

Требования
по защите информации при использовании системы
Интернет Клиент-Банк «iBank2»

Для обеспечения достаточного уровня защиты информации при работе с системой «iBank2» необходимо соблюдать следующие меры компьютерной безопасности:

1. Использовать только лицензионное ПО (операционные системы, офисные пакеты, антивирус и пр.);
2. Обеспечить своевременное автоматическое обновление системного и прикладного ПО при выходе соответствующих обновлений, особенно ОС Windows и Java;
3. Применять на рабочем месте лицензионные средства антивирусной защиты (NOD32, Антивирус Касперского и пр.), обеспечить возможность своевременного автоматического обновления антивирусных баз, настроить автоматическое удаление обнаруженного вирусного программного обеспечения (далее – ВПО), а также ежедневно производить полное сканирование компьютера в автоматическом режиме;
4. Установить пароль на изменение настроек антивируса с целью недопущения несанкционированного изменения параметров антивирусной защиты;
5. Активировать и обеспечить работоспособность штатных средств защиты информации операционной системы Windows (в зависимости от версии), в том числе:
 - a. Включить систему защиты брандмауэр Windows (Панель управления – Брандмауэр Windows) или установить персональный межсетевой экран (*firewall*) стороннего производителя
 - b. Активировать «Защитник windows»
 - c. Активировать «Контроль учетных записей» (UAC)
6. Ограничить доступ к компьютеру из любых компьютерных сетей (ЛВС организации, Интернет, и др.), а также запретить/исключить доступ/посещение любых Интернет-сайтов за исключением доступа к системе «iBank2» ПАО АКБ «Приморье» (URL адрес: **https://client.primbank.ru/**, IP адрес: **91.213.113.5**), а также доступа к серверам обновлений операционной системы и антивирусных баз; Рекомендуется ограничить или полностью отказаться от приема внешней (из сети Интернет) электронной почты;
7. Работу на компьютере осуществлять только с правами ПОЛЬЗОВАТЕЛЯ, с обязательной установкой пароля на вход в операционную систему;
8. Исключить использование любого программного обеспечения развлекательного и социального характера и др., за исключением необходимого для работы;
9. Подсоединять носитель ключевой информации (USB-токен, Смарт-Карту) к компьютеру **ТОЛЬКО** в момент начала работы с интернет-банкингом, и **ОБЯЗАТЕЛЬНО** извлекать его из компьютера сразу после окончания работы;
10. Не оставлять носитель ключевой информации (USB-токен, Смарт-Карту) в компьютере, когда не производится работа с ним и в нерабочее время;
11. Хранить токен так, чтобы исключить несанкционированный доступ к нему посторонних лиц, согласно Правилам хранения и использования Ключевого носителя Договора;
12. При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями;
13. Не передавать ключи ЭП ИТ-сотрудникам для проверки работы системы "Интернет Клиент-Банк", проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок *только лично владелец ключа ЭП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа системы, и лично ввести пароль, исключая его компрометацию;*
14. При увольнении сотрудника, имевшего технический доступ к секретному (закрытому) ключу ЭП, обязательно позвонить в банк и заблокировать ключ ЭП;
15. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой "Интернет-банк", произвести проверку

- антивирусными средствами для обеспечения отсутствия вредоносных программ на компьютере;
16. При возникновении подозрений на компрометацию (копирование) секретных (закрытых) ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить в банк и заблокировать ключи ЭП;
 17. Регулярно проводить контроль сумм и получателей платежных документов в информационном окне системы «iBank2», а также контролировать количество и сумму отправленных документов;
 18. Регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее Вас подразделение ПАО АКБ «Приморье» обо всех подозрительных или несанкционированных операциях;
 19. В случае выхода из строя ПК, либо некорректной работы системы «iBank2», или признаков наличия вредоносного ПО, а также нестандартного поведения ПК при работе с USB-токеном или Смарт-картой, **необходимо незамедлительно прекратить работу на ПК, вынуть USB-токен или Смарт-карту, отключить ПК от локальной корпоративной сети, срочно запросить в ПАО АКБ «Приморье» выписку по счету, и сообщить о данном случае Вашему Руководителю / ИТ-специалисту, а также позвонить в службу технической поддержки систем ДБО ПАО АКБ «Приморье» для получения рекомендаций:**
 - 8 (423) 2-433-519 – для звонков из г. Владивосток**
 - 8 (423) 2-400-300 – для звонков из г. Владивосток**
 - 8-800-200-20-86 – для звонков из других городов (звонок бесплатный)**
 20. **Основными признаками наличия ВПО являются:**
 - наличие платежных поручений, созданных или отправленных в Банк, которые Клиент самостоятельно не создавал;
 - уведомления от антивируса и прочих средств защиты информации;
 - наличие программ удаленного администрирования, как то Radmin, VNC, TeamViewer, AmmyAdmin и пр.;
 - нетипичное поведение ПК: мерцающие и сворачивающиеся окна, дергание мыши, выдача ошибок или дополнительных окон, которые ранее не появлялись;
 - наличие в автозагрузке операционной системы посторонних процедур;
 - наличие посторонних процессов в диспетчере процессов;
 - изменение в свойствах обозревателя нетипичных настроек прокси-сервера;
 - уведомление из Банка о подозрении на наличие ВПО.
 21. При обнаружении несанкционированных платежных операций информировать руководство, обязательно позвонить в Банк и заблокировать ключи ЭП, написать официальное письмо, а также обратиться с соответствующим заявлением в правоохранительные органы;
 22. Работоспособность поврежденного ПК не восстанавливать до проведения технической экспертизы. Работу с системой «iBank2» проводить только на новом ПК с соблюдением всех рекомендаций по информационной безопасности;
 23. В целях оценки текущего состояния уровня защищенности компьютера, с которого осуществляется работа с системой ДБО «iBank2», и необходимости принятия действенных мер по усилению защиты, рекомендуется назначить ответственного сотрудника (ИТ-специалиста), который произведет заполнение Анкеты (**см. «Анкета оценки информационной безопасности персонального компьютера»**) с предоставлением результата Руководству организации, а также будет осуществлять регулярный контроль состояния защищенности компьютера и информирование обо всех выявленных нарушениях.

Рекомендации по обеспечению безопасности с помощью дополнительных услуг:

- Подключить услугу «**IP-фильтрация**» (информация, передаваемая в Банк по системе Интернет Клиент-Банк «iBank2», будет обработана только в случае совпадения IP-адреса передающего компьютера, с IP-адресом Клиента, хранящимся в базе данных Банка);
- Использовать **ОТР-токен** (генератор одноразовых паролей):

1. Аутентификация с помощью одноразового персонального пароля при входе в систему «iBank2».

Вход в систему выполняется после дополнительного подтверждения путем ввода одноразового пароля, полученного с ОТР-токена;

2. Авторизация с помощью одноразового персонального пароля при совершении платежа в системе «iBank2» с использованием ОТР-токена.

Направление платежного поручения в Банк осуществляется с дополнительным подтверждением путем ввода одноразового пароля, полученного с ОТР-токена.

- Подключить услугу «**SMS информирование**» для оперативного контроля движения средств по счету и входа в систему «iBank2»:

1. «SMS оповещение», типы SMS уведомлений:

- ✓ Об отвлении документа;
- ✓ О поступлении в банк документа;
- ✓ О входящих документах;
- ✓ О движении по счету;
- ✓ О входе в систему;
- ✓ О текущих остатках;
- ✓ Выписка по счету.

2. «SMS подтверждение на отправку платежей в «iBank2».

Направление платежного поручения в Банк осуществляется с дополнительным подтверждением путем ввода одноразового пароля (полученного в SMS - сообщении);

3. «Одноразовый SMS пароль на вход в «iBank2».

Вход в систему выполняется после дополнительного подтверждения путем ввода одноразового пароля (полученного в SMS - сообщении).

Анкета

**Оценки информационной безопасности персонального компьютера
(с которого осуществляется работа с системой ДБО Интернет Клиент-Банк «iBank2»).**

Дата выполнения контроля: «__» _____ 20__ г.

№ п/п	Рекомендация	Отметка о выполненном контроле
1.	Установлено и используется лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.).	Да Нет по причине:

2.	Обеспечивается своевременное автоматическое обновление системного и прикладного ПО (операционные системы, офисные пакеты, java и пр.).	Да Нет по причине:
3.	Установлено и постоянно включено Антивирусное программное обеспечение с парольной защитой с целью недопущения несанкционированного изменения настроек, ежедневно производится обновление антивирусных баз.	Да Нет по причине:
4.	Программное обеспечение развлекательного, социального характера и др., за исключением необходимого для работы, на компьютере не установлено.	Да Нет по причине:
5.	Включен и работает сервис защиты Брандмауэр Windows (Панель управления – Брандмауэр Windows), или другой персональный межсетевой экран (<i>firewall</i>).	Да Нет по причине:
6.	Доступ к компьютеру с системой ДБО «iBank2» запрещен из любых компьютерных сетей (ЛВС организации, Интернет, и др.).	Да Нет по причине:
7.	Доступ в Интернет с компьютера ЗАПРЕЩЕН за исключением доступов: <ul style="list-style-type: none"> • к серверу системы «iBank2» ПАО АКБ «Приморье» (URL адрес: https://client.primbank.ru/, IP адрес: 91.213.113.5); • к доверительным источникам обновлений системного, прикладного ПО и антивирусных баз. 	Да Нет по причине:
8.	Удаленный доступ к рабочей станции по протоколу RDP или посредством различного ПО для удаленного управления (Teamviewer , Radmin, DameWare, Ammyu Admin и прочие) ЗАПРЕЩЕН. Программы удаленного доступа, включая выше указанные - на компьютере отсутствуют	Да Нет по причине:
9.	Работа на компьютере осуществляется только с правами ПОЛЬЗОВАТЕЛЯ	Да Нет по причине:
10.	Носитель ключевой информации (USB-токен, Смарт-Карта) подключается к компьютеру ТОЛЬКО в момент начала работы с интернет-банкингом, и ОБЯЗАТЕЛЬНО извлекается из компьютера сразу после окончания работы.	Да Нет по причине: