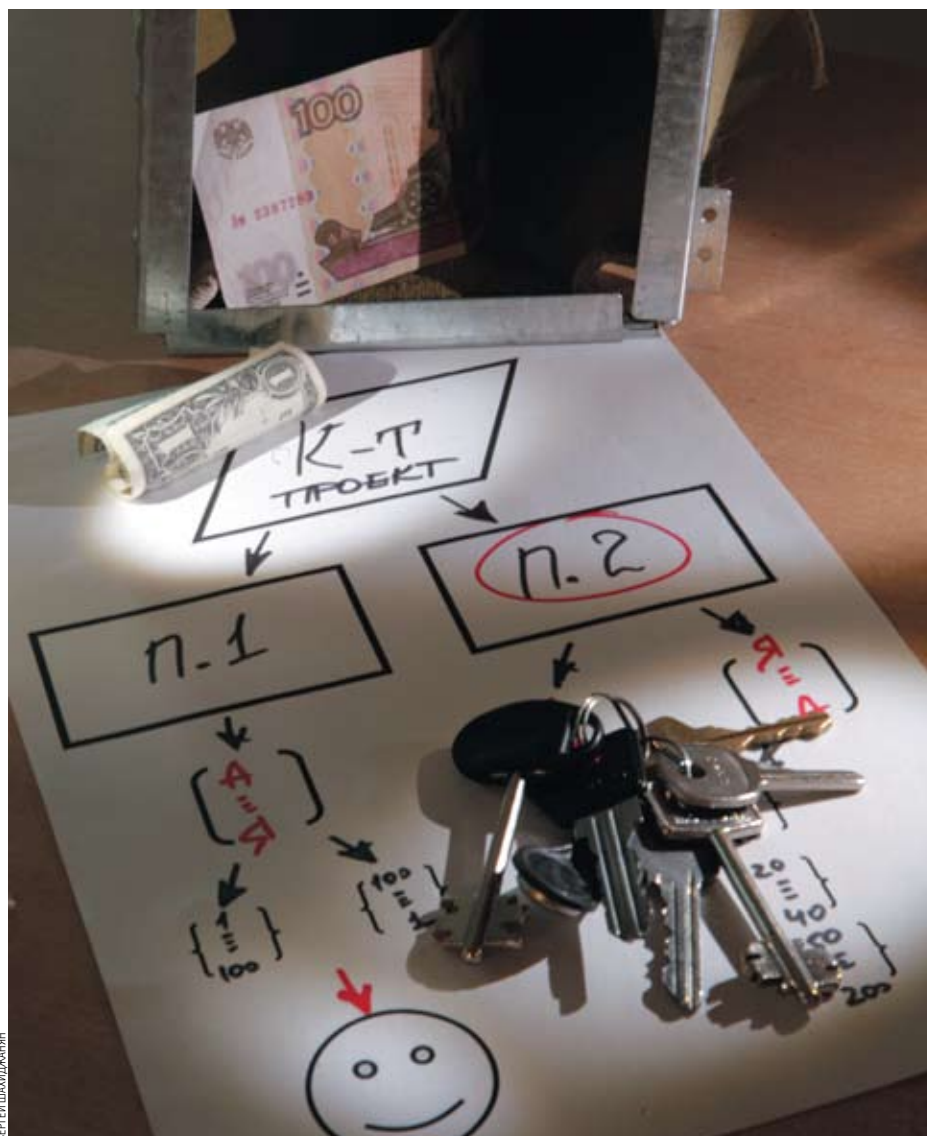


В BSGV Direct, системе управления счетами физических лиц через интернет, для обеспечения конфиденциальности пользовательских данных применяются средства по стандартам Банка России, рассказывает Елена Шевелева, генеральный директор петербургского филиала банка «Сосьете Женераль Восток» (BSGV). Для обеспечения более высокого уровня конфиденциальности и безопасности личной информации в ноябре 2009 года банк внедрил виртуальную клавиатуру для входа в BSGV Direct.

ПРЕДУПРЕЖДЕН — ЗНАЧИТ ВООРУЖЕН

Между тем никогда не стоит пренебрегать инструкциями, которые дают и сами банки. Прежде всего нужно обязательно пользоваться антивирусной программой и своевременно ее обновлять. Это касается и частных, и корпоративных пользователей. Программное обеспечение должно быть лицензионным. Не стоит соединяться с компьютера, предназначенного для работы в системах интернет-банкинга, с сайтами сомнительного содержания, а также открывать без проверки файлы, полученные в почтовых сообщениях и на съемных носителях от неизвестных лиц, советуют специалисты ВТБ24. И вообще лучше ограничить доступ в интернет с компьютера, где установлена система online-банкинга, оставив возможность подключения только к серверам банка системы. Доступ ко всем другим сайтам с этого компьютера компании должен быть закрыт, так же как и доступ к данному компьютеру из интернета.

Файлы с ключами ЭЦП нужно хранить на флешках и подключать их к компьютеру только на время работы с системой. А сами флешки в нерабочее время



ХАКЕРЫ НАУЧИЛИСЬ ПОДБИРАТЬ КЛЮЧИ К ВЕБ-САЙТАМ БАНКОВ

лучше прятать в сейф, рекомендует господин Шелин. Хорошо бы дублировать такие файлы, ведь во время работы с системой на зараженном компьютере ключи могут «уплыть» с флешки так же легко, как если бы они лежали на жестком диске. Если в выписке обнаружены несанкционированные расходные операции, утерян или похищен ключевой носитель с закрытым ключом ЭЦП или компьютер, на котором был установлена система «Банк-Клиент», необходимо срочно обращаться в банк, отмечают в пресс-службе банка СИАБ. Для более надежной защиты ключей в банке также рекомендуют пользоваться специальными устройствами — USB-токенами. Это аналог смарт-карты с разъемом USB, обеспечивающий надежное хранение ключей ЭЦП. Секретный ключ ЭЦП находится в защищенной памяти токена и не может быть скопирован из токена без ведома его владельца.

Необходимо использовать сложные пароли и периодически их менять. «Нельзя использовать в качестве пароля числа, которые легко угадать, например, дату рождения», — говорит госпожа Шевелева. Она также советует не пользоваться интернет-банком в общественных местах и каждый раз проверять соответствие дизайна и наполнения привычному виду сайта банка, так как иногда мошенникам удается с точностью воспроизвести содержимое сайта, обновлять новости и поддерживать все имеющиеся страницы. Если при вводе логина и пароля для входа в систему дополнительно запрашиваются конфиденциальные сведения — это является вероятным признаком, что вы работаете с «чужой» страницей, отмечает госпожа Шевелева. ■





ПЕРВОБАНК
ПЕРВЫЙ ОБЪЕДИНЕННЫЙ БАНК

|812| 448 36 00
ул. 7-я Красноармейская, 25А

-  **Балтийская**
-  **Фунзенская**
-  **Технологический институт**

ВКЛАДЫ НА ВАШ ВКУС

Открытое акционерное общество «Первый Объединенный Банк». Генеральная лицензия ЦБ РФ № 3461 от 27.02.2008 г.