ПАМЯТКА КЛИЕНТУ

Для обеспечения безопасности при работе с Системой «Клиент-Банк» Клиент должен:

- Выделить отдельный компьютер (далее – ПК) для работы с Системой «Клиент-Банк» и определить должностное лицо, ответственное за обеспечение безопасности информации и эксплуатации СКЗИ.
- Не использовать на ПК нелицензионное программное обеспечение (операционную систему, иное программное обеспечение) (далее – ПО). Клиент предупрежден, что оно может заведомо содержать вредоносный код.
- Установить на ПК антивирусную программу с актуальными базами, регулярно обновляемую.
- При первом входе в систему, а так же регулярно (один раз в месяц) менять пароли на Систему «Клиент-Банк»
- Ежегодно производить перегенерацию криптографических ключей.
- Использовать секретные ключи (подключение внешнего носителя с ключом) только в момент работы с Системой «Клиент-Банк». Извлекать ключевой носитель из ПК в другое время. Не оставлять внешний носитель с ключом постоянно подключенным к ПК.
- Не оставлять секретные Ключи без присмотра. Клиент предупрежден, что в противном случае он рискует скомпрометировать секретные ключи. Никогда и никому не сообщать логины \ пароли Систем «Клиент-Банк» и тем более не доверять секретные ключи, включая родственников и сотрудников Банка.
- Обеспечить соответствие пароля доступа к ключу ЭЦП требованиям сложности (пароль должен быть не менее 6 символов, состоять из прописных и\или строчных латинских букв с цифрами и\или символами);
- Избегать использования Системы «Клиент-Банк» на чужих компьютерах или в интернет-кафе, на подобных ПК Вы рискуете скомпрометировать свои ключи \ логин \ пароль.
- Контролировать действия IT-специалистов, особенно внештатных, в момент технического обслуживания, установки программного обеспечения на компьютер с установленной Системой «Клиент-Банк», не сообщать IT-специалистам пароли для проверки работы Системы – делать это самостоятельно.
- Осуществлять постоянный контроль за отправляемыми платежными документами при работе с Системой «Клиент-Банк», а также за состоянием своего банковского счета не реже 3 раз в операционный день с интервалом не более 3 часов и не менее 1 часа.
- Проверять информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему.
- Не использовать ПК с установленной системой «Клиент-Банк» для работы с электронной почтой. Клиент предупрежден, что электронные письма - это самый популярный способ распространения вредоносного ПО.
- Перед открытием внешнего подключаемого носителя – обязательно проверить его содержимое на вирусы.

КЛИЕНТ ДОЛЖЕН НЕМЕДЛЕННО СООБЩИТЬ В БАНК в случае, если:

- Сломался ПК, на котором установлена Система «Клиент-Банк»;
- Заблокировался логин;
- Невозможно войти в Систему «Клиент-Банк»;
- Потерян контроль над носителем с секретными ключами;
- Потерян контроль над программой «Банк-Клиент»;

- Возникли подозрения в несанкционированном доступе к Системе «Клиент-Банк»:
    - Появляются \ *исчезают* документы \ *контрагенты*;
    - Остатки на банковском счете в Системе «Клиент-Банк» не соответствуют Вашим данным;
    - Есть проблемы при работе ПК («тормозит»), особенно при работе с Системой «Клиент-Банк»
    - Любое другое подозрение

Примерный сценарий реагирования Банка на инциденты в Системе «Клиент-Банк». При получении информации об инциденте, предусмотренной п.7.5. Регламента, сотрудник Банка:

- Идентифицирует пострадавшего клиента, фиксирует полученную информацию от Клиента об инциденте;
- Информирует непосредственное руководство о получении от Клиента информации об инциденте (Приложение №13);
- Дает Клиенту инструкции о совершении необходимых действий, сохранению доказательств. Приостанавливает исполнение ЭПД Клиента по Системе «Клиент-Банк»;
- Информирует официальным письмом банк – получатель денежных средств о факте инцидента и необходимости отменить операцию (транзакцию);
- Направляет (при необходимости) информационное письмо о факте совершения мошенничества в полицию;
- Собрать журналы работы с Системой «Клиент-Банк» пострадавшего Клиента за 2 месяца до инцидента;
- Осуществить выезд к пострадавшему Клиенту с целью сбора дополнительной информации об инциденте.

РИСКИ, СВЯЗАННЫЕ С НЕСВОЕВРЕМЕННЫМ СООБЩЕНИЕМ В БАНК О СЛУЧАЯХ УТРАТЫ ИЛИ КОМПРОМЕТАЦИИ СЕКРЕТНЫХ КЛЮЧЕЙ ЭЦП, НЕСЕТ КЛИЕНТ.