РОССИЙСКИЙ ПРОФЕССИОНАЛЬНЫЙ СОЮЗ
ЖЕЛЕЗНОДОРОЖНИКОВ И ТРАНСПОРТНЫХ СТРОИТЕЛЕЙ

ЦЕНТРАЛЬНЫЙ КОМИТЕТ

109029 г. Москва, ул. Новорогожская, дом 29

Тел.: 262-58-73, 262-53- 66
Факс: 262-72-80

20.09.2012 г. № И-530/11

На №_____ от _____

ДОРПРОФЖЕЛ

ОРГАНИЗАЦИЯМ ПРЯМОГО ПОДЧИНЕНИЯ ЦК ПРОФСОЮЗА

О защите информации

Информационное письмо

В связи с необходимостью защиты программно-технических средств от несанкционированного доступа и в целях обеспечения информационной безопасности базы данных программных средств:

1. Разработать и принять политику информационной безопасности Автоматизированной системы управления профсоюзным бюджетом на базе программного обеспечения 1С, в том числе, организационно- распорядительные и программно-технические меры направленные на:
   - защита серверов
   - защита рабочих станций
   - управление доступом к информационным ресурсам
   - администрирование системы
   - ответственность за нарушение политики информационной безопасности
2. Назначить ответственного за обеспечение информационной безопасности.
3. На всех рабочих станциях (компьютерах) пользователей установить средства антивирусной защиты.
4. Постоянно производить антивирусный контроль программ и файлов данных.
5. Обновления антивирусных баз производить регулярно.
6. Защитить с помощью паролей персональный компьютер.
7. Переустановить программное обеспечение «Банк-Клиент» на отдельно выделенный компьютер с помощью специалистов банка.
8. Защитить с помощью паролей персональную ключевую информацию, хранящуюся на персональных компьютерах пользователей, в том числе «Банк-Клиент».
9. Персональные ключи хранить в тайне каждым пользователем.
10. Персональные ключи - электронно-цифровую подпись хранить в сейфе.

11. Систематически производить замену паролей и ключей.
12. Сотрудники несут ответственность за нарушение правил использования средств защиты информации и хранение устройств идентификации. Электронные идентификаторы не должны храниться рядом с компьютером.
13. Обратиться в банк с письмом о проведении представляемых платежей после поступления реестра с указанием количества и суммы платежей.
14. Обязать пользователя немедленно ставить в известность ответственного за обеспечение информационной безопасности в случае утери индивидуального устройства идентификации или при подозрении компрометации персональных ключей и паролей.

Председатель Профсоюза **Н.А. Никифоров**

РОССИЙСКИЙ ПРОФЕССИОНАЛЬНЫЙ СОЮЗ
ЖЕЛЕЗНОДОРОЖНИКОВ И ТРАНСПОРТНЫХ СТРОИТЕЛЕЙ

ЦЕНТРАЛЬНЫЙ КОМИТЕТ

ДОРПРОФЖЕЛ

109029 г. Москва, ул. Новорогожская, дом 29

Тел.: 262-58-73, 262-5366
Факс: 262-72-80

№ И-71/11 от 18.02.2013 г.
На №

О мерах по защите информации

Информационное письмо

Обеспечение безопасности финансовых операций в системе дистанционного банковского обслуживания Банка – это ответственность пользователя. Рекомендации о мерах по защите информации и применяемый широкий комплекс мер по обеспечению безопасности операций в системе дистанционного банковского обслуживания (далее- система ДБО банка) «Клиент- Банк» необходимо принять к руководству в работе централизованных бухгалтерий Профсоюза.

Банк обращается к пользователям системой ДБО «Клиент-Банк» и обращает внимание на необходимость оперативной связи с сотрудником операционного отделения для уточнения информации о последних платежах, **в случае, если программа « Клиент-Банк» или компьютер в целом неожиданно вышли из строя.** В большинстве случаев именно таким приемом пользуются мошенники, чтобы Вы не сразу смогли увидеть информацию о мошеннических действиях.

В случае же оперативного оповещения сотрудников банка о сбое системы «Клиент-Банк» - несанкционированный платеж, вероятнее всего, будет остановлен.

Рекомендации пользователю по обеспечению безопасной работы с системой «Клиент-Банк» и об основных мерах обеспечения безопасности при работе с системой дистанционного банковского обслуживания «Клиент-Банк», предлагаемых банком:

1.Никому не сообщайте логины и пароли, не записывайте их на бумаге, мониторе или клавиатуре; Не используйте функцию запоминания логина и пароля в браузерах; Не используйте одинаковые логин и пароль для доступа к различным системам;

2. Регулярно, не реже одного раза в месяц, производите смену пароля. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Не используйте в качестве пароля имена, памятные даты, номера телефонов; При первом входе в систему ДБО Банка необходимо изменить пароль доступа и хранить его в секрете;

3. Если Вы получили на электронную почту письмо с просьбой обновить персональную информацию, содержащее ссылку на какой-либо сайт (в том числе – сайт Банка) - перезвоните в Службу технической поддержки банка и сообщите о письме. Банк никогда не просит передать данные по электронной почте. Не от-

крывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах и не отвечайте на них;

4. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное ПО), способное украсть ваши идентификационные данные для входа в Систему;

5. Не позволяйте третьим лицам производить за Вас генерацию ключей ЭЦП;

6. Не передавайте третьим лицам и не храните ключевой носитель ЭЦП в общедоступных местах, допускающих возможность его несанкционированного использования или копирования;

7. Присоединяйте ключевой носитель ЭЦП к компьютеру только непосредственно перед операцией подписи документов. По окончанию операции подписи - извлекайте ключевой носитель из компьютера;

8. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверия источников;

9. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе либо при выявлении сбоев в работе компьютера либо выходе из строя программы Клиент-Банк, незамедлительно отключите компьютер от сети интернет и сообщите в банк о неполадках компьютера;

10. Используйте дополнительные меры безопасности, предоставляемые банком – устройства **для хранения ключей eToken, СМС- и E-mail-уведомления, фиксация и контроль IP-адресов.** Для подключения необходимо обратиться в обслуживающее подразделение банка.

11.Необходимо использовать компьютер только для целей осуществления электронных платежей в системе ДБО Банка. Не следует использовать компьютер для посещения сайтов в сети Интернет, а также для получения писем с неизвестных адресов электронной почты – это может привести к заражению компьютера вирусами. Установите и настройте персональный межсетевой экран (firewall) на компьютере с системой ДБО Банка. Разрешите доступ с компьютера только на необходимые для работы IP-адреса (сервер системы ДБО Банка, серверы обновления операционной системы и антивируса).

12. Убедитесь, что Ваш компьютер не заражен вирусами. Установите и периодически проверяйте корректность работы антивирусного программного обеспечения. Ежедневно обновляйте антивирусные базы. Обращаем Ваше внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Ваших паролях и ключах электронной подписи.

13.Используйте лицензионное программное обеспечение, полученное только из проверенных и надежных источников. Для устранения существующих уязвимостей оперативно устанавливайте последние пакеты обновлений (Service Packs) и актуальные патчи безопасности для операционной системы и прикладного программного обеспечения. Удалите с компьютера программное обеспечение, не связанное с подготовкой и осуществлением электронных платежей в системе ДБО Банка.

14.Необходимо ограничить доступ к компьютеру, с которого осуществляется подключение к системе ДБО Банка. Для этого установите компьютер в недоступном для посторонних лиц месте. Желательно, чтобы это помещение закрывалось на ключ. Иногда одним ограничением физического доступа снимаются многие проблемы с безопасностью.

15.Необходимо установить пароль на доступ к компьютеру. Крайне желательно установить на рабочий стол «экранную заставку» со временем начала работы не более 5 минут (т.е. если ответственный сотрудник не работает за компьютером более 5 минут – компьютер включает «экранную заставку»), которую можно разблокировать только после ввода пароля. Длину пароля лучше выбрать не менее 8 символов. Желательно, чтобы этот пароль нельзя было угадать, т.е. цифры вашего телефона, имена близких людей, клички домашних животных и прочие известные о Вас факты в пароле использовать не стоит. Хранение пароля в электронном виде недопустимо!

16.После проведения процедуры перегенерации ключей электронной подписи необходимо перенести секретные ключи на внешний носитель (например, флэшку), а также удалить файл ключа электронной подписи с жесткого диска компьютера. Крайне внимательно относитесь к ключевому носителю, не оставляйте его без присмотра и не передавайте третьим лицам, извлекайте ключевые носители из компьютера, если они не используются для работы. Ключ должен храниться отдельно от компьютера в сейфе директора компании или у ответственного сотрудника и не должен быть доступен посторонним лицам (в том числе и сотрудникам компании, не связанным с проведением электронных платежей).

17.Ключевые файлы системы могут похищаться специалистами сторонних организаций во время ремонтных и настроечных работ на компьютере, а также при установке нового программного обеспечения. Не оставляйте ключевые файлы, дискеты и флэшки без присмотра во время работы данных специалистов с Вашим компьютером. Отправляя в ремонт компьютерное оборудование, проследите, чтобы на жестком диске компьютера не оставалось ключей электронной подписи и другой конфиденциальной информации.

18.Хорошей практикой является использование двух электронных подписей – подписи директора и бухгалтера. Подпись документов, в этом случае, рекомендуется осуществлять с разных компьютеров. Ключи электронной подписи необходимо хранить в разных местах, т.к. данная мера снижает вероятность их одновременной кражи злоумышленником.

19.При возникновении малейших подозрений на компрометацию ключей электронной подписи, а также о фактах выхода из строя компьютера с установленной системой ДБО «Банк-Клиент» необходимо незамедлительно информировать Банк для принятия неотложных мер по блокировке ключей электронной подписи с целью недопущения их несанкционированного использования.

Руководитель Департамента
финансов, учета и планирования-
главный бухгалтер З.А. Титова