МЕРЫ БЕЗОПАСНОСТИ
при работе в Системе «Интернет Сервис Банк»

КБ «Геобанк» (ООО) информирует о необходимости использования клиентами следующих мер при работе в Системе дистанционного банковского обслуживания «Интернет Сервис Банк» для повышения безопасности:

При организации рабочего места для работы с Системой ИСБ:

• Старайтесь не работать с непроверенных компьютеров (интернет-кафе, киоски и т.д.).

• Не оставляйте компьютер с активной Системой без присмотра. Выходите из Системы, даже если необходимо отойти на непродолжительное время. Ограничьте доступ посторонних лиц к компьютеру, с которого Вы осуществляете работу с Системой.

• Убедитесь, что ваш компьютер/телефон не заражен вирусами. Установите и активизируйте антивирусное ПО. Регулярно обновляйте антивирусные базы. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о вашем пароле и ключе электронной подписи.

• Установите и настройте персональный брандмауэр (firewall) на вашем компьютере, это позволит предотвратить несанкционированный доступ к информации на вашем компьютере.

• Используйте лицензионное программное обеспечение из проверенных и надежных источников. Выполняйте регулярные обновления операционной системы и прикладного программного обеспечения (браузер, программы для работы с документами и т.д.).

Обращаем Ваше внимание! Банк не направляет клиентам SMS-сообщения с информацией о блокировке/разблокировке доступа в Систему ИСБ.

Не следует реагировать на подозрительные SMS-сообщения, которые запрашивают у Вас конфиденциальную информацию.

При формировании пароля для входа в Систему, предлагается соблюдать следующие правила:

• рекомендуемая длина пароля должна быть не менее 8 символов;

• рекомендуется использовать латинские буквы, набранные в разных регистрах (a-z, A-Z, a-Z) и цифры;

• при смене пароля для входа в Систему новое значение должно отличаться от предыдущего не менее чем на 3 символа;

• новое значение пароля для входа в Систему не должно совпадать с предыдущими паролями на протяжении четырех смен;

• пароль не должен основываться на информации, которую другие могут легко угадать или узнать (имена, номера телефонов, даты рождения, идентификаторы пользователей, наименования рабочих станций и т.п.);

• пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.);

• пароль не должен являться словарным словом (например, «password» - это ненадежный пароль);

• пароль не должен являться копией других паролей пользователя, используемых в личных целях (на развлекательных и почтовых сайтах в Интернете);

• пароль не должен содержать последовательность одинаковых символов и групп символов (например, не должны применяться пароли, состоящие из одинаковых цифр или из одинаковых букв);

• периодически производите замену пароля для входа в Систему ИСБ;

• ни при каких условиях не сообщайте информацию о Вашем пароле никому, включая сотрудников Банка, родственников и иных третьих лиц;

• не сохраняйте информацию о Вашем пароле на вход в Систему ИСБ или пароль от ключа усиленной электронной подписи на любых носителях, включая компьютер;

• рекомендуем хранить ключ носитель с ключами усиленной электронной подписи (USB-ключ) в недоступном для посторонних лиц месте (сейфы, закрываемые шкафы);

• не держите носители с ключами усиленной электронной подписи (USB-ключ) постоянно вставленными в компьютер, используйте их только в случае необходимости заверения документов в Системе ИСБ.

При использовании Системы ИСБ

• Проверяйте, что соединение установлено именно с сервером Интернет-Банк КБ «Геобанк» (ООО) по адресу http://www/geobank.ru.

• Обращайте внимание на изменения привычных вам страниц входа в Интернет-банк КБ «Геобанк» (ООО) или подтверждения операции. Любые изменения, особенно касающиеся безопасности, обязательно заранее анонсируются в новостях системы. Если вы сомневаетесь, действительно ли содержимое страницы вы получаете с сервера банка, а не от компьютерного вируса, обязательно позвоните в Контакт-центр Банка или попробуйте открыть ту же страницу системы на другом компьютере, подключенном к другой сети. **БАНК ВСЕГДА ПРЕДУПРЕЖДАЕТ ОБО ВСЕХ ИЗМЕНЕНИЯХ, ПРОИЗВОДИМЫХ В СИСТЕМЕ. НИКОГДА НЕ ПОЛЬЗУЙТЕСЬ ИНТЕРФЕЙСОМ, ИЗМЕНЕНИЕ КОТОРОГО НЕ ПОДТВЕРЖДЕНО БАНКОМ.**

• Заходите в систему не реже одного раза в 5 (пять) календарных дней, в том числе, для ознакомления с информацией, размещаемой Банком и касающейся работы в системе.

• Внимательно контролируйте все операции, совершенные в Системе ИСБ.

• После окончания работы в Системе обязательно закройте окно системы с помощью кнопки «Выход». После выхода из Системы необходимо обязательно извлечь из компьютера носитель, на котором хранится ключ усиленной электронной подписи.

При возникновении кризисных ситуаций

В случае возникновения подозрений на мошеннические действия:

• в системе присутствуют действия, которые Вы не совершали;

• подозрительная активность на компьютере, с которого осуществляется работа с Системой (самопроизвольные движения мышью, открытие/закрытие окон, набор текста и т.п.);

• изменения адреса для соединения с Системой;

• изменения IP адреса, с которого осуществлялось подключение к системе (изменилась сеть);

• невозможности получения доступа к Системе по причине несовпадения пароля на вход в систему;

• Изменение интерфейса Системы;

• или при возникновении опасений, что Ваш пароль или ключ усиленной электронной подписи стал известен посторонним

необходимо выполнить следующие действия:

• выйдите из Системы;

• заблокируйте технические средства (в том числе, выключите компьютер), используемые для работы в Системе;

• обратитесь в Банк для приостановления/ограничения дистанционного обслуживания в Системе и/или приостановления/аннулирования действия Сертификата Ключа проверки электронной подписи. Это можно сделать в офисе Банка, а также по телефону ***+7 (495) 221-33-41***;

• при оформлении письменного заявления обязательно опишите обстоятельства компрометации пароля, ключей усиленной электронной подписи или несанкционированного доступа, либо другую информацию по фактам, вызвавшим Ваши подозрения.

• возобновление доступа в Систему и возобновление действия Сертификата Ключа проверки электронной подписи производится в офисе Банка при личном обращении клиента.

Рекомендуем Вам всегда иметь при себе контактные телефоны Банка на различных носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о пароле доступа.

Для блокировки доступа в Систему ДБО Вы можете обратиться по телефону круглосуточной поддержки +7 (495) 221-33-41

Для получения дополнительной информации по техническим вопросам Вы можете ежедневно по рабочим дням с 9-00 до 18-00 обратиться:
Служба технической поддержки: (495) 221-33-41 доб.47-56, 47-13
По организационным вопросам: (495) 221-33-41 доб.47-22