ЗАЯВЛЕНИЕ
о выполнении требований по защите от вредоносного кода

_____ , в лице _____(далее - Клиент), действующего на основании _____, заявляет о выполнении требований по защите от вредоносного кода:

1. К средствам защиты от вредоносного кода относятся средства, используемые для:
   - выявления и обезвреживания вредоносного кода (антивирусы);
   - межсетевого экранирования рабочего места или корпоративной сети;
   - Web-фильтрации;
   - обнаружения и предотвращения вторжений;
   - контроля выполнения приложений.

2. На рабочих местах ответственных сотрудников установлены и непрерывно используются следующие средства защиты от вредоносного кода:
   - антивирусная программа _____

с

функциями контроля выполнения приложений, проверки почты на наличие вредоносного кода, проверки безопасности Web-сайтов.

3. Обновление антивирусного средства на рабочем месте производится автоматически.

4. Обеспечивается непрерывное использование средств защиты от вредоносного кода и периодический контроль целостности системного, прикладного и специального программного обеспечения;

5. Полная проверка рабочего места на наличие вредоносных программ производится не реже, чем 1 раз в сутки.

1. Регулярно проводится обновление прикладного программного обеспечения рабочего места.

2. Регулярно производится установка пакетов обновления безопасности операционной системы рабочего места.

3. На рабочем месте используется лицензионное программное обеспечение или программное обеспечение, полученное исключительно из доверенных источников.

4. На рабочем месте используется для работы в системе учетная запись пользователя, не входящая в группу «Локальные администраторы» или аналогичную группу пользователей.

5. С рабочего места осуществляется вход в сеть Интернет исключительно для подключения к сайту Банка или для обновления антивирусной программы, прикладного или системного программного обеспечения.

6. Съемные носители информации перед использованием на Рабочем месте предварительно проверяются на выделенном компьютере на наличие вредоносного кода.

7. Для защиты ключей ЭП от хищения вредоносными программами рекомендуется использовать аппаратное устройство.

8. Установите и регулярно обновляйте специальное антивирусное ПО для мобильных устройств.

9. Скачивайте и устанавливайте программное обеспечение из проверенных источников (рекомендованных производителями мобильных устройств).

10. На устройствах, используемых для работы с приложением, не рекомендуется

выполнять процедуры получения доступа к файловой системе устройства (Jailbreak, Rooting). Такие операции наносят существенный ущерб системе безопасности, предоставленной производителем устройства.

Примечание:

В целях безопасности Банк может запретить доступ к приложению с устройств, на которых была осуществлена процедура получения доступа к файловой системе.

11. Скачивайте и устанавливайте приложение "Мобильный Банк для корпоративных клиентов" только из официальных магазинов приложений Google Play, AppStore. Разработчиком приложения должна быть указана компания "БИФИТ".

12. Не записывайте и не сохраняйте свой код доступа к приложению на устройстве, с которого осуществляется работа в приложении.

13. Не сообщайте код доступа третьим лицам, в том числе сотрудникам банка.

14. При получении любых сообщений или писем, связанных с работой приложения, обращайте внимание на отправителя. Подобные сообщения должны поступать только с официального сервисного номера или адреса электронной почты вашего банка. Не переходите по ссылкам и не открывайте вложения из писем от подозрительных или неизвестных отправителей.

15. После завершения работы с документами и банковскими счетами каждый раз выполняйте выход из приложения (Меню → Выход).

16. При подозрении, что ваш код доступа к приложению стал известен посторонним лицам или при получении уведомлений об операциях по счету, которых вы не совершали, немедленно обратитесь в ваш банк и заблокируйте свою учетную запись.

_____ _____ (_____)

(должность руководителя) (подпись) (Ф.И.О.)

М.П.