ПАМЯТКА пользователю Системы «iBank2» для корпоративных клиентов.

Требования по обеспечению информационной безопасности при работе с Системой

При работе в сети Интернет рекомендуем Вам соблюдать общие правила безопасности, применяющиеся для защиты любых данных, хранящиеся на компьютерах:

1. Используйте только доверенные компьютеры с лицензионным программным обеспечением, установленным и запущенным антивирусным программным обеспечением (ПО) и персональным межсетевым экраном, своевременно обновляйте антивирусные базы. Регулярно проводите полную проверку компьютера на предмет наличия вредоносного ПО, своевременно обновляйте лицензионную операционную систему и браузеры. Будьте внимательны: в случае возникновения подозрений на мошенничество необходимо максимально быстро сообщить о происшествии в Банк с целью оперативного блокирования доступа!
2. При работе с электронной почтой не открывать письма и вложения к ним, полученные от неизвестных отправителей, не переходить по содержащимся в таких письмах ссылкам.
3. Своевременно обновлять операционную систему (установка патчей, критичных обновлений).
4. Доступ к рабочему месту и к ключевому носителю (usb-токен) с Системой должен быть предоставлен только Уполномоченным сотрудникам Клиента и техническому персоналу. Не допускайте посторонних лиц к компьютеру и usb-токену.
5. Не использовать права администратора при отсутствии необходимости. В повседневной практике входить в систему как пользователь, не имеющий прав администратора. Полностью заблокируйте сетевой доступ к компьютеру (удаленный доступ, удаленный поомщник и т.д.).
6. Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
7. Установить и своевременно обновлять на компьютере антивирусное ПО (NOD32, Kaspersky lab, Symantec AntiVirus и т.д.).
8. Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.
9. При выходе в Интернет использовать сетевые экраны (Kerio winroute, Outpost firewall и т.д.), разрешив доступ только к доверенным ресурсам Сети.
10. 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.
11. Не давать разрешения неизвестным программам выходить в Интернет.
12. При работе в Интернет не соглашаться на установку каких-либо дополнительных программ от недоверенных издателей.
13. При вводе личной информации, ПОМНИТЕ, что любой веб-адрес (URL) в адресной строке должен начинаться с "https". "S" означает "secure" (защищенный). Если в адресе не указано "https", это значит, что вы находитесь на незащищенном веб-сайте, и вводить данные нельзя.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей финансовых интернет-систем файлов с секретными ключами Электронной подписи (ЭП) и пароли, вводимые с клавиатуры. Трояны распространяются через e-mail, по каналам ICQ, Skype, через принадлежащие преступникам сайты.

14. Безопасность работы в Системе «iBank2» обеспечена комплексом организационных и логических мер, направленных на предотвращение мошенничества и разглашения конфиденциальной информации.

Со стороны пользователей безопасность работы в Системе обеспечивается выполнением следующих рекомендаций:

1. Храните usb-токен в максимально защищенном месте, исключающим доступ посторонних лиц (хранилище, сейф). Не оставляйте usb-токен в доступном месте без присмотра. Не передавайте usb-токен, пароли лицам, не допущенным до работы в Системе.
2. Пароль для доступа к Системе должен быть надежным, содержать от 8 символов, специальные символы, цифры, буквы разных регистров. Не используйте в качестве пароля конфиденциальную информацию (имена, фамилии, № телефонов и т.п.). Меняйте пароль не реже одного раза в 90 дней. Храните пароли отдельно от usb-токена.
3. Usb-токен следует подключать к компьютеру только на время работы с Системой, а по окончании работы в обязательном порядке извлекать из компьютера.
4. Для обеспечения максимального уровня безопасности используйте: многофакторную аутентификацию, одноразовые пароли и коды.
5. Обращать внимание на дату и время последних входов в систему (данные фиксируются на первой странице после входа в Систему).
6. Регулярно контролировать состояние счёта (путем просмотра выписки).
7. В случае утраты usb-токена, электронного устройства – незамедлительно сообщите в Банк для своевременной блокировки доступов.
8. Если у Вас неожиданно сломался компьютер, он работает странно или нет доступа в Систему, а также если у Вас есть подозрения на компрометацию ключей, незамедлительно обратитесь в Банк для блокировки счета в Системе.
9. К событиям компрометации относятся следующие: потеря ключевых носителей; потеря ключевых носителей с их последующим обнаружением; увольнение сотрудника, имевшего доступ к ключевым носителям; нарушение правил хранения ключевых носителей, получение доступа к ключевой информации посторонним лицам; временный доступ неуполномоченного лица к ключевой информации; случаи, когда нельзя достоверно установить, что произошло с ключевым носителем.

При возникновении следующих ситуаций, просим незамедлительно обращаться в Банк, с целью оперативного блокирования доступа:

1. На компьютере или электронном устройстве, используемом для работы в Системе, обнаружено вредоносное ПО (вирусы, «трояны» и т.д.).
2. В «Журнале сеансов работы» обнаружены факты проникновения в систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время).
3. В выписке обнаружены несанкционированные Вами расходные операции, либо Вы получили SMS уведомление об операции, которую не совершали.
4. Вы получили SMS или e-mail-уведомление об изменении адреса e-mail или номера мобильного телефона для отправки уведомлений, при этом изменения были совершены без Вашего ведома.

Перед началом использования Системы «iBank2» внимательно изучите информацию по обеспечению безопасности, размещенную на сайте http://rostfinance.ru.