г. Москва, ул. Щипок, д.4,стр.1
тел.:+7(495)223-00-63
www.newbank.ru

Утверждена Приказом Председателя Правления КБ «Новый век» (ООО) № 0807/01 от 08.07.2019

ПАМЯТКА

ДБО «iBank» для корпоративных клиентов

Коммерческого Банка «Новый век» (Общество с ограниченной ответственностью) 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.

2. Будьте внимательны: в случае возникновения подозрений на мошенничество максимально быстро сообщите о происшествии в Банк с целью оперативного блокирования доступа!

3. При работе с электронной почтой не открыватйте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

4. Своевременно обновляйте операционную систему (установка патчей, критичных обновлений).

5. 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.

6. Не используйте права администратора при отсутствии необходимости. В повседневной практике входите в систему как пользователь, не имеющий прав администратора. Полностью блокируйте сетевой доступ к компьютеру (удаленный доступ, удаленный помощник и т.д.).

7. Установите и своевременно обновляйте на компьютере антивирусное ПО (Avast, Eset, Kaspersky Lab, Symantec AntiVirus и т.д.). Антивирусное ПО должно быть запущено постоянно с момента загрузки компьютера. Рекомендуется полная еженедельная проверка компьютера на наличие вирусов, удаление обнаруженного вредоносного ПО.

8. Не давайте разрешения неизвестным программам выходить в Интернет. Исключите посещение с Вашего компьютера сайтов сомнительного содержания и любых других Интернетресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников.

9. Категорически не рекомендуется работать с Системой ИБК из мест, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатные беспроводные сети Wi-Fi и т.п.), так как это существенно увеличивает риск кражи Ваших персональных данных.

10. При работе в Интернет не соглашайтесь на установку каких-либо дополнительных программ от недоверенных издателей.

11. При вводе личной информации, ПОМНИТЕ, что веб-адрес (URL) системы ДБО Ibank 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.

12. Безопасность работы в Системе «iBank2» должна быть 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 не менее 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. Если Вы используете несколько ключей при работе в Системе ИБК (например, первая и вторая подписи или ключи с правом подписи и без права подписи (просмотр и создание платежного документа)) – не сохраняйте/не переносите эти ключи на один съемный ключевой носитель, а также не подключайте одновременно различные ключевые носители к одному компьютеру

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 контролируйте 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.

В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к ДБО Ibank отложите совершение операций и обратитесь в службу поддержки Банка по телефонам 8 (495) 223-00-70 либо отправьте сообщение на электронный адрес info@newbank.ru.

ВАЖНО! Обращаем Ваше внимание, что одним из распространенных мошеннических методов завладения средствами клиента является изменение вирусной программой в реально подготовленном Вами платежном документе перед его окончательным подписанием электронно-цифровой подписью реквизитов получателя (например, номера счета получателя, его ИНН и БИК банка получателя без изменения наименования получателя). Настоятельно рекомендуем, с учетом вышеизложенных мер технической и антивирусной защиты, перед окончательным подписанием документов электронно-цифровой подписью внимательно проверять все реквизиты получателей, сумму платежа и другие значимые параметры документа