Удостоверяющий центр
КГБУЗ «МЕДИЦИНСКИЙ ЦЕНТР– УПРАВЛЯЮЩАЯ КОМПАНИЯ АЛТАЙСКОГО МЕДИЦИНСКОГО КЛАСТЕРА»

РУКОВОДСТВО

по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи

Серийный номер сертификата	
Серийный номер носителя	
Владелец сертификата	
Название средства электронной подписи	**СКЗИ "ViPNet CSP 4.2"**

Барнаул 2018

Уважаемый Пользователь!

В данном руководстве содержатся рекомендации по обеспечению безопасности при использовании средств квалифицированной электронной подписи, Владельцем которых Вы теперь являетесь, и квалифицированного сертификата ключа проверки электронной подписи, выпущенного на Ваше имя.

Пожалуйста, ознакомьтесь с рекомендациями по обеспечению безопасности и постарайтесь их соблюдать!

Квалифицированный сертификат является Вашим цифровым удостоверением в электронном мире. С помощью него Вы можете формировать квалифицированную электронную подпись на электронных документах при совершении гражданско-правовых сделок, получении государственных и муниципальных услуг и других юридически значимых действиях.

Согласно федеральному законодательству информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью (п.1 ст.6 Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»), поэтому, любой электронный документ, на котором будет стоять Ваша квалифицированная электронная подпись, будет иметь такую же юридическую силу, как если бы Вы подписали данный документ на бумаге.

Ваш квалифицированный сертификат записан на ключевой носитель. Обращайтесь с ним очень бережно, также как Вы обращаетесь с банковской картой или паспортом. Также, как и банковская карта контейнер с ключевой информацией квалифицированного сертификата оснащен паролем для обеспечения безопасности. Ни в коем случае не передавайте носитель и не сообщайте пароль третьим лицам.

Если носитель и пароль попадут к злоумышленникам, все документы, которые будут подписаны ими с его помощью с целью извлечения собственной выгоды, будут считаться подписанными от Вашего имени и порождать для Вас юридическую ответственность. Поэтому, в случае утери или кражи носителя Вам необходимо как можно быстрее принять меры по приостановлению действия (или отзыву) Вашего квалифицированного сертификата. Для этого Вам нужно оповестить свой Удостоверяющий центр одним из следующих способов:

1) по телефону + 7 (3852) 555-471;
2) по электронной почте mcuc@zdravalt.ru

Сотрудники удостоверяющего центра оперативно проконсультируют Вас по дальнейшим действиям. Только после аннулирования (отзыва) или приостановления действия квалифицированного сертификата можно осуществлять расследование причин утери или кражи носителя.

Для работы с квалифицированной подписью необходимо использовать только сертифицированные средства электронной подписи. Это средства электронной подписи, полностью соответствующие требованиям Российского законодательства и прошедшие ряд государственных проверок. В случае, если вы самостоятельно затрудняетесь определить если ли у средства электронной подписи сертификат соответствия – Вы можете обратиться за консультацией в удостоверяющий центр или к разработчику данного средства электронной подписи.

Государственные информационные системы, предназначенные для оказания государственных и муниципальных услуг в электронном виде, не принимают электронную подпись, созданную с использованием несертифицированных средств электронной подписи, поэтому в случае использования несертифицированных средств электронной подписи существует риски отказа в оказании государственных и муниципальных услуг, приеме заявлений и других электронных документов. Также могут возникнуть риски, связанные с проверкой электронной подписи в электронном документе в ходе судебного разбирательства, где рассматриваемый электронный документ был представлен в качестве доказательства

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ

Для обеспечения безопасности на рабочем месте:

- должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию;

- носители ключевой информации должны использоваться только их владельцем на использование данного носителя и храниться в месте, не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.);

- носитель ключевой информации должен быть вставлен в считывающее устройство рабочего места 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.