Открытое акционерное общество
«БПС-Сбербанк»

ДОПОЛНЕНИЕ 12

21.10.2019 № 01/01-07/

г. Минск

УТВЕРЖДЕНО

Протокол заседания Правления

21.10.2019 №

к Условиям дистанционного банковского обслуживания корпоративных клиентов в ОАО «БПС-Сбербанк» от 23.06.2014 №01-07/203

1. В Условия дистанционного банковского обслуживания корпоративных клиентов в ОАО «БПС-Сбербанк» от 23.06.2014 № 01-07/203 (далее – Условия) внести следующие изменения и дополнения:

1.1. пункт 59 изложить в следующей редакции:

«59. С целью обеспечения информационной безопасности Клиент обязуется ознакомиться и руководствоваться при работе с СДБО требованиями к защите клиентского рабочего места, указанными в приложении 11 к настоящим Условиям.

Доступ к компьютеру, мобильному устройству и рабочему месту Клиента в СДБО должен быть ограничен программно-техническими средствами регламентации доступа.»;

1.2. дополнить Условия приложением 11 следующего содержания:

«Приложение 11 к Условиям
дистанционного банковского
обслуживания корпоративных
клиентов в ОАО «БПС-Сбербанк»

ТРЕБОВАНИЯ К ЗАЩИТЕ КЛИЕНТСКОГО РАБОЧЕГО МЕСТА СДБО

1. Программное обеспечение СДБО должно быть установлено на выделенном автоматизированном рабочем месте (далее – АРМ), размещенном в доверенном сегменте сети Клиента. Размещение элементов программного обеспечения СДБО на файловом сервере не допускается.

Доверенный сегмент организуется, как физически отдельный сегмент локально-вычислительной сети (далее – ЛВС) Клиента либо как отдельный виртуальный сегмент ЛВС (VLAN). Политикой безопасности коммуникационного оборудования ЛВС должны быть созданы листы доступа, разрешающие информационное взаимодействие из VLAN, в котором размещен АРМ СДБО Клиента, только с необходимыми для работы хостами (устройствами) сети Клиента и только по необходимым протоколам. В

доверенном сегменте допускается размещение других АРМ, обрабатывающих информацию, составляющую банковскую и/или коммерческую тайну.

2. Для АРМ СДБО Клиента должен использоваться выделенный персональный компьютер, предназначенный исключительно для задач обмена финансовыми документами и информацией с использованием СДБО.

В случае производственной необходимости допускается организация автоматизированного взаимодействия между клиентской составляющей СДБО и ERP-системой Клиента или автоматизированной системой (АС) бухгалтерского учета. Разрешается установка на АРМ СДБО Клиента компонент этих АС, коннекторов к ним или передача информации в режиме файловой перекладки через защищенный файловый сервер в ЛВС Клиента при условии соблюдения требований информационной безопасности к АРМ СДБО Клиента, указанных в настоящем приложении к Условиям.

Установка на АРМ СДБО Клиента иного программного обеспечения (в том числе офисного, кроме необходимого для осуществления деятельности) – не допускается. Если АРМ ранее использовалось в качестве технологического компьютера или рабочего места работника, перед установкой на него программного обеспечения СДБО носители информации АРМ должны быть отформатированы, операционная система и иное программное обеспечение, необходимые для функционирования СДБО – переустановлены с лицензионных дистрибутивов. Установка программного обеспечения СДБО выполняется после размещения АРМ СДБО в доверенном сегменте сети Клиента.

3. На межсетевом экране Клиента должна быть заблокирована возможность установления соединений с АРМ СДБО Клиента со стороны сети Интернет. Также должен быть заблокирован доступ с АРМ СДБО Клиента в сеть Интернет, за исключением минимально необходимых для работы программного обеспечения СДБО протоколов и IP-адресов серверов Банка.

Должна быть предусмотрена полная гарантированная автоматическая или ручная блокировка доступа в сеть Интернет для АРМ СДБО Клиента в нерабочее время.

4. На АРМ СДБО Клиента должен физически отсутствовать функционал Wi-Fi, Bluetooth, иных средств беспроводной связи. Запрещено подключение (даже кратковременное) к АРМ СДБО Клиента мобильных телефонов, коммуникаторов, КПК, фотоаппаратов, плееров, модемов любого типа.

5. На АРМ СДБО Клиента должно использоваться только лицензионное и регулярно обновляемое программное обеспечение. Перечень программного обеспечения, устанавливаемого на АРМ СДБО, должен быть сокращен до минимально необходимого. Должны быть установлены последние пакеты обновления (Service Pack) и все обновления безопасности операционной системы и прикладного программного обеспечения.

6. На АРМ СДБО Клиента необходимо использовать лицензионное антивирусное программное обеспечение с актуальными базами и модулями, обновляющимися ежедневно. Антивирусное программное обеспечение должно выполнять полное сканирование АРМ СДБО не реже 1 раза в неделю.

7. Внутренними подразделениями Клиента, ответственными за

применение информационных технологий и/или информационную безопасность либо специализированными организациями, осуществляющими сопровождение АС Клиента, для АРМ СДБО должны быть разработаны и применены максимально возможно ограничивающие политики безопасности, предотвращающие доступ к АРМ всем работникам, кроме уполномоченных лиц.

На АРМ СДБО Клиента должна быть отключена учетная запись Guest, переименована учетная запись Administrator, удалены все привилегии у группы Everyone, запрещено удаленное управление реестром, подключение по null-session. Кроме того, должна быть отключена функция autorun для любых видов носителей информации, выключена служба Server и другие неиспользуемые службы.

8. На АРМ СДБО Клиента должны быть активированы подсистемы аудита. Все системные журналы должны иметь размер не менее 20 MB каждый и автоматически перезаписываться по мере их наполнения.

9. На АРМ СДБО Клиента должны быть заведены персонифицированные учетные записи работников, ответственных за проведение операций в СДБО, под которыми функционирует программное обеспечение СДБО. Также на АРМ СДБО должен быть заведен один административный пользователь (с правами локального администратора), под которым на АРМ СДБО Клиента выполняются исключительно работы по установке и настройке программного обеспечения, необходимого для функционирования АРМ СДБО Клиента. Средствами операционной системы должно быть ограничено число неправильных попыток ввода пароля Клиента блокировки учетной записи пользователя (3 попытки).

10. Права пользователя, под которым функционирует АРМ СДБО Клиента, должны быть установлены в минимально необходимые, не должны использоваться права local administrator и power user.

11. Не рекомендуется установка на АРМ СДБО Клиента любых средств удалённого управления и администрирования.

12. В целях исключения ошибочных или преднамеренных действий пользователей рекомендуется средствами политик безопасности операционной системы или специализированными средствами защиты персонального компьютера от НСД, реализовать для пользователя функционально-замкнутую среду, позволяющую ему запускать и работать только с разрешенным программным обеспечением без доступа к файловой системе и реестру операционной системы.

13. В случае неожиданного выхода из строя АРМ СДБО Клиента, нарушения работы или исчезновения на нем программного обеспечения СДБО, необходимо незамедлительно отключить АРМ СДБО от всех видов сетей, включая локальную корпоративную сеть, и срочно запросить в Банке выписку по счетам Клиента. При обнаружении несанкционированных платежных операций необходимо незамедлительно предоставить соответствующее заявление в Банк. Работоспособность поврежденного АРМ СДБО запрещается восстанавливать до проведения технической экспертизы. Переустановку программного обеспечения СДБО требуется проводить на новом АРМ. После переустановки программного обеспечения должна быть произведена

немедленная смена всех ключей ЭЦП, используемых для работы в СДБО.

14. Установка носителя электронных ключей на АРМ СДБО должна выполняться только в момент его использования для работы с СДБО с последующим незамедлительным извлечением устройства.».

2. Настоящее Дополнение вступает в силу с 01.11.2019.

Директор Департамента
корпоративных продуктов А.В.Николаевский