Требования по обеспечению информационной безопасности

1. Меры по обеспечению защиты от несанкционированного доступа:

1.1. Периодически, не реже одного раза в 3 месяца, меняйте пароль. Пароль следует запомнить. Его хранение в письменном виде (файл, содержащий логин и пароль, записанный на ключевой носитель либо жесткий диск компьютера; бумажка, прикрепленная к монитору и т.п.) не рекомендуется, так как при этом возникает возможность доступа к паролю неуполномоченных лиц. Пароль должен быть не менее 8 символов, он не должен быть слишком простым, не рекомендуется использовать имена, числа и даты, связанные с владельцем пароля, а также пароли типа USER, ADMIN.

Категорически не допускается сообщать информацию о вашем пароле никому, включая лиц, представляющимися сотрудниками Банка. Сотрудники Банка никогда не просят сообщать подобные сведения. О таких случаях следует немедленно сообщать в Банк.

1.2. Работайте с Системой ДБО под учетной записью пользователя операционной системы, не имеющей прав локального администратора.

1.3. На компьютерах, используемых для работы по Системе ДБО, исключите посещение всех Интернет-сайтов непроизводственного характера (конференции, чаты, социальные сети, телефонные сервисы, новостные сайты, сайты сомнительного содержания), кроме используемых для входа в Систему ДБО и доверенных ресурсов сети Интернет, необходимых для выполнения должностных обязанностей. Перед началом работы по Системе ДБО закрывайте все открытые интернет-страницы. По окончании работы с системой «Интернет–Банк» также следует закрыть окно интернет-браузера.

1.4. При входе в систему «Интернет–Банк» контролируйте имя Интернет-сервера Банка: https://dbo.zhivagobank.ru.

1.5. Установите и настройте на рабочем месте лицензионное средство антивирусной защиты с ежедневным автоматическим обновлением антивирусных баз. Осуществляйте периодическую проверку ПЭВМ (рекомендуется ежедневная) средствами антивирусной защиты на предмет нахождения вирусов и других вредоносных программ.

1.6. Используйте только лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.), обеспечьте автоматическое обновление системного и прикладного программного обеспечения с сайтов производителей данного программного обеспечения, а также исключите установку развлекательных и игровых программ.

1.7. При обслуживании компьютера ИТ-сотрудниками (системными администраторами) обеспечивайте контроль над выполняемыми ими действиями.

1.8. Не предоставляйте общий доступ к жесткому диску компьютера, на котором установлена Система ДБО, исключите использование средств удаленного администрирования компьютера, в том числе встроенных в операционную систему (например, удаленное управление рабочим столом).

1.9. Режимы безопасности, реализованные в применяемой операционной системе и интернет–браузере, должны быть настроены на максимальный уровень.

1.10. В случае получения по электронной почте якобы от Банка любых сообщений, содержащих вложенные файлы или ссылки на какие-либо Интернет-ресурсы, не открывайте вложения и не переходите по ссылке; следует позвонить в Банк по телефону (не из поступившего сообщения), а известному из других проверенных источников, и получить разъяснения о достоверности содержащейся в нем информации.

1.11. Запрещается вносить какие-либо изменения в программное обеспечение Системы ДБО.

2. Меры по организационному обеспечению безопасности при работе в Системе ДБО:

2.1. В организации Клиента выделяются (определяются) должностные лица, ответственные за эксплуатацию Системы ДБО.

2.2. Соблюдайте регламент ограниченного доступа к компьютеру, на котором функционирует Система ДБО.

3. Требования по размещению оборудования с установленной Системой ДБО и режиму охраны:

3.1. Помещение, где установлен компьютер, на котором функционирует Система ДБО, должно исключать возможность бесконтрольного проникновения в него посторонних лиц.

3.2. Входные двери помещений должны быть оборудованы замками, обеспечивающими их надежное закрытие в нерабочее время.

3.3. Системные блоки компьютеров с установленной Системой ДБО могут быть оборудованы средствами контроля вскрытия, место опечатывания должно быть таким, чтобы его можно было визуально контролировать.

3.4. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения Системы ДБО.

4. Требования по обеспечению безопасности использования ключей электронной подписи:

4.1. Учет и хранение ключей электронной подписи поручается специально уполномоченным сотрудникам. Чрезвычайно важно обеспечить доступ к ключевым носителям только специально назначенным сотрудникам. ***Электронная подпись Руководителя организации под электронным расчетным платежным документом вырабатывается с использованием ключевого носителя. Право доступа к ключевому носителю фактически означает право ставить подпись от имени Руководителя организации***.

4.2. Место хранения ключевых носителей (сейф, металлический шкаф и т.д.) должно обеспечивать их безопасность и надежную защиту от несанкционированного доступа посторонних лиц.

4.3. Никогда, даже на короткое время, не передавайте ключевой носитель другим лицам, например, для проверки работы Системы ДБО, проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только владелец ключа ЭП может подключить ключевой носитель к компьютеру.

4.4. Не выводите ключевую информацию на дисплей, принтер и иные средства отображения информации.

4.5. Категорически запрещено передавать ключевую информацию по техническим средствам связи.

4.6. Не отлучайтесь от компьютера, пока в нем находится ключевой носитель. Перед тем, как покинуть рабочее место (даже на короткое время), уберите ключевой носитель в недоступное место и заблокируйте свой сеанс работы по Системе ДБО.

4.7. Извлекайте из компьютера ключевой носитель сразу после завершения работы по Системе ДБО, окно Интернет-браузера при работе в системе “Интернет-Банк” закрывайте. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

4.8. Не записывайте на ключевой носитель какую-либо постороннюю информацию (в том числе рабочие или личные файлы).

4.9. Категорически запрещается хранить ключи ЭП на жестком диске компьютера. Ключевая информация должна размещаться на съемном носителе информации. Размещение

ключевой информации на локальном или сетевом диске способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

4.10. Не используйте бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации.

4.11. Исключите неконтролируемое копирование информации с ключевого носителя.

4.12. Периодически проводите разъяснительную работу среди сотрудников, уполномоченных для работы по Системе ДБО. При этом обратите особое внимание на необходимость строгого сохранения в тайне ключа ЭП.

5. Компрометация ключевой информации или подозрение на компрометацию:

5.1. В случае выявления явных или косвенных признаков компрометации ключей ЭП или обнаружении вредоносных программ (действий) в компьютере, используемом для работы по Системе ДБО, незамедлительно уведомите Банк в соответствии с п. 6.3.19 Условий предоставления услуг с использованием системы дистанционного банковского обслуживания с целью блокирования возможности использования скомпрометированных ключей ЭП с последующей их заменой.

5.2. К событиям, связанным с компрометацией ключей ЭП или подозрением на компрометацию относятся, включая, но, не ограничиваясь, следующие:

– утеря ключевого носителя, в том числе с его последующим обнаружением;

– выход из строя ключевого носителя, когда невозможно достоверно определить причину этого события (доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

– обнаружение факта или угрозы использования (копирования) ключа ЭП и/или доступа к Системе ДБО с использованием ключа ЭП неуполномоченными лицами (несанкционированная отправка электронных документов);

– увольнение или смена ответственного сотрудника организации, имевшего доступ к ключу ЭП или Руководителя и/или Главного бухгалтера организации;

– обнаружение или подозрение, что компьютер, на котором установлена Система ДБО, подвергся заражению компьютерными вирусами, программами-шпионами и т.д.;

– возникновение трудностей в подключении к Системе ДБО, проявление нестабильного функционирования ЭВМ, системы во время дистанционного банковского обслуживания;

– невозможность войти в систему «Интернет–Банк» под своими учетными данными (логин и пароль);

– возникновение подозрений на утечку информации или её искажения при работе в Системе ДБО;

– нерасшифровывание входящих или исходящих сообщений у абонентов;

– утрата ключей (личных печатей) от помещения или сейфа (контейнера) с ключевыми носителями;

– нарушение печати на сейфе или контейнере с ключевыми носителями;

– несанкционированное вскрытие опечатанного корпуса ЭВМ, на котором установлено программное обеспечение Системы ДБО.

5.3. В этих и подобных случаях следует немедленно прекратить использование Системы ДБО, отключить компьютер от сети и начать расследование инцидента.

6. Дополнительные требования:

6.1. Дополнительные требования по обеспечению информационной безопасности при работе по Системе ДБО могут дополнительно устанавливаться Банком путем размещения на Сайте Банка, а также информированием средствами Системы ДБО.