# Требования и рекомендации

**по обеспечению информационной безопасности АРМ Клиента**

**Размещение АРМ**

Охрана и организация режима помещений, в которых расположены АРМ и хранятся носители ключевой информации, должны исключать возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

**Защита АРМ и закрытых ключей ЭП от несанкционированного доступа**

Клиентом должны быть разработаны и строго им соблюдаться нормативные документы, регламентирующие правила хранения, доступа и использования закрытых ключей ЭП.

Клиент, эксплуатирующий АРМ, должен принять необходимые меры, позволяющие исключить внесение несанкционированных изменений в технические и программные средства АРМ, изменение их состава, появление на АРМ и в системе ДБО компьютерных вирусов, а также программ, направленных на разрушение или модификацию программного обеспечения системы ДБО, ЭД, либо на перехват паролей, закрытых ключей ЭП и другой конфиденциальной информации.

На АРМ должен быть реализован комплекс мер и средств защиты от угроз публичной сети Интернет, обеспечивающий защиту данных от несанкционированного доступа по сети. Рекомендуется на вышестоящем уровне (как правило – на прокси-сервере) введение ограничения для компьютера, на котором работает АРМ, доступа в Интернет только несколькими сайтами, необходимыми для производственной деятельности. Клиент, эксплуатирующий АРМ, должен постоянно использовать антивирусное программное обеспечение и своевременно осуществлять его обновление, а также обновления операционной системы и web-браузеров.

Запрещается установка на АРМ Клиента программных средств, не предназначенных для выполнения служебных обязанностей абонентов Клиента, допущенных к работе на АРМ.

Носители ключевой информации должны браться на учет в специально выделенных для этих целей журналах.

Порядок хранения и использования носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

При выявлении признаков нарушения информационной безопасности АРМ Клиента рекомендуется временно приостановить его эксплуатацию.

Если в качестве АРМ для работы в «Интернет-Клиент» системы ДБО выбран переносной компьютер (ноутбук), его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.) должно быть исключено. В случае передачи сторонним лицам (списания, утилизации и т.п.) стационарного компьютера (или ноутбука), на котором ранее была установлена Система ДБО, необходимо гарантированно удалить с него всю информацию, использование которой третьими лицами может потенциально нанести вред финансовой деятельности или имиджу Вашей организации, в том числе следы работы в Системе ДБО.

В случае возникновения сбоев в работе «Интернет-Клиент» Системы ДБО (невозможно установить связь с сервером Системы или компьютер с установленной Системой внезапно вышел из строя: нет доступа, невозможно войти в систему, возникли ошибки при загрузке операционной системы и т.д.) необходимо незамедлительно сообщить об этом в БАНК.

**Правила и рекомендации хранения носителей ключевой информации**

Для хранения носителей ключевой информации необходимо использовать надежные металлические хранилища, оборудованные внутренними замками.

Хранение носителей ключевой информации допускается в хранилище, используемом совместно с другими сотрудниками, но при этом в отдельной упаковке (контейнере), опечатанной личной печатью владельца носителей ключевой информации и исключающей возможность негласного доступа к ним посторонних лиц.

Запрещается передавать носители ключевой информации другим лицам, выводить закрытые ключи ЭП на дисплей или принтер, оставлять носители ключевой информации без присмотра, а также записывать на носитель ключевой информации постороннюю информацию.

**Требования к абонентам Клиента**

Сотрудники, допущенные к работе на АРМ, назначаются приказом и должны иметь утвержденные должностные инструкции.

Непосредственная работа сотрудников на АРМ возможна только после прохождения обучения и проверки знания ими правил эксплуатации АРМ.

Каждый сотрудник, имеющий доступ к носителям ключевой информации, паролям и другой конфиденциальной информации, должен быть проинформирован об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства.

ОЗНАКОМЛЕН:

КЛИЕНТ

Наименование ИНН/КПП

Банковские реквизиты:

Подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

М.П.