**Требования по безопасности**

**при использовании средств электронной подписи.**

**1. Основные риски при использовании электронной подписи (далее — ЭП) связаны с несанкционированным доступом к ключам ЭП (т.е. использованием без ведома их владельца), вследствие чего становится возможным возникновение электронных документов, порождающих нежелательные юридически значимые последствия в отношении владельца сертификата ЭП. Источниками несанкционированного доступа могут быть как преднамеренные либо неумышленные действия человека, так и активность вредоносного программного обеспечения. Далее приводится краткий перечень основных мер безопасности для владельцев ЭП, направленных на избежание указанных рисков.**

**2. Перед началом работы с электронной подписью владелец ЭП обязан ознакомиться с "Правилом по обеспечению информационной безопасности на рабочем месте" (далее АРМ).**

**3. Хранить электронную подпись в шкафах (ящиках, хранилищах, сейфах) индивидуального пользования, исключающий бесконтрольный доступ к ним.**

**4. Сдать токен со средствами электронной подписи в Службу информационной безопасности Сеченовского Университета при увольнении, переводе на другую должность или отстранении от исполнения должностных обязанностей с использованием ЭП;**

**5. При использовании электронной подписи владелец ЭП обязан:**

**- не записывать на ключевые носители постороннюю информацию;**

**- не оставлять технические средства с установленными средствами электронной подписи при их использовании без визуального контроля;**

**- не вносить какие-либо изменения в программное обеспечение средств электронной подписи и криптографической защиты;**

**- не осуществлять несанкционированное копирование ключевых носителей;**

**- не разглашать содержимое носителей ключевой информации или передавать сами носители посторонним лицам, не выводить ключевую информацию на дисплей и принтер;**

**- не подключать к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты дополнительные устройства и соединители, не предусмотренные штатной комплектацией;**

**- не осуществлять несанкционированное вскрытие корпуса технического средства с установленными средствами электронной подписи и средствами криптографической защиты;**

**- незамедлительно уведомлять Службу информационной безопасности Сеченовского Университета о попытках или факте компрометации (утрате, хищении, разглашении, несанкционированного копирования при передаче по линии связи в открытом виде) СКЗИ, ключевых документов к ним**

**6. Использовать электронную подпись работник должен только на своем АРМ при выполнении следующих требований:**

**- использовать программные и антивирусные средства последних версий, проводить своевременное их обновление;**

**- использовать пароль доступа на АРМ, соответствующий политике безопасности Университета, обеспечивать смену пароля для АРМ не реже одного раза в полугодие;**

**- при подключении АРМ к сети Интернет выполнять необходимые меры безопасности.**

**7. При возникновении вопросов:**

**- по применению ЭП обращаться в подразделение информационных технологий;**

**- при нарушении требований по защите информации, компрометации ключа электронной подписи обращаться в Службу информационной безопасности (тел.: 35-10, электронная почта: iss\_sign@staff.sechenov.ru).**