ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение города Москвы «Колледж малого бизнеса № 4»

Дубининская улица, д. 25, стр. 1, Москва,115054
Телефон: (499) 235-52-94 Факс: (499) 235-52-94 E-mail: spo-4@edu.mos.ru http://www.kmb-4.mskobr.ru
ОКПО 75587448, ОГРН 1057705001970, ИНН / КПП 7705513678 / 770501001

УТВЕРЖДАЮ
Директор ГБПОУ КМБ № 4

Т.П. Антонова
17.01.2018 г.

ПОЛОЖЕНИЕ

О ПРАВИЛАХ ИСПОЛЬЗОВАНИЯ И ХРАНЕНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

(далее – «Положение»)

Номер в перечне локальных актов	Срок действия	Количество листов	Разработчик	
			Фамилия, инициалы	Должность
№ 5.6., приложение к приказу № 01-10/7/1 от 17.01.2018 г.	5 лет	15	Ращупкина Е. В. Фролов А.Е.	Главный бухгалтер Педагог-организатор

1. Настоящее Положение о Правилах использования и хранения электронной подписи в Государственном бюджетном профессиональном образовательном учреждении города Москвы «Колледж малого бизнеса №4» (далее - Колледж) разработано в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Термины определения

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.

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

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;

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, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

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

Аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего Федерального закона;

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;

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

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а

также граждане;

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

3. Общие положения

3.1. Принципами использования электронной подписи являются:

- право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

- возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

- недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

3.2. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

3.3. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия.

3.4. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ **должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.**

3.5. Если федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами предусмотрено, что документ должен подписываться несколькими лицами, электронный документ должен быть подписан лицами (уполномоченными должностными лицами органа, организации), изготовившими этот документ, тем видом подписи, который установлен законодательством Российской Федерации для подписания изготовленного электронного документа электронной подписью.

3.6. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов. Исключение составляют случаи, когда в состав пакета электронных документов лицом, подписавшим пакет, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные ими тем видом электронной подписи, который установлен законодательством Российской Федерации для подписания таких документов. В этих случаях электронный документ, входящий в пакет, считается подписанным лицом, первоначально создавшим такой электронный документ, тем видом электронной подписи, которым этот документ был подписан при создании, вне зависимости от того, каким видом электронной подписи подписан пакет электронных документов.

3.7. Срок действия ЭП указан в сертификате.

3.8. По истечении этого срока владельцу ЭП необходимо провести плановую смену ЭП в Удостоверяющем центре.

3.9. Использование ЭП в конкретной информационной системе (программе) определяется руководством по эксплуатации данной системы (программы).

4. Использование простой электронной подписи

4.1. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

- простая электронная подпись содержится в самом электронном документе;
- ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

4.2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

- правила определения лица, подписывающего электронный документ, по его простой электронной подписи;
- обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

4.3. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

5. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

5.1. При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

5.2. Для работы с ЭП в качестве пользователя привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации.

Работу с ключами ЭП и шифрования координирует администратор безопасности. Должностные лица, уполномоченные соответствующим приказом руководителя организации, могут эксплуатировать получать и использовать ключи шифрования и ЭП, несут персональную ответственность за:

· сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы;

· сохранение в тайне содержания закрытых ключей ЭП;

· сохранность носителей ключевой информации.

5.3. В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

5.4. Для обеспечения безопасности ЭП Пользователя, необходимо:

1) хранить ключи ЭП на специальных защищенных носителях – электронных идентификаторах с использованием надежного пароля.

2) обеспечить надежное хранение носителей ключевой информации, исключающее доступ к ним посторонних лиц, не передавать сами носители лицам, к ним не допущенным;

3) вставлять ключевой носитель при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.);

4) не записывать на ключевой носитель постороннюю информацию;

5) не вносить какие-либо изменения в программное обеспечение и средств ЭП;

6) не использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования.

6. Проверка электронной подписи

Для создания и проверки электронной подписи используются средства ЭП, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

При проверке электронной подписи средства ЭП должны:

3) показывать содержимое электронного документа, подписанного электронной подписью;

4) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

5) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы. Пользователь может осуществлять проверку ЭП как с помощью используемых средств ЭП, так и обратившись в Удостоверяющий центр. Процедура проверки ЭП в электронном документе в Удостоверяющем центре описана в Регламенте оказания услуг Удостоверяющего центра, опубликованного на сайте ca.citvo.ru.

7. Уничтожение ключевой информации

После прекращения действия ключей ЭП пользователь должен удалить их путем форматирования ключевого носителя. Инструкцию по форматированию конкретного ключевого носителя необходимо скачать с сайта производителя.

8. Плановая замена ключей и сертификатов ключей

Плановая смена ключей и сертификатов открытых ключей осуществляется за месяц до окончания срока действия имеющихся ответственным лицом организации пользователя.

9. Внеплановая замена ключей и сертификатов ключей

Внеплановая замена ключей и сертификатов закрытых ключей проводится в следующих случаях:

1. Компрометация ключей;

2. Изменение идентификационных данных и/или областей использования ключа, указанных в заявлении на изготовление ключей;

3. Выход из строя ключевого носителя.

К событиям, относящимся к компрометации ключей, относятся следующие ситуации:

1) утрата ключевых носителей ключа;

2) утрата носителей ключа с последующим обнаружением;

3) увольнение сотрудников, имевших доступ к ключевой информации;

4) возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

5) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

7) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

8) доступ посторонних лиц к ключевой информации.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя.

Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет организация, в которой работает Пользователь.

При компрометации ключа пользователь должен немедленно поставить в известность Удостоверяющий центр о факте компрометации ключей, сообщив номер сертификата.

В течение 30 минут после поступления сообщения о компрометации ключа, действие его будет приостановлено до подачи в Удостоверяющий центр письменного заявления об аннулировании скомпрометированных ключей. Возобновление работы с ЭЦП будет возможно только после замены скомпрометированных ключей.

10. Эксплуатация и хранение электронного ЭП

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

В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания.

2. 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.

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

4. 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.

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

6. Ответственные исполнители ЭП обязаны вести журнал учета хранения электронных носителей конфиденциальной информации и своевременно заполнять его (см. Приложение №1).

7. Закрытые ключи изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя.

8. При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом администратора безопасности.

9. Категорически не допускается:

- осуществлять несанкционированное администратором безопасности 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. Для нормальной работы носителя ЭЦП, необходимо придерживаться следующих правил эксплуатации и хранения:

1. Не разбирать электронный идентификатор, это ведет к потере гарантии! Кроме того, при этом возможна поломка корпуса электронного идентификатора, поломка элементов печатного монтажа и т. д.

2. Оберегать электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), воздействия высоких и низких температур, агрессивных сред, высокого напряжения.

3. Не прилагать излишних усилий при подсоединении электронного идентификатора к порту компьютера.

4. Не допускать попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема электронного идентификатора принять меры для его очистки. Для очистки корпуса и разъема использовать сухую ткань. Использование органических растворителей недопустимо.

5. В случае неисправности или неправильного функционирования электронного идентификатора обращаться в Удостоверяющий центр.

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие:

– Потеря ключевых носителей.

– Потеря ключевых носителей с их последующим обнаружением.

– Увольнение сотрудников, имевших доступ к ключевой информации.

– Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа.

– Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

– Нарушение печати на сейфе с ключевыми носителями.

–Случаи, когда нельзя 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).

1. Порядок действий пользователя

Автоматизированное рабочее место пользователя Системы использует СКЗИ для обеспечения целостности, авторства и конфиденциальности информации, передаваемой в рамках информационной системы.

Порядок обеспечения информационной безопасности при работе в Системе определяется организацией, подключающейся к Системе, на основании действующего российского законодательства в области защиты информации.

Владелец сертификата ключа обязан:

- Не использовать для электронной цифровой подписи и шифрования открытые и закрытые ключи, если ему известно, что эти ключи используются или использовались ранее.
- Хранить в тайне закрытый ключ.
- Немедленно требовать приостановления действия сертификата ключа при наличии

оснований полагать, что тайна закрытого ключа нарушена (компрометация ключа).

- Обновлять сертификат ключа подписи в соответствии с установленным регламентом.

2. Рекомендуемые организационно-технические меры по обеспечению информационной безопасности в организации

Для хранения носителей закрытых ключей ЭЦП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).

Использовать АРМ со встроенными средствами криптографической защиты в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях при невозможности использования парольной защиты, допускается загрузка ОС без запроса пароля. При этом должны быть реализованы дополнительные организационно-режимные меры, исключающие несанкционированный доступ к этим АРМ.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ со встроенными СКЗИ.

Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными СКЗИ.

Администрирование должно осуществляться доверенными лицами.

В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭЦП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

Список работников,

допущенных к работе с ключами средств криптографической защиты информации

Список составлен «____» _____ 201__ г.

_____/Должность,

отдел(подразделение)/

_____ / ФИО должностного лица /

№ п/п	Наименование СКЗИ	Должность работника	Ф.И.О. работника	Информационная система, в которой применяется СКЗИ	Подпись работника
1					
2					
3					
4					
5					
6					

Приложение

Журнал учета криптографических ключей

Журнал начат «____» _____ 201__ г. Журнал завершен «____» _____ 201__г.

_____ /Должность/ _____ /Должность/

_____ / ФИО должностного лица /_____ / ФИО должностного лица /

На _____ листах

№ п/п	Номера экземпляров (криптографичес-кие номера) ключевых документов	Номера серий криптогра-фических ключей	Наименование СКЗИ	От кого получены	Дата и номер сопроводительного письма, приказа, списка.	Ф.И.О. пользователя	Дата получения ключей	Дата уничтожения ключей	Ф.И.О. пользователя СКЗИ, производившего уничтожение	Номер акта или расписка об уничтожении

Журнал учета носителей персональных данных

Журнал начат «____» _____ 201__ г. Журнал завершен «____» _____ 201__г.

_____ /Должность/ _____ /Должность/

_____ / ФИО должностного лица /_____ / ФИО должностного лица /

На _____ листах

№ п/п	Регистра-ционный номер	Дата учета	Тип/емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположе-ние носителя	Сведения об уничтожении носителя /стирании информации
1								
2								
3								
4								
5								

Журнал учета средств защиты информации

Журнал начат «____» _____ 201__ г. Журнал завершен «____» _____ 201__г.

_____ /Должность/ _____ /Должность/

_____ / ФИО должностного лица /_____ / ФИО должностного лица /

На _____ листах

№ п/п	Наименование СЗИ	Регистрационный номер СЗИ	От кого получены (источник)	Дата и номер сопроводительного письма и/или лицензии	Ф.И.О. пользователя СЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Аппаратные средства, на которые установлены или к которым подключены СЗИ	Дата изъятия (удаления) СЗИ	Ф.И.О. пользователя СЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об удалении	Примечание

Журнал учета средств криптографической защиты информации

Журнал начат «____» _____ 201__ г. Журнал завершен «____» _____ 201__г.

_____ /Должность/ _____ /Должность/

_____ / ФИО должностного лица /_____ / ФИО должностного лица /

На _____ листах

№ п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	От кого получены (источник)	Дата и номер сопроводительного письма и/или лицензии	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Аппаратные средства, на которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	Примечание

Журнал учета съемных носителей персональных данных

Журнал начат «____» _____ 201__ г. Журнал завершен «____» _____ 201__г.

_____ /Должность/ _____ /Должность/

_____ / ФИО должностного лица /_____ / ФИО должностного лица /

На _____ листах

№ п/п	Регистрационный номер	Фамилия, должность исполнителя	(Получил, вернул, передал)	Дата последнего изменения информации	Подпись исполнителя	Примечание
1						
2						
3						
4						
5						