Рекомендации по информационной безопасности при дистанционном банковском обслуживании с использованием Системы ДБО iBank2

Обращаем Ваше внимание на тот факт, что системы дистанционного банковского обслуживания и взаимодействующие с ними финансовые (бухгалтерские) системы клиентов являются постоянной мишенью для различного рода злоумышленников. Распространяемые ими вредоносные программы нацелены на хищение денежных средств со счетов клиентов путём создания, подписания электронной подписью (ЭП) и отправки в банки платёжных документов якобы от имени клиентов, которые практически неотличимы от документов, создаваемых самими клиентами. Эти программы создаются профессионалами высокого класса с учётом особенностей конкретных информационных систем. Киберпреступники не обошли своим вниманием и используемую в ПАО Банк ЗЕНИТ (далее – Банк) Систему ДБО iBank2 (далее – система ДБО) компании «БИФИТ».

Существуют риски получения доступа злоумышленников к защищаемой информации для осуществления переводов денежных средств, если Вами не будут соблюдаться правила безопасного использования системы ДБО, приведённые в настоящем документе мер информационной безопасности, не будет обеспечена защита логинов/паролей, ЭП и криптографических ключей (ключевых носителей), а также используемых Вами технических средств.

Безопасность работы клиентов с системой ДБО является важнейшим приоритетом для Банка, поэтому нами разработаны обязательные для выполнения всеми пользователями Системы ДБО iBank2 меры информационной безопасности, основанные на требованиях:

- Письма Банка России от 07.12.2007 № 197-Т «О рисках при дистанционном банковском обслуживании»,
- Письма Банка России от 31.03.2008 № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга»,
- Письма Банка России от 30.01.2009 № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга»,
- Письма Банка России от 25.06.2009 № 76-Т «О рекомендациях по информированию клиентов о размещении на Web-сайте Банка России списка адресов Web-сайтов кредитных организаций»,
- Положения Банка России от 09.06.2012 № 382-П «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Меры информационной безопасности, необходимые для выполнения пользователями Системы ДБО iBank2

1. Общие принципы обеспечения безопасности:

1.1. Помните, что ни одна программа и(или) техническое решение не даёт 100% гарантии защиты Вашего компьютера, планшета, смартфона или иного устройства, с которого вы осуществляете операции в системе ДБО, и(или) на которые вы получаете SMS-пароли или услуги SMS-информирования (далее – Устройство) от несанкционированного использования

злоумышленниками, поражения вирусом или иным вредоносным программным кодом. Старайтесь использовать указанные в настоящих Рекомендациях защитные меры в комплексе.

1.2. Регулярно самостоятельно контролируйте состояние своих банковских счетов и операций по ним.

1.3. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи (телефоны, факсы, веб-сайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, полученных непосредственно в подразделениях Банка.

1.4. Ни при каких условиях не сообщайте третьим лицам, включая любых работников Банка, Вашу конфиденциальную информацию и секретные реквизиты для взаимодействия с Банком и работы с использованием Устройств, токенов, с системой ДБО (логины, пароли, кодовые слова). Исключите возможность неправомерного получения информации о паролях к системе ДБО и (или) токенам, SMS-паролям.

1.5. Не сохраняйте конфиденциальную информацию в файлах (включая графические изображения) или в памяти Устройств, в справочниках или «облачных» сервисах хранения информации и ресурсах в сети Интернет. Не фиксируйте конфиденциальную информацию на бумажных носителях (листы для записей, распечатки документов и т.п.), доступ к которым могут получить несанкционированные лица.

1.6. Исключите возможность неправомерного доступа, использования токенов и(или) Устройств для доступа к системе ДБО. Не передавайте их неуполномоченным лицам, храните в надёжном и недоступном для третьих лиц месте. Обязательно установите пароль на доступ к Устройству и никому его не раскрывайте. Помните, что посторонние люди могут, в том числе и не преднамеренно, нарушить работоспособность Устройств, занести вредоносные программы как со своих носителей информации, так и путём посещения вредоносных интернет-сайтов.

1.7. Не используйте чужие компьютеры или мобильные устройства для доступа к системе ДБО, не работайте с системой ДБО с «гостевых» рабочих мест (в интернет-кафе и т.д.) и(или) при использовании публичных сетей беспроводного доступа. При этом увеличивается риск хищения и(или) дальнейшего неправомерного использования ключа ЭП и другой аутентификационной информации при доступе к системе ДБО и(или) токенам.

2. Обеспечение безопасности на Устройствах, используемых для взаимодействия с Банком:

2.1. Не доверяйте администрирование (установку и настройку аппаратного и программного обеспечения) Ваших Устройств случайным людям. Приходящий администратор для своего удобства или злонамеренно может установить программу удалённого управления и получит возможность тайно от Вас на Вашем Устройстве выполнять различные программы, в том числе и вредоносные.

2.2. Используйте на Устройствах только лицензионное программное обеспечение, полученное из надёжных источников. Программы, полученные с непроверенных интернет-сайтов или носителей информации, зачастую содержат в себе вредоносные компоненты: вирусы и троянские программы. Не устанавливайте на Устройства программы с нарушением рекомендованных производителями требований.

2.3. Своевременно устанавливайте обновления установленного на Устройстве программного обеспечения, выпускаемые его производителями. Отдельно обращаем внимание на необходимость использования актуальной версии используемого интернет-браузера и среды исполнения Java, которая требуется для работы система ДБО.

2.4. Используйте на Устройстве современную антивирусную программу с функциями защиты от различного вида угроз. Своевременно, желательно – в автоматическом режиме, устанавливайте обновления всех компонентов и информационных баз антивирусной программы.

2.5. Следует периодически (раз в неделю) осуществлять полную антивирусную проверку Устройства, на котором работаете с системой ДБО. При возможности, используйте программы контроля конфигураций операционной системы на Устройстве – это позволит своевременно выявить вредоносные программы.

2.6. Используйте на Устройстве межсетевой экран («файервол»). Это затруднит несанкционированный удалённый доступ к Вашему Устройству из сети Интернет.

2.7. Работайте на Устройстве с системой ДБО только с правами обычного пользователя (не администратора). По возможности, не используйте данную учётную запись для действий в сети Интернет либо во внутренней сети, не связанными с работой в системе ДБО.

2.8. На Устройствах под управлением операционных систем семейства Windows не отключайте функцию «Контроль учетных записей пользователей» (UAC – User Account Control). Отключайте стандартную учётную запись администратора, предварительно назначив административные права иной учётной записи с нестандартным именем. Установите для неё сложный пароль, отличающийся от паролей остальных учётных записей. Используйте такую учётную запись только для настройки Устройства, установки доверенного программного обеспечения и т.д.

2.9. Не используйте для проведения операций или получения SMS-паролей и(или) SMS-информирования мобильные Устройства с отключёнными функциями безопасности, предусмотренными производителем (с использованием программ для получения Jailbreak или Root доступа к Устройству).

2.10. Применяйте разные пароли для различных Устройств и программ, регулярно осуществляйте их смену. Используйте пароли более 8 символов с применением и цифр, и специальных символов, больших и маленьких букв. Не используйте попеременно и(или) одни и те же пароли для разных Устройств и(или) программ, доступа к публичным интернет-сайтам и информационным сервисам:

- для доступа в Устройства;
- для входа в учётные записи;
- для изменения настроек программного обеспечения, прежде всего – обеспечивающего безопасность (антивирус, файервол);
- для работы с системой ДБО;
- для работы с токеном;
- для работы с ключами ЭП;
- для работы с иными финансовыми (бухгалтерскими) программами;
- для доступа к электронной почте, в социальные сети, службы мгновенных сообщений и т.д.

2.11. Делайте резервные копии Ваших данных и диски аварийного восстановления операционных систем Устройств.

2.12. Обязательно завершайте работу с системой ДБО, с интернет-браузером, с Устройством путём выполнения стандартных процедур (нажатия соответствующей кнопки в интерфейсе программ, кнопки питания Устройства).

3. Обеспечение безопасности токенов:

3.1. Производите замену ключей ЭП до истечения срока их действия и во всех случаях увольнения и(или) смены полномочий и(или) лиц, имеющих доступ к системе ДБО или право подписи доверенностей на получение ключей ЭП.

3.2. Используйте только аппаратные криптоустройства с неизвлекаемыми ключами, подключаемыми через USB-порт – токены (Рутокен и(или) «iBank2 Key»). Это снизит вероятность, что ключи ЭП будут незаметно скопированы и использованы в другом месте.

3.3. Всегда отсоединяйте токен от Устройства, закончив работу с системой ДБО. Храните токены в условиях, исключающих возможность несанкционированного доступа к ним третьих лиц. Это снизит риск, что в Ваше отсутствие не произойдёт несанкционированное использование системы ДБО вредоносной программой или злоумышленником.

3.4. Если в работе Вами используется больше одной ЭП, то следует хранить ключи на разных токенах и использовать их для работы с системой ДБО через различные Устройства. Это сделает невозможным отправку электронного платёжного документа вредоносной программой, заразившей одно из Устройств.

3.5. Скачивайте программное обеспечение iBank2 (плагин для браузера "BIFIT Signer", драйверы для USB-токенов) только по ссылкам, размещенным на официальном сайта Банка. Проводите проверку целостности плагина BIFIT Signer. Это возможно сделать с использованием встроенных средств операционной системы, для чего необходимо зайти в свойства файла (путем нажатия правой кнопки мыши на файле) и просмотреть закладку "Цифровые подписи". Имя подписавшего должно быть "Open Joint-Stock Company BIFIT" или "BIFIT".
Проверка целостности мобильного приложения "ЗЕНИТ Бизнес" проводится автоматически операционной системой мобильного устройства. Устанавливайте мобильное приложение только из официальных магазинов приложений (Google Play, Apple AppStore), перед установкой убедившись, что автором приложения указан "PJSC Bank ZENIT" или "BANK ZENIT, PAO".?

4. Дополнительные меры по обеспечению безопасности:

4.1. Используйте для оперативного контроля операций в системе ДБО альтернативные механизмы, такие как SMS-информирование. В связи с возможностью круглосуточного проведения операций с использованием системы ДБО, обеспечьте постоянный контроль поступающей информации об операциях в виде SMS-сообщений и реагирование в случае несанкционированных операций. Не отключайте на своих мобильных Устройствах в ночное время звуковое уведомление о получении SMS.

4.2. Используйте для подтверждения операций в системе ДБО одноразовые SMS-пароли. Это снизит риск несанкционированных переводов денежных средств даже в тех случаях, когда вредоносная программа получила полный доступ к Вашему Устройству с подключённым токеном. SMS-сообщения, кроме пароля, содержат часть реквизитов платежа, дополнительный контроль которых снизит риск подмены получателя и(или) суммы платежа вредоносной программой.

4.3. Внимательно проверяйте суммы и реквизиты проводимых платежей в приходящих информационных сообщениях или сообщениях с одноразовыми паролями, не подтверждайте подозрительные операции, и незамедлительно информируйте Банк о попытках и (или) выявленных фактах мошеннических платежей.

4.4. При использовании для подтверждения операций в системе ДБО одноразовых SMS-паролей и(или) при использовании SMS-информирования, обеспечьте, чтобы мобильные Устройства, используемые для получения SMS-сообщений, не использовались Вами для проведения (инициирования и подтверждения) операций в системе ДБО.

4.5. Обеспечьте правильность указания в оформляемых Вами заявлениях и в других документах номеров телефонов для связи, номеров мобильных телефонов для получения услуги SMS-информирования и получения SMS-паролей, иных координат для связи с Вами (с уполномоченными лицами).

5. Безопасность при работе с публичными информационными ресурсами в сети Интернет:

5.1. Не посещайте непроверенные интернет-сайты, особенно интернет-сайты, которые распространяют пиратское программное обеспечение или аудио/видео файлы, так как на большом количестве подобных сайтов размещён специальный программный код, заражающий Устройства различного рода вирусами и иными видами вредоносного программного обеспечения.

5.2. Не открывайте файлы или интернет-ссылки, пришедшие к Вам по публичным информационным каналам (по электронной почте, через SMS и с помощью иных служб мгновенных сообщений, из социальных сетей и т.п.) даже от знакомых Вам людей, если только они не были присланы по Вашей просьбе или дополнительно подтверждены отправителем альтернативным способом. Сообщение может быть отправлено с подделанным адресом отправителя электронной почты, или от имени знакомого Вам человека вредоносной программой, захватившей контроль над его компьютером, мобильным устройством или учётной записью в социальной сети, в почтовой системе.

5.3. Исключите возможность запуска на исполнение получаемых файлов, включая выполняемые файлы, макросы в файлах Microsoft Office (например, в файлах Word или Excel) или скрипты с расширениями .js и .vbs.

5.4. В ряде случаев злоумышленниками могут создаваться в сети Интернет поддельные сайты, полностью имитирующие официальный сайт Банка, сайты Банковской группы ЗЕНИТ, распространяться поддельные приложения, использующие символику (зарегистрированные товарные знаки), наименование и интерфейс настоящих сайтов и приложений.

5.5. Сообщите в Банк о случае выявления Вами ложного Web-сайта, мобильного приложения Банка или о полученных сведениях подобного рода.

5.6. Схемы мошенничества, как правило, выглядят следующим образом.

- Злоумышленники распространяют вредоносные программы через различные интернет-ресурсы — от социальных сетей до обычных новостных сайтов или электронной почты. Если на Устройстве отсутствуют настройки безопасности, актуальные обновления программ безопасности, интернет-браузера или другого программного обеспечения, поражение Устройства вредоносным программным обеспечением возможно даже просто при подключении Устройства к сети Интернет или к недоверенной сети.
- Клиент, Устройство которого заражено, при попытке войти в систему ДБО перенаправляется на поддельные («фишинговые») интернет-сайты, которые внешне практически не отличаются от подлинного сайта Банка.
- На поддельном сайте Вас могут попросить ввести идентификаторы и пароли, мобильный телефон и другие персональные данные, необходимые мошенникам для обмана.

5.7. Как распознать «подделку»?

- операция может проводиться в незащищённом режиме (иконки интернет-браузера, указывающие на работу в защищённом режиме, не активны);
- при входе на сайт Банка интернет-браузер может предупреждать, что сертификату безопасности сайта нельзя доверять;

- адрес может не совпадать с официальными адресами сайта Банка в сети Интернет: http://www.zenit.ru, https://www.zenit.ru, https://cb.zenit.ru/;
- проверяйте, что установлено защищённое SSL-соединение с официальным сайтом системы ДБО: **https**://cb.zenit.ru.

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

ВНИМАНИЕ!

При подозрении или в случае:

- несанкционированного списании денежных средств со счёта,
- утраты токена и(или) Устройства, с которого осуществлялась работа с системой ДБО, либо мобильного Устройства, на которое получаете одноразовые SMS-пароли (потере, хищении, нарушении работоспособности), или при вынужденной срочной смене мобильного телефонного номера,
- доступа третьих лиц к токену либо к Устройству с работающей системой ДБО без Вашего ведома,
- компрометации секретных реквизитов (логина, пароля, кодового слова),
- обращения к Вам от имени Банка с просьбой сообщить секретные реквизиты,
- отсутствия возможности подключения к веб-сайту системы ДБО,
- входа и(или) работы с поддельным сайтом Банка, системы ДБО,
- нестабильной и(или) нестандартной работы Устройства и(или) системы ДБО

следует незамедлительно прекратить работу в системе ДБО, извлечь из Устройства токен, выключить Устройство и обратиться в Банк с предоставлением полной информации о случившемся, что поможет оперативно приостановить возможные мошеннические операции и предотвратить финансовые потери, по следующим номерам телефонов круглосуточного колл-центра:

8 (800) 500-66-77 или +7 (495) 777-57-07, +7 (495) 937-07-37