электронная подпись, соответствующая следующим признакам: получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после его подписания; ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

2.3. **Ключ электронной подписи** – уникальная последовательность символов, предназначенная для создания электронной подписи.

2.4. **Ключ проверки электронной подписи** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

2.5. **Ключевая информация** – ключи, предназначенные для формирования (проверки) электронной подписи, действующие в течение определенного срока.

2.6. **Ключевой носитель** – физический носитель с ключом электронной подписи, предназначенный для хранения ключевой информации, а при необходимости – контрольной, служебной и технологической информации.

2.7. **Корпоративный центр регистрации (КЦР)** – это веб-сервис для ускоренного выпуска сертификатов электронной подписи на рабочем месте организации. Позволяет сократить затраты и централизованно управлять процессом выдачи подписей

2.8. **Компрометация ключа** – несанкционированное копирование ключа или его разглашение (доведение) постороннему лицу, хищение, утрата ключевых носителей или иные события, когда местонахождение ключевых носителей неизвестна хотя бы временно.

2.9. **Владелец электронной подписи** – работник, назначенный приказом ректора, с установлением соответствующей ответственности и уполномоченный им использовать электронную подпись для подписания электронного документа.

2.10. **Ответственный за учет и выдачу сертификатов и ключевых носителей** – работник, отвечающий за учет и выдачу сертификатов и ключевых носителей.

2.11. **Пользователь сертификата ключа подписи** – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной подписи владельцу сертификата ключа подписи.

2.12. **Сертификат ключа проверки электронной подписи** – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

2.13. **Средства криптографической защиты информации (СКЗИ)** – программно-аппаратные средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения безопасности.

2.14. **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.

2.15. **Удостоверяющий центр (УЦ)** – 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 Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

2.16. **Управление ключами** – создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение, а также выдача и отзыв сертификатов ключей подписей в соответствии с политикой безопасности удостоверяющего центра.

2.17. **Электронный документ** – документ, в котором информация представлена в электронно-цифровой форме.

2.18. **Электронная подпись (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.

3. Требования к организации режима обеспечения безопасности помещений, в которых эксплуатируются средства квалифицированной электронной подписи

3.1. При эксплуатации средств ЭП должны быть реализованы меры, препятствующие возможности неконтролируемого использования посторонними лицами ключевых носителей ЭП. Указанные меры могут быть реализованы, в том числе, путем:

а) запрета на передачу ключевого носителя другим работникам и посторонним лицам;

б) оснащения помещений, где расположены автоматизированные рабочие места (АРМ) с установленными на них средствами криптозащиты, входными дверьми с замками, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений;

в) утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

3.2. В случае необходимости присутствия посторонних лиц в помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства обработки информации и передаваемую информацию.

3.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ

сохранность доверенных им документов и сведений, включая ключи электронной подписи.

4. Требования по защите информации от несанкционированного доступа средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

4.1. При использовании средств ЭП должны выполняться следующие меры по защите информации от несанкционированного доступа:

4.1.1. Необходимо применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии со следующими правилами:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– личный пароль пользователь не имеет права никому сообщать;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

4.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

– не использовать нестандартные, измененные или отладочные версии операционных систем;

– исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

– на средствах вычислительной техники с установленными средствами ЭП должна быть установлена только одна операционная система;

– все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

– необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

4.1.3. На средствах вычислительной техники необходимо:

– организовать стирание (по окончании сеанса работы средств электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы (с использованием программных средств Dallas Lock, Secret net или CCleaner). Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

– исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

– регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

4.1.4. В случае подключения технических средств с установленными средствами ЭП к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в т.ч. Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства ЭП и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства

защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

4.1.5. Необходимо организовать и использовать:

– систему аудита, организовать регулярный анализ результатов аудита.

– комплекс мероприятий по антивирусной защите.

4.2. Запрещается:

– осуществлять несанкционированное копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– вносить какие-либо изменения в программное обеспечение средств ЭП;

– работать со средствами электронной подписи при включенных в техническое средство штатных средствах выхода в радиоканал;

– записывать на ключевые носители постороннюю информацию;

– оставлять средства вычислительной техники с установленными средствами ЭП без контроля после ввода ключевой информации;

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

– удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

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

5.1. Меры защиты ключей ЭП.

Ключи ЭП при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством ЭП согласно технической и эксплуатационной документации к ним.

Ключи ЭП на ключевом носителе должны быть защищены паролем (ПИН-кодом).

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 системах обмена электронными документами, по электронной почте сети Интернет или по внутренней электронной почте (кроме файлов квалифицированных сертификатов ключей проверки электронной подписи).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB- flash накопитель, e-Token, Рутокен, ESMART Token и др.). Размещение ключевой информации в реестре Windows, на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами ЭП способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя и недоступном для посторонних лиц месте.

Носитель ключевой информации должен подключаться в считывающее устройство только на время выполнения средствами электронной подписи операций формирования и проверки ЭП, 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 средств вычислительной техники с установленными средствами ЭП

С целью контроля исходящего и входящего подозрительного трафика, средства вычислительной техники с установленными средствами ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку во внешние сети информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

– на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3;

– 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 ЭП третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

– должна быть активирована подсистема регистрации событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного работника с рабочего места.

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук, планшет). Если выбран переносной компьютер, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

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

6. Порядок учета, хранения, обращения сертификатов ключей проверки электронной подписи и ключевых носителей

6.1. Организация учета, хранения ключевых носителей, порядок обращения с ними является составной частью обеспечения безопасности информационного обмена электронными документами по телекоммуникационным каналам связи.

6.2. В КНИТУ функции организации учета и выдачи ключевых носителей владельцам ЭП, возлагаются на ЦКБ.

Регистрация сертификатов ключей проверки электронной подписи и ключевых носителей, а также выдача ключевых носителей, выполняется работником, ответственным за учет и выдачу сертификатов и ключевых носителей в «Журнале регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей».

6.3. За хранение ключевых носителей отвечает лично владелец ключевого носителя.

6.4. Подразделение КНИТУ, в котором существует необходимость использования в процессе работы ЭП, организует работу по получению ЭП, в соответствии с Регламентом получения сертификата электронной подписи (приложение №3).

6.5. На ключевые носители наносятся учетные атрибуты: название организации, учетный номер, дата постановки на учет, владелец ключа, краткое наименование подразделения КНИТУ и подпись ответственного за учет ЭП. Если учетные атрибуты невозможно разместить на ключевом носителе из-за маленьких размеров, то они наносятся несмывающимся фломастером на пластмассовой или прочной картонной бирке, прикрепляемой к корпусу носителя любым доступным способом, не повреждающим носитель.

Пример:

Уч. № 001 – кт от 15.01.2019 Иванов Иван Иванович Диссертационный совет (подпись ответственного за учет сертификатов ЭП)

6.6. Ключи электронной подписи с истекшими сроками действия и утратившими свою практическую надобность отзываются и уничтожаются отделом, ответственным за учёт и выдачу сертификатов ЭП с соответствующей отметкой в «Журнале регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей». Уничтожение ключей должно выполняться путем надежного стирания ключей без повреждения ключевого носителя.

6.7. Владельцы ЭП и ответственные за организацию электронного документооборота (далее – ЭД) несут персональную ответственность за соответствие информации, содержащейся в документах на бумажном носителе и в ЭД, за правильность подписания ЭП, передаваемых по системе ЭД.

6.8. Владелец ЭП обязан:

- выполнять требования соответствующих инструкций по эксплуатации используемой системы ЭД;

- исполнять требования настоящего Руководства;

- пройти инструктаж под роспись в «Журнале доведения инструкций по обращению с СКЗИ, действиях лиц, допущенных к работе в информационных системах»;

- хранить ключевые носители с ключом ЭП в недоступном для посторонних лиц месте;

- контролировать отправку и получение ЭД;

- осуществлять взаимодействие по вопросам обмена ЭД с организаторами системы;

- использовать ключевые носители с ключом ЭП только на момент необходимости использования в системе электронного документооборота;

- прекратить работу на рабочей станции в случае: аппаратно-программных сбоев в работе, приводящих к самопроизвольным перезагрузкам, и иных признаков несанкционированных действий с системой и сообщить об этом руководителю подразделения и в ЦКБ (если сертификат ЭП был выпущен в КЦР через ЦКБ) или в ПФУ (если сертификат ЭП был выпущен в ТОФК через ПФУ);

- при оповещении об окончании срока действия ЭП, своевременно докладывать в ЦКБ (если сертификат ЭП был выпущен в КЦР через ЦКБ) или в ПФУ (если сертификат ЭП был выпущен в ТОФК через ПФУ) о получении данного типа сообщения;

- участвовать в плановых и внеплановых проверках на наличие ключевых носителей с закрытым ключом ЭП и порядка обращения с ними.

Запрещается:

– разглашать используемые для работы значения паролей и ключевых фраз;

– оставлять без присмотра ключевые носители с ключом ЭП на столах, в незапертых ящиках столов и других открытых хранилищах, даже временно, при выходе из рабочего помещения;

– создавать копии ключевого носителя, распечатывать и переписывать с носителя информацию на иной носитель;

– изменять информацию, находящуюся на ключевом носителе;

– пользоваться скомпрометированными ключами ЭП и неисправными ключевыми носителями;

– совершать действия, которые могут привести в негодность ключевой носитель или записанную на нем информацию.

6.9. На руководителя подразделения КНИТУ, в котором используется ЭП, возлагаются следующие обязанности:

– подготовка, участие и актуализация локальных нормативных актов о назначении ответственных за использование ЭП, организацию обмена ЭД;

– осуществление контроля за соблюдением работниками подразделения установленного порядка обмена информацией в системе ЭД, соответствием переданных электронных документов подписанных ЭП и оформленных в установленном порядке документов в бумажном виде;

– организация получения сертификатов ключа проверки ЭП на соответствующих лиц при внедрении новой системы ЭД и при истечении срока действия действующих сертификатов;

– принятие своевременных мер по организации устранения нарушений в функционировании используемой системы ЭД, а также в случае компрометации ключевой информации.

6.10. На работника, ответственного за учет и выдачу сертификатов и ключевых носителей, возлагаются следующие обязанности:

- проведение инструктажа под роспись в «Журнале доведения инструкций по обращению с СКЗИ, действиях лиц, допущенных к работе в информационных системах»;

- организация учета и выдачи ответственным за использование ЭП ключевых носителей с ключом ЭП;

- своевременное ведение записей в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов», в журналах и книгах учета группы криптографической защиты;

- контроль за сроком действия ЭП и обеспечения своевременного переоформления сертификатов ключей проверки ЭП и ключевых носителей по окончании срока их действия, а также в случае замены лиц, имеющих право подписи;

- контроль выполнения требований безопасности при использовании ключевых носителей, исключающих несанкционированный доступ к ним посторонних лиц;

- организация и контроль своевременного сопровождения программного и технического обеспечения рабочего места системы ЭД;

- организация своевременных мер по устранению выявленных нарушений в функционировании с используемой системой ЭД, а также в случае компрометации ключевой информации;

- проведение плановых (не реже одного раза в квартал) и внеплановых проверок наличия ключевых носителей с ключом ЭП и порядка обращения с ними;

- принятие своевременных мер по организации устранения нарушений в функционировании используемой системы ЭД, а также в случае

компрометации ключевой информации.

7. Действия при компрометации ключей квалифицированной электронной подписи

7.1. К событиям, относящимся к компрометации ключей ЭП, относятся следующие ситуации:

1) ознакомление неуполномоченного лица (лиц) с ключами ЭП;

2) утрата ключевого носителя с ключами ЭП;

3) увольнение пользователя ключа ЭП;

4) нарушение целостности хранилища ключевой информации;

5) утрата хранилища ключевой информации в случае нахождения в них ключевых носителей;

6) случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника, утрата ключевого носителя с последующим обнаружением).

7.2. В случае компрометации ключей ЭП владелец квалифицированного сертификата ключа проверки электронной подписи должен:

1) прекратить использование ключа квалифицированной электронной подписи и соответствующего квалифицированного сертификата ключа проверки электронной подписи;

2) незамедлительно обратиться к ответственному за учет ЭП для передачи информации в Удостоверяющий центр в целях аннулирования (прекращения действия) соответствующего квалифицированного сертификата ключа проверки электронной подписи и получения (при необходимости) нового квалифицированного сертификата ключа проверки электронной подписи в соответствии с Регламентом оказания услуг Удостоверяющего центра.

Приложение № 2
к приказу ФГБОУ ВО «КНИТУ»
от 17.07.2023 № 648-О

Инструкция
пользователя средствами электронной подписи

1. Общие положения

1.1. Настоящая Инструкция разработана для работников ФГБОУ ВО «КНИТУ» (далее – КНИТУ) осуществляющих электронное взаимодействие со сторонними организациями с использованием средств электронной подписи (ЭП).

1.2. Основные термины:

1.2.1 **Компрометация ключевой информации** – утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации НКИ или любые другие ситуации, при которых достоверно не известно, что произошло с НКИ. К компрометации ключевой информации также относится увольнение работников, имевших доступ к ключевой информации.

1.2.2 **Корпоративный центр регистрации (КЦР)** – веб-сервис для ускоренного выпуска сертификатов электронной подписи на рабочем месте организации. Позволяет сократить затраты и централизованно управлять процессом выдачи подписей.

1.2.3 **Машиночитаемая доверенность (МЧД)** – электронная форма бумажной доверенности, подписанная квалифицированной электронной подписью (КЭП) руководителя организации или индивидуального предпринимателя. Создается и представляется в файле формата XML.

1.2.4 **Носитель ключевой информации (НКИ)** – носитель информации (дискета, флэш-память, и прочие носители) на которых храниться электронный ключ, предназначенный для защиты электронных взаимодействий.

1.2.5 **Открытый (публичный) ключ подписи** – ключ, автоматически формируется при изготовлении секретного ключа подписи и однозначно зависящий от него. Открытый ключ предназначен для проверки корректности электронной подписи электронного документа. Открытый ключ считается принадлежащим участнику электронных взаимодействий, если он был сертифицирован (зарегистрирован) установленным порядком.

1.2.6 **Секретный (закрытый) ключ подписи** – ключ, предназначенный для формирования им электронной подписи электронных документов.

1.2.7 **Территориальный орган федерального казначейства (ТОФК)** – федеральный орган исполнительной власти, осуществляющий в соответствии с законодательством Российской Федерации правоприменительные функции по обеспечению исполнения федерального бюджета, кассовому обслуживанию

исполнения бюджетов бюджетной системы Российской Федерации, предварительному и текущему контролю за ведением операций со средствами федерального бюджета главными распорядителями, распорядителями и получателями средств федерального бюджет

1.2.8 **Удостоверяющий центр (УЦ)** – 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 Федеральным законом «Об электронной подписи» от 06.04.2011 № 63 ФЗ.

1.2.9 **Шифрование** – специализированный метод защиты информации от ознакомления с ней третьих лиц, основанный на кодировании информации по алгоритму ГОСТ 28147-89 с использованием соответствующих ключей.

1.2.10**Электронная подпись (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. Организация работы с НКИ средств ЭП

2.1. Лица, имеющие доступ к НКИ, несут за нее персональную ответственность. Список лиц, получивших сертификат ЭП установленным порядком ведется Центром компьютерной безопасности (далее – ЦКБ).

2.2. ЦКБ проводит обучение и инструктаж ответственных работников подразделений, участвующих в электронном взаимодействии со сторонними организациями с помощью ЭП и средств криптографической защиты информации (далее – СКЗИ).

2.4. Контроль за использованием НКИ осуществляют руководители подразделений.

3. Порядок учета и использования НКИ средств ЭП

3.1. Учет НКИ средств ЭП

Ключи и сертификаты ЭП маркируются и учитываются в «Журнале регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей» (ведется в ЦКБ) и выдаются ответственному лицу под подпись в этом журнале.

НКИ должны иметь соответствующие бирки, на которых отражается: ограничительный гриф, наименование организации, регистрационный номер носителя (по «Журналу регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей»), дата постановки на учет, владелец ключа, краткое наименование подразделения и подпись ответственного за учет сертификатов ЭП.

3.1.2. Порядок использования НКИ

Каждому работнику (исполнителю), которому в соответствии с матрицей доступа или приказом ректора предоставлено право постановки на электронный документ ЭП, выдается персональный НКИ, на который записана уникальная ключевая информация («секретный ключ ЭП»), относящаяся к категории сведений ограниченного распространения, и МЧД.

Персональные НКИ пользователь должен хранить недоступном для посторонних лиц месте.

НКИ извлекаются исполнителями из места хранения только на время работы с НКИ.

МЧД хранится в информационной системе, где происходит подписание документов.

Работник может отправлять МЧД двумя способами:

а) отдельным файлом вместе с пакетом подписанных документов. Тогда сотрудник находит файл доверенности в архиве системы, прикрепляет его к подписанным документам и отправляет.

б) указать только номер МЧД, хранящейся в сторонней системе. Такая система не только хранит МЧД, но и передает информацию из них в общую базу доверенностей. Поэтому отправлять сам файл доверенности не нужно — получатель документов введет номер МЧД и узнает необходимые данные.

Получатель машиночитаемой доверенности может проверить:

а) срок действия доверенности;

б) полномочия сотрудника, указанные в МЧД;

в) электронную подпись директора, которой подписана МЧД.

4. Обязанности и права пользователя НКИ

4.1. Обязанности пользователя НКИ

4.1.1. Пользователь, которому в соответствии с его должностными функциями предоставлено право постановки на электронный документ ЭП, несет персональную ответственность за сохранность и правильное использование вверенной ему ключевой информации и содержание документов, на которых стоит его ЭП.

Пользователь НКИ **ОБЯЗАН**:

– под подпись в «Журнале регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей» получить НКИ, убедиться, что она правильно маркирована и на ней установлена защита от записи.

– пройти инструктаж под подпись в «Журнале доведения инструкций по обращению с СКЗИ, действиях лиц, допущенных к работе в информационных системах»

– осуществлять хранение НКИ в недоступном для посторонних лиц месте.

– использовать для работы только рабочий НКИ.

– прекратить работу на рабочей станции в случае аппаратно - программных сбоев в работе, приводящих к самопроизвольным

перезагрузкам, и иных признаков несанкционированных действий с системой и сообщить об этом руководителю подразделения и в ЦКБ (если сертификат ЭП получен в КЦР через ЦКБ) или ПФУ (если сертификат ЭП получен в УЦ ТОФК через ПФУ)

– подписывать документы организации новым типом электронной подписи — ЭП физлица (в ней нет данных организации). Чтобы подтвердить полномочия, сотрудник должен приложить к документам МЧД.

– после использования НКИ ЭП для подписи исполнитель должен убрать НКИ в недоступное для посторонних лиц место.

– по окончании рабочего дня убрать НКИ в недоступное для посторонних лиц место.

– в случае порчи НКИ (например при ошибке чтения) исполнитель обязан передать его уполномоченному работнику ЦКБ (если сертификат ЭП был выпущен в КЦР) и ПФУ (если сертификат ЭП были выпущен в УЦ ТОФК), который должен сделать новый НКИ и выдать ее исполнителю взамен старой (испорченной).

– испорченный НКИ должен быть уничтожен установленным порядком путем надежного удаления информации с носителя в присутствии исполнителя. Все эти действия должны быть зафиксированы в «Журнале регистрации и учета сертификатов ключей проверки электронной подписи и ключевых носителей».

– на период временного отсутствия (отпуск, командировка и т.п.) поместить ключевые носители недоступное для посторонних лиц место.

– при оповещении об окончании срока действия ЭП, своевременно докладывать в ЦКБ (если сертификат ЭП получен в КЦР через ЦКБ) или ПФУ (если сертификат ЭП получен в УЦ ТОФК через ПФУ) о получении данного типа сообщения.

4.1.2. Пользователю носителей ключевой информации **ЗАПРЕЩАЕТСЯ:**

– оставлять персональный ключевой носитель без личного присмотра где бы то ни было;

– оставлять ключевой носитель ЭП в компьютере;

– передавать персональный НКИ другим лицам (кроме как для хранения руководителю подразделения в опечатанном пенале);

– делать копии НКИ, распечатывать или переписывать с нее файлы на иной НКИ информации (например, жесткий диск ПЭВМ), снимать с НКИ защиту от записи, вносить изменения в файлы, находящиеся на НКИ, хранить на НКИ иную информацию (в том числе рабочие или личные файлы);

– использовать персональный НКИ на заведомо неисправной ПЭВМ;

– подписывать своим персональным «секретным ключом ЭП» любые электронные сообщения и документы, кроме тех видов документов, которые определены матрицей полномочий по доверенностям или приказами ректора о наделении правом электронной подписи.

4.2. Права пользователя НКИ

Пользователь имеет право обращаться в ЦКБ (если сертификат ЭП был выпущен в КЦР) и ПФУ (если сертификат ЭП были выпущен в УЦ ТОФК) за консультациями по вопросам использования НКИ и по вопросам обеспечения информационной безопасности технологического процесса.

Пользователь имеет право требовать от своего непосредственного руководителя создания необходимых условий для выполнения перечисленных выше требований.

Пользователь имеет право представлять свои предложения по совершенствованию мер защиты на своем участке работы.

5. Порядок действий при компрометации НКИ

К событиям, связанным с компрометацией ключевой информации, должны быть отнесены следующие события:

- утрата НКИ;
- утрата НКИ с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажения в системе связи;
- невозможность расшифровки входящих или исходящих сообщений у абонентов.

Первые три события должны трактоваться как безусловная компрометация действующих ключей ЭП. Два следующих события требуют специального рассмотрения в каждом конкретном случае. При компрометации ключей ЭП пользователь немедленно:

- прекращает передачу информации с использованием скомпрометированных ключей ЭП;
- сообщает о факте компрометации в ЦКБ (если сертификат ЭП был выпущен в КЦР) или ПФУ (если сертификат ЭП были выпущен в УЦ ТОФК).

Если у работника больше нет полномочий подписывать документы организации или его полномочия изменились, ректор может отозвать машиночитаемую доверенность.

Приложение № 3
к приказу ФГБОУ ВО «КНИТУ»
от 17.07.2023 № 648-О

Регламент
получения сертификата электронной подписи

1. ЭП оформляется работникам, включенным в «Матрицу полномочий по доверенностям».

В случае, если работник не включен в «Матрицу полномочий по доверенностям», но, получение ЭП вызвано служебной необходимостью, руководитель подразделения представляет на имя ректора служебную записку о необходимости получения ЭП. В служебной записке необходимо отразить следующую информацию: фамилия, имя, отчество, должность, назначение ЭП (для какой системы электронного документооборота предназначена ЭП), какие электронные документы будут подписываться ЭП. Служебная записка должна быть согласована с курирующим проректором, проректором по режиму и безопасности, управлением кадров и документационного обеспечения и правовым управлением и центром компьютерной безопасности.

2. Оформление сертификата электронной подписи (далее – сертификат ЭП) для работников через корпоративный центр регистрации (далее – КЦР) организует центр компьютерной безопасности.

3. Оформление сертификата ЭП (для ректора, отдельных работников бухгалтерии, работников отделов закупок и работников ПФУ) для подписания финансовых документов через территориальный орган Федерального казначейства (далее – ТОФК) организует ведущий программист планово-финансового управления КНИТУ.

4. Работник ЦКБ, на которого возложены полномочия администратора корпоративного центра регистрации (далее – администратор КЦР), запрашивает у оформляемого работника данные (цветной скан паспорта, СНИЛС и ИНН), необходимые для создания личного кабинета оформляемого работника в удостоверяющем центре.

В обязательном порядке администратор КЦР в ходе личного общения с оформляемым работником осуществляет сверку представленных копий документов с их оригиналами.

5. ЦКБ в течение пяти рабочих дней формирует заявку о создании личного кабинета в сервисе удостоверяющего центра «Корпоративный центр регистрации» (далее – личный кабинет) для получения (продления) сертификата электронной подписи.

6. Оформляемый работник после получения от администратора КЦР данных для аутентификации в личном кабинете, загружает копии всех необходимых документов (паспорт, СНИЛС, ИНН, заявление на выдачу сертификата электронной подписи, доверенность) в свой личный кабинет удостоверяющего центра (при необходимости, данную операцию может выполнить администратор КЦР в присутствии оформляемого работника).

7. Личный кабинет автоматически рассмотрит заявку на получение ЭП и в срок, не превышающий трех суток, оповестит администратора КЦР об изготовленном сертификате.

8. Администратор КЦР после получения сертификата электронной подписи, и его записи на ключевой носитель, ставит на учет ключевые носители и сертификаты в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов», под подпись в этом журнале выдает работнику ключевой носитель и доводит требования приказа «Об организации работ с электронной подписью» под роспись до работника.

9. Ведущий программист ПФУ, на которого возложены полномочия ответственного за учёт сертификатов ЭП, выданных в ТОФК, после получения подтверждения от ЦКБ об обоснованности оформления ЭП, запрашивает у работника, которому оформляется сертификат ЭП (далее - оформляемый работник), данные (данные паспорта, ИНН, СНИЛС и доверенность по форме казначейства), необходимые для формирования запроса на сертификат ЭП.

После рассмотрения оформляемый работник лично приходит в ТОФК с паспортом и получает сертификат ЭП.

10. После получения сертификата электронной подписи в ТОФК, и его записи на ключевой носитель владелец ЭП обязан прибыть в ЦКБ для постановки ЭП на учет и ознакомления с приказом ректора «Об организации работ с электронной подписью» под роспись и получения инструктажа о порядке работы с СКЗИ.