Приложение 4
К Правилам пользования системой
дистанционного банковского обслуживания
банковских счетов физических лиц в АО «ИТ Банк»

Памятка безопасного использования Системы «Интернет-Банк» для физических лиц АО «ИТ Банк»

На персональном компьютере, ноутбуке:

1. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
2. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
3. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора.
4. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
5. Установить и своевременно обновлять на компьютере антивирусное программное обеспечение (далее – ПО) (NOD32, AVP Kaspersky, Symantec AntiVirus и т.д.). Можно скачать бесплатную версию Kaspersky, Dr.Web, но лучше приобрести и регулярно обновлять лицензионную версию антивирусного ПО.
6. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
7. При выходе в Интернет использовать сетевые экраны (Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам сети Интернет.
8. Запретить в межсетевом экране соединение с Интернет по протоколам ftp, smtp. Разрешить соединения smtp только с конкретными почтовыми серверами, на которых зарегистрированы Ваши электронные почтовые ящики.
9. Не давать разрешения неизвестным программам выходить в Интернет.
10. При работе в Интернет не соглашаться на установку каких-либо дополнительных программ.

При использовании мобильного приложения рекомендуется:

1. Устанавливать мобильное приложение только по ссылкам на официальном сайте Банка elf.faktura.ru/elf/app, или в авторизованном магазине приложений (Google Play);
2. Установить пароль для доступа на Ваше мобильное устройство;
3. Установить и своевременно обновлять лицензионные антивирусные программы на Вашем мобильном устройстве;
4. Всегда совершать выход из Системы после окончания работы;
5. Не хранить Логин и Пароль для доступа в Систему на своём мобильном устройстве или в общедоступном месте и не сообщать его никому;
6. Ни при каких обстоятельствах не передавать и не сообщать никому (в том числе работникам Банка, родственникам и друзьям) данные для входа в мобильное приложение, пароли для подтверждения платежей, а также номера Ваших карт и CVV2/CVC2 коды;
7. Никогда не отвечать на электронные письма, входящие звонки, SMS-сообщения, письменные/устные обращения, в которых запрашивается персональная информация;

8. В случае утери мобильного телефона или в случае обнаружения подозрительных действий, совершенных от вашего имени в Системе, незамедлительно сменить Логин и Пароль, а также обратиться в Банк.
9. По окончании работы в мобильном приложении обязательно необходимо завершить сеанс работы с Системой выбором пункта меню «Выйти».