Приложение № 8
к Регламенту обслуживания корпоративных клиентов
с использованием системы дистанционного банковского
обслуживания «iBank» АО Банк «Объединенный капитал»

Требования по обеспечению информационной безопасности при работе с Системой ДБО «iBank»

Следующие требования информационной безопасности обязательны для выполнения Клиентом:

1. Клиент должен назначить Администратора информационной безопасности – работника, ответственного за настройку безопасности эксплуатации средств защиты информации, установленных на АРМ Клиента.
2. Ключевые носители с ключами должны быть подключены к АРМ Клиента только на время работы в Системе ДБО «iBank».
3. На АРМ Клиента должно быть установлено лицензионное антивирусное программное обеспечение и выполнена настройка автоматического обновления программного обеспечения и антивирусных баз с официального web-сайта разработчика антивирусного ПО.
4. На АРМ Клиента, при наличии, должен быть настроен персональный межсетевой экран (Firewall) имеющийся в составе операционной системы.
5. На АРМ Клиента должны быть отключены сервисы, позволяющие удаленно управлять компьютером.
6. На АРМ Клиента должно использоваться лицензионное программное обеспечение (операционные системы, офисные пакеты, прикладные программы) и обеспечено автоматическое обновление системного и прикладного ПО. Не должно устанавливаться ПО с нарушением рекомендованных производителями требований.
7. Клиент обеспечивает хранение и использование Ключевого носителя таким образом, чтобы исключить доступ к нему неуполномоченных лиц. Запрещается сохранять конфиденциальную информацию в файлах (включая графические изображения) или в памяти устройств, в справочниках или «облачных» сервисах хранения информации и ресурсах в сети «Интернет». Запрещается фиксировать конфиденциальную информацию на бумажных носителях (листы для записей, распечатки документов и т.п.), доступ к которым могут получить неуполномоченные лица.
8. По окончании работы с Системой ДБО «iBank» Ключевой носитель должен быть извлечен и хранится в месте, обеспечивающем его защиту от доступа посторонних лиц, неуполномоченных для работы в Системе. Запрещается оставлять Ключевой носитель без присмотра.
9. Запрещается использовать «чужие» компьютеры или мобильные устройства для доступа к Системе ДБО «iBank», работать с Системой ДБО «iBank» с «гостевых» рабочих мест (в интернет-кафе и т.д.) при использовании публичных сетей беспроводного доступа.
10. Не рекомендуется использовать компьютер, на котором установлено рабочее место Системы ДБО «iBank», не по назначению, например, для игр, просмотра фильмов и т.п.
11. Производить замену ключей ЭП до истечения срока их действия во всех случаях увольнения и(или) смены полномочий и(или) лиц, имеющих доступ к Системе ДБО «iBank» или право подписи доверенностей на получение ключей ЭП.

В целях повышения безопасности информации, обрабатываемой в Системе ДБО «iBank», помимо обязательных мер, Банк рекомендует:

1. Выделить отдельную ПЭВМ, предназначенную только для работы в Системе ДБО «iBank».
2. При отсутствии возможности использования отдельной ПЭВМ, выполнить настройку множественной загрузки ПЭВМ с созданием отдельного профиля для работы только с Системой ДБО «iBank».
3. Установить на АРМ Клиента лицензионное специализированное программное обеспечение, повышающее уровень защищенности: межсетевой экран (Firewall), антишпионское ПО (antispyware). В настройках межсетевого экрана запретить любые соединения, кроме IP- адреса Банка.
4. Отключить неиспользуемые на АРМ Клиента сетевые протоколы и службы.
5. Отключить все общие ресурсы операционной системы, в том числе и создаваемые по умолчанию при ее установке.
6. Установить для учетной записи оператора АРМ Клиента минимальный уровень прав доступа, необходимого для нормальной работы в Системе ДБО «iBank». Работу оператора АРМ Клиента под учетной записью с правами «администратора» исключить. Отключить стандартную учётную запись администратора, предварительно назначив административные права иной учётной записи с

нестандартным именем. Установить для неё сложный пароль, отличающийся от паролей остальных учётных записей. Использовать такую учётную запись только для настройки компьютера, установки доверенного программного обеспечения и т.д.

7. Ограничить доступ работников и посторонних лиц к АРМ, используемому для работы с Системой ДБО «iBank». Доступ к АРМ Клиента предоставить только лицам, непосредственно работающим с Системой ДБО «iBank».
8. При использовании услуг сторонней организации или частных лиц по настройке и обслуживанию ПЭВМ, обеспечить контроль действий лица, осуществляющего непосредственную настройку и не допускать его к Системе ДБО «iBank» и Ключам ЭП. При необходимости проверки работоспособности Системы ДБО «iBank» она должна выполняться исключительно лицами, уполномоченными для работы с Системой.
9. Использовать услугу фильтрации IP-адресов. Для этого необходимо заполнить соответствующий раздел Заявления о присоединении к Регламенту (Приложение 1 к Регламенту). Банк обязуется изменить настройки Системы ДБО «iBank» в соответствии с указаниями Клиента не позднее дня, следующего за днем приема данного Заявления.
10. Использовать услугу дополнительного подтверждения платежных поручений с помощью Кодов подтверждения в SMS- сообщениях.
11. Организовать хранение Ключевых носителей в персональных надежных опечатываемых хранилищах (сейфах). При использовании более одного ключа ЭП следует хранить ключи ЭП на разных ключевых носителях и использовать их для работы с Системой ДБО «iBank» через различные устройства - это сделает невозможным отправку электронного платёжного документа вредоносной программой, заразившей одно из устройств.
12. Обеспечить использование паролей ключей ЭП, удовлетворяющих следующим минимальным требованиям:
    Пароль -
    - не должен состоять из одних цифр;
    - должен быть длиннее 8 знаков;
    - должен содержать в себе строчные и прописные буквы, цифры и знаки препинания;
    - не должен состоять из символов, находящихся на одной линии на клавиатуре;
    - не должен быть легкоугадываемым (легкоузнаваемым) значимым словом (имя, фамилия, дата рождения, девичья фамилия супруги, кличка собаки, кошки и т.д.).
13. Внимательно проверять суммы и реквизиты проводимых платежей в приходящих уведомлениях или сообщениях с Кодами подтверждения, не подтверждать подозрительные операции, и незамедлительно информировать Банк о попытках и (или) выявленных фактах мошеннических платежей.

Обращаем Ваше внимание, что выполнение указанных выше требований не сможет полностью обезопасить Вас и Ваши устройства от действий злоумышленников, но существенно поможет снизить вероятность и нежелательные последствия от таких действий.