

УТВЕРЖДЕНО
Правлением АО СПВБ
Протокол от 18 марта 2019 года № 10/19

Управляющий

/К.В. Артёмов/

**ТЕХНИЧЕСКИЕ УСЛОВИЯ
ПОДКЛЮЧЕНИЯ РАБОЧИХ МЕСТ
АО СПВБ**

Санкт---Петербург
2019

Требования к организации рабочего места Участника

1. Под Рабочим местом в настоящем документе подразумевается персональный компьютер, предназначенный для организации доступа уполномоченного сотрудника (Пользователя) Участника торгов либо Участника СЭД (далее именуемые – Участники) к следующим электронным системам (далее вместе именуемым – Системы) Акционерного общества «Санкт-Петербургская валютная биржа» (Далее — Биржа):
 - Торговая система (ТС);
 - Система электронного документооборота (СЭД).
2. Для получения услуги доступа к Системам, Участник должен иметь обслуживаемые сотрудниками Участника программно-технические средства (далее - ПТС) - состоящие из комплекса средств автоматизации его деятельности по осуществлению электронного документооборота и для участия в торгах в Биржевых секциях.
3. Требования к предустановленному программному обеспечению (ПО) автоматизированного рабочего места (АРМ):
 - операционная система – лицензионная версия Microsoft Windows
 - сертифицированное ФСБ РФ средство криптографической защиты информации (далее - СЗКИ) «КриптоПро CSP» 4.0;
 - источник бесперебойного питания;
4. Требования к каналам связи:
 - наличие канала связи от АРМ пользователя до шлюзов доступа АО СПВБ;
 - основной канал связи может быть организован через выделенную линию, арендуемую у одного из сетевых провайдеров АО СПВБ или через VPN соединение с использованием сети Интернет;
 - при использовании VPN соединения, необходимо наличие подключения к сети Интернет с пропускной способностью не менее 512 Kb/s и статического IP адреса, полученного у провайдера телекоммуникационных услуг;
 - для повышения отказоустойчивости подключения к Системам, наряду с основным каналом связи, настоятельно рекомендуется организовать также и резервный канал, построенный при помощи VPN соединения по сети Интернет;
 - основной и резервный каналы связи АРМ, построенные при помощи VPN соединения, могут использовать одно и то же подключение к сети Интернет, и один и тот же статический IP адрес, но будут осуществлять доступ к разным шлюзам АО СПВБ, имеющим независимые выходы в сеть Интернет.
5. Для получения доступа к Системам СЭД (во всех вариантах подключения) и(или) Торговой Системы (при подключении через VPN), необходимо наличие у Пользователей Систем, ключевой информации электронной подписи (далее - ЭП) на ключевых носителях ЭП – ключа ЭП и сертификата ключа проверки ЭП (далее - Сертификат), отвечающих установленным требованиям к системам для данных целей использования, выданных Удостоверяющим Центром АО СПВБ.
6. При осуществлении электронного документооборота, электронные документы заверяются (подписываются) ЭП сотрудника Участника.
7. При организации доступа к Системам Участник обязан в письменном виде сообщить Бирже статический IP адрес, полученный у провайдера телекоммуникационных услуг

и используемый для организации подключения.

8. Участник обязан обеспечить соблюдение требований действующего законодательства, регулирующего использование средств ЭП и СКЗИ, исключить компрометацию ключей ЭП сотрудников Участника торгов. Под компрометацией ключа ЭП понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам.
9. В случае компрометации ключа ЭП сотрудника Участник обязан незамедлительно прекратить использование таких ключей ЭП и сообщить об этом в удостоверяющий центр, сформировавший ключевую информацию ЭП.
10. Сертификат ключа проверки ЭП действителен в течение срока, указанного в Сертификате. В целях обеспечения бесперебойной работы Участнику рекомендуется направлять заявку на переформирование Сертификата не позднее, чем за 1,5 месяца до окончания срока действия предыдущих Сертификатов.
11. Участник обязан содержать в исправном состоянии комплекс ПТС, которые подключены к Системам Биржи, принимать организационные, правовые и технические меры защиты информации для предотвращения несанкционированного доступа (далее - НСД) к ПТС, ключам ЭП и СКЗИ, а также предотвращения НСД в помещении, в которых установлены указанные средства. Участнику для обеспечения защиты информации в ПТС рекомендуется обеспечить разграничение и контроль доступа должностных лиц к ресурсам ПТС с использованием сертифицированных средств защиты информации:
 - антивирусных программных средств;
 - комплексов средств защиты информации (далее - СЗИ) от НСД;
 - межсетевых экранов (далее - МЭ).
12. Для подключения АС Участника к Информационным системам Биржи, Участнику рекомендуется использовать сертифицированные ФСБ РФ средства защиты.
13. Участник обязан следить за защищенностью и актуальностью используемого в работе программного обеспечения (далее - ПО), своевременно производить обновление версий программного обеспечения ТС и СЭД, соблюдать требования эксплуатационной и технической документации на СКЗИ, СЗИ от НСД и МЭ.
14. Биржа не несет ответственности за функционирование ПТС Участника торгов.
15. При использовании Рабочих мест Биржи запрещается:
 - Использовать Рабочие места Биржи для иных целей, чем осуществление электронного документооборота и/или участие в торгах в Биржевых секциях.
 - Производить самовольное (несанкционированное) проникновение в любые технологические компоненты (узлы), программы, базы данных и иные составляющие элементы Систем Биржи.
 - Использовать Рабочее место для передачи информации, распространение которой, так или иначе, противоречит российскому или международному праву.
 - Использовать на Рабочем месте программы(информацию), которые(ая) содержит(может содержать) в себе вредоносные программы (вирусы) или другие вредоносные компоненты или вредоносный код.