Приложение №5.2.
к Условиям дистанционного банковского обслуживания по банковским счетам юридических лиц, индивидуальных предпринимателей, лиц, занимающихся частной практикой в ООО «Земский банк»

**Требования и обязательства Клиента по выполнению правил безопасной работы при дистанционном банковском обслуживании, направленные на снижение рисков осуществления переводов денежных средств без согласия Клиента**

**Настоящим подтверждаю, что ознакомлен до заключения Договора с требованиями и обязательствами по соблюдению безопасности при работе в Системе, мне известны последствия несоблюдения вышеуказанных мер безопасности, и я полностью беру на себя ответственность за такие последствия в случае нарушения мною требований и обязательств по соблюдению безопасности при работе в Системе включая, но не ограничиваясь следующими:**

**1. Выполнение правил выбора пароля доступа к Системе**

-Пароль выбирается самостоятельно;

-Если пароль записан на бумаге, то хранится в месте, недоступном для посторонних лиц;

-Пароль подлежит обязательной смене, если он стал известен постороннему лицу;

-В качестве пароля не используются простые, легко угадываемые комбинации букв и цифр, а также пароли, используемые для доступа в других системах. 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). Пароль не должен являться персональной информацией (имена и даты рождения членов семьи, адреса, телефоны и т.п.) или распространенным (словарным) словом (например, password, default, admin, guest – это ненадежный пароль). Пароль должен соответствовать следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

-При возникновении подозрений в осуществлении несанкционированных операций в Системе либо при компрометации пароля на вход в Систему или Средства подтверждения/Ключа ЭП необходимо последовательно выполнить следующие действия:

- Выйти из Системы с помощью кнопки «Выход;
- Заблокировать устройства, используемые для работы в Системе (в том числе выключить/перевести в режим гибернации (сна) компьютер);
- Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе, аннулирования действия Сертификата/Ключа ЭП. Это можно сделать в офисе Банка, а также по звонку в Банк 8 (8464) 986767, 987825 с последующим оформлением в Банке соответствующих письменных заявлений.
- В письменном заявлении описать обстоятельства компрометации пароля, ключей электронной подписи или несанкционированного доступа либо другую информацию по фактам, вызвавшим Ваши подозрения

**2. Исключение доступа посторонних лиц к носителям ключевой информации (дискета, CD, flash-карта, OTP-устройство, USB-токен, смарт-карта, жесткий диск)**

-Носители ключевой информации и пароли доступа к ним необходимо хранить в недоступном для окружающих месте отдельно друг от друга;

-По завершении работы в Системе или перерыва в работе носитель ключевой информации извлекается из устройства;

-Хранение носителя ключевой информации осуществляется в условиях, исключающих возможность несанкционированного использования третьими лицами;

-Носитель ключевой информации используется только для подписания ЭД или многофакторной аутентификации;

-Ключ ЭП запрещается копировать или передавать третьему лицу;

- Запрещено осуществлять хранение Ключа ЭП на жестком диске компьютера, в памяти иного устройства, с использованием которого осуществляется выход в Интернет, а также иным способом, делающим данную информацию доступной для третьих лиц;

-В случае смены ответственного лица, осуществляющего подпись ЭД, утере носителя ключевой информации, а также о любом подозрении на компрометацию ключа ЭП незамедлительно сообщается в Банк для блокировки ключа ЭП.

**3. Требования к рабочим местам, с которых осуществляется работа с ПО Системы** (далее «Рабочие места Системы»):

- Для работы в Системе использовать выделенный персональный компьютер;

- Исключить работу в Системе на персональном компьютере со свободным доступом (Интернет-кафе, бесплатный Wi-Fi и пр.);

- Запрещено использовать системы удалённого управления персональным компьютером, а также привлекать для администрирования и обслуживания данного персонального компьютера ИТ-персонал на условиях предоставления ему удаленного доступа;

- Право доступа необходимо предоставлять лицам, непосредственно осуществляющим работу в Системе;

- Рабочие места Системы запрещается оставлять без контроля (при кратковременном отсутствии средствами операционной системы блокировать Рабочее место Системы).

**4. Настройка "доверенной среды" и исключение несанкционированного изменения программного обеспечения на Рабочих местах Системы:**

-Используется только лицензионное программное обеспечение;

-Устанавливаются все обновления системы безопасности, рекомендуемые производителем операционной системы, установленной на компьютере;

-Отключается учетная запись для гостевого входа (Guest);

- Использовать для доступа в Систему отдельную учетную запись пользователя компьютера. Доступ к этой учетной записи должен быть защищен паролем, неизвестным любым третьим лицам, включая сотрудников Банка и родственников, удовлетворяющий требованиям п.1 настоящих обязательств;

-Для защиты от несанкционированного доступа из внешней или локальной сети используется и своевременно обновляется специализированное ПО для защиты информации – антивирусное ПО с регулярно обновляемыми базами, персональные межсетевые экраны, средства защиты от несанкционированного доступа и другие технические средства защиты;

-При подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы, работа в Системе немедленно прекращается, а об инциденте сообщается в Банк.

- Не оставлять устройство с активной Системой без присмотра.

- Обязательно осуществлять выход из Системы при необходимости на любое, даже непродолжительное время оставить вне контроля (поля зрения) устройство, на котором осуществляется работа в Системе, и/или устройство.

- После окончания работы в Системе необходимо в обязательном порядке закрыть окно Системы с помощью кнопки «Выход», а также извлечь из компьютера носитель, на котором хранится Сертификат/Ключ ЭП, если операции осуществлялись с его использованием.

-На устройстве, используемом для доступа к Системе, не должно быть установлено программное обеспечение удаленного управления, в том числе TeamVeiwer, RAdmin, VNC и иное подобное программное обеспечение.

**5. Соблюдение правил безопасной работы в сети Интернет на Рабочих местах Системы:**

- Не допускается открывать сайт Системы по ссылкам (особенно баннерным или полученным через электронную почту);

- Не допускается отвечать на подозрительные письма с просьбой выслать Закрытый ключ ЭП, пароль и другие конфиденциальные данные Системы;

- Не допускается сохранять на персональный компьютер подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные на форумах;

- Не допускается устанавливать на персональный компьютер и запускаются программы, полученные от недостоверных источников;

- Исключить посещение сайтов сомнительного содержания и любых других Интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сети и т.п.).

- При каждом сеансе работы с Системой через браузер, проверить подлинность соединения, для чего убедиться, что: включен защищенный режим SSL, то есть в адресной строке браузера web-адрес начинается с символов «https://», на зеленом фоне и в окне web-браузера отражается символ «закрытый замок».

- Соединение установлено именно с сервером ООО «Земский банк», то есть в адресной строке интернет-страницы указан точный адрес: https://ib1.zemsky.ru/RSPortal/StartHTML/example.htm (не допускается никаких отличий в написании web-адреса, вплоть до любого знака);

- В сертификате сайта в строке «Кем выдан» указано точное значение «zemsky.ru».

- До начала проведения операций в Системе проверить историю входов в Систему на предмет соответствия действительным входам в Систему пользователем, отсутствия в ней сведений о входах с IP-адресов, неизвестных пользователю, а также на предмет отсутствия какой-либо истории, которая может свидетельствовать о нахождении на сайте злоумышленника, а не Банка.

- Необходимо обращать пристальное внимание на неанонсированные Банком изменения страниц входа в Систему и работы с ней (интерфейс Системы), особенно касающиеся безопасности. При возникновении подозрений в подмене злоумышленником страниц Интернет-банка запрещено звонить по номеру телефона, указанному на подозрительной странице, а необходимо незамедлительно связаться с Банком по телефонам 8 (8464) 986767, 987825.

**6. Действия в случае возникновения подозрений в осуществлении несанкционированных операций:**

При возникновении подозрений в осуществлении несанкционированных операций в Системе либо при компрометации пароля на вход в Систему или Средства подтверждения/Ключа ЭП необходимо последовательно выполнить следующие действия:

- Выйти из Системы с помощью кнопки «Выход;

- Заблокировать устройства, используемые для работы в Системе (в том числе выключить/перевести в режим гибернации (сна) компьютер);

- Незамедлительно обратиться в Банк для смены пароля, приостановления дистанционного обслуживания в Системе, аннулирования действия Сертификата/Ключа ЭП. Это можно сделать в офисе Банка, а также по звонку в Банк 8 (8464) 986767, 987825 с последующим оформлением в Банке соответствующих письменных заявлений.

- В письменном заявлении описать обстоятельства компрометации пароля, ключей электронной подписи или несанкционированного доступа либо другую информацию по фактам, вызвавшим Ваши подозрения;

- Возобновление доступа в систему и возобновление действия Сертификата/Ключа ЭП производится в офисе Банка при личном обращении клиента.

О проявлении злоумышленных действий в Системе, требующих незамедлительного обращения в Банк, могут свидетельствовать следующие факты:

- В истории поручений в Системе указаны поручения, которые Вы не совершали;

-Подозрительная активность на компьютере, с которого осуществляется работа с Системой (самопроизвольные движения курсором мыши, открытие/закрытие окон, набор текста и т.п.);

- Входящий звонок от лиц, представляющихся работниками ООО «Земский банк», уведомляющих Вас о регламентных/восстановительных работах в Системе или Банке;

- Получение сообщения о блокировке/разблокировке доступа в Систему;

- Изменение адреса в адресной строке браузера при работе с Системой;

- Наличие в истории входов в Систему информации о входе в Систему с незнакомого IP-адреса;

- Невозможность получения доступа к Системе по причине несовпадения пароля при введении заведомо верного пароля;

- Изменение интерфейса или настроек безопасности Системы без предварительного уведомления на сайте Банка.