

(заполняется в обязательном порядке при подписании Заявления о присоединении к Правилам)

Обязательства Клиента по выполнению правил безопасной работы при использовании Клиентской части Системы «Клиент-Банк»

В соответствии с Договором № _____ от «__» _____ 20__ г., подтверждаю, что для обеспечения безопасной работы в Клиентской части Системы «Клиент-Банк»

_____ (наименование КЛИЕНТА)

будут соблюдаться следующие организационные меры:

- Требования к сохранности пароля:
 - пароль выбирается самостоятельно;
 - если пароль записан на бумаге, то хранится в месте, недоступном для неуполномоченных лиц, рекомендуется использовать надежные металлические хранилища, оборудованные внутренними замками;
 - запрещено записывать пароль на съемный носитель, монитор, клавиатуру и пр.;
 - пароль должен содержать не менее 8 различных символов (буквы, цифры, большой / малый регистр);
 - в качестве пароля не должны быть использованы: ИНН и другие реквизиты Клиента, имена и фамилии, последовательности, состоящие из повторяющихся или одних цифр (в том числе номера телефонов, памятные даты, номера автомобилей и прочее, что можно связать с Клиентом);
 - пароль обязательно меняется, если он стал известен постороннему лицу;
 - рекомендуемая периодичность смены пароля – не реже 1 (одного) раза в 3 (три) месяца.

- Правила хранения и использования носителей ключевой информации:
 - для хранения носителей ключевой информации необходимо использовать надежные металлические хранилища, оборудованные внутренними замками, для исключения возможности негласного доступа к ним неуполномоченных лиц;
 - запрещается извлекать из хранилища носители с Ключами ЭП, если они не используются для работы с Системой «Клиент-Банк»;
 - никогда не передавать Ключи ЭП третьим лицам для проверки работы Системы «Клиент-Банк», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец Ключа ЭП должен лично подключить носитель к рабочей станции, убедиться, что пароль доступа к ключу вводится в интерфейс Системы «Клиент-Банк», и лично ввести пароль, исключая возможность его компрометации;
 - запрещается передавать носители ключевой информации третьим лицам, оставлять носители ключевой информации без присмотра, а также (предпринимать попытки по проведению записи) записывать на носитель ключевой информации постороннюю информацию;
 - при возникновении любых подозрений на Компрометацию секретных Ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – заблокировать Ключи ЭП.

- Правила хранения и использования Генератора одноразовых кодов:
 - для хранения Генератора одноразовых кодов необходимо использовать надежные металлические хранилища, оборудованные внутренними замками, для исключения возможности несанкционированного доступа к нему неуполномоченных лиц и повреждение материального носителя;
 - не извлекать из хранилища Генератор одноразовых кодов, если он не используется для работы с Системой «Клиент-Банк»;

- не раскрывать третьим лицам информацию о Генераторе одноразовых кодов, находящемся в его распоряжении;
 - не передавать его в пользование лицам, не являющимся Владельцами **ключей проверки ЭП**, для распоряжения денежными средствами, находящихся на Счете, или в иных целях, оставлять носители ключевой информации без присмотра;
 - в случае утраты или поломки Генератора одноразовых кодов необходимо уведомить об этом Банк посредством личного обращения в Банк или путем обращения по телефону службы технической поддержки Системы «Клиент-Банк» в соответствии с пп. 4.10.29 Договора присоединения.
- Ограничение доступа и требования к рабочим местам, с которых осуществляется работа с Системой «Клиент-Банк»:
- право доступа предоставляется только уполномоченным лицам, непосредственно осуществляющим работу с Системой «Клиент-Банк». Исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой «Клиент-Банк»;
 - запрещается установка программных средств, не предназначенных для выполнения служебных обязанностей уполномоченных лиц Клиента, допущенных к работе с Системой «Клиент-Банк»;
 - применять на рабочем месте лицензионные ПО (операционные системы, офисные пакеты и пр.), лицензионные средства антивирусной защиты, обеспечить возможность регулярного автоматического обновления антивирусных баз;
 - работа с Системой «Клиент-Банк» немедленно прекращается при подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы – обязательно позвонить в Банк и заблокировать Ключ ЭП в порядке, предусмотренном в п. 4.4 Договора присоединения.
- Соблюдение правил безопасной работы в сети интернет на рабочих местах Системы «Клиент-Банк»:
- не открывать сайт Системы «Клиент-Банк» по ссылкам (особенно баннерным или полученным через электронную почту);
 - не отвечать на подозрительные письма с просьбой выслать авторизационные и другие конфиденциальные данные;
 - на компьютерах, используемых для работы с Системой «Клиент-Банк», исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелегального ПО и т. п.;
 - не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;
 - на компьютере запрещено запускать программы, полученные не из доверенных источников;
 - если Клиент эксплуатирует выделенный высокоскоростной канал доступа в сеть интернет, ограничить диапазон IP-адресов, с которых разрешён доступ к Системе «Клиент-Банк» с использованием Ключей ЭП, зарегистрированных Банком по письму, переданному Клиентом на бумажном носителе в Банк.
- Требования к сотрудникам Клиента:
- Клиент обязан назначить Приказом уполномоченных лиц по работе с Системой «Клиент-Банк», утвердить соответствующие должностные инструкции, исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой «Клиент-Банк»;
 - при регистрации в Системе «Клиент-Банк» в соответствии с пп. 4.7.2 настоящих Правил, руководствоваться Инструкцией по установке Системы «Клиент-Банк» (Приложения №№ 5 - 5а к Договору);

- каждое уполномоченное лицо, имеющее доступ к носителям ключевой информации, паролям и другой конфиденциальной информации, должно быть проинформировано об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства;
- при обслуживании компьютера Уполномоченного лица Клиента, на котором используется Система «Клиент-Банк», третьими лицами – обеспечивать контроль над выполняемыми ими действиями;
- при увольнении уполномоченного лица, имевшего доступ к Ключу ЭП, обязательно проинформировать об этом Банк и заблокировать Ключ ЭП;
- при увольнении Уполномоченного лица Клиента, имевшего технический доступ к секретному Ключу ЭП, обязательно проинформировать об этом Банк и заблокировать Ключ ЭП;
- при увольнении Уполномоченного лица Клиента, осуществлявшего обслуживание рабочей станции, используемой для работы с Системой «Клиент-Банк», принять меры для обеспечения отсутствия вредоносных программ на компьютерах;
- по требованию сотрудника технической поддержки Системы «Клиент-Банк» в случае подозрения на Компрометацию Ключа ЭП выполнить антивирусную проверку АРМ Клиента;
- при наличии Счета в Банке:
 - контролировать актуальность номеров телефонов для направления Одноразовых кодов подтверждения, а в случае их изменения – незамедлительно информировать о таком изменении Банк по форме Заявления о присоединении (Приложение № 1 к настоящим Правилам).
 - в случае утраты телефона, на который приходят SMS-сообщения с Одноразовыми кодами подтверждения, обеспечить немедленную блокировку номера телефона у оператора сотовой связи.
 - при поступлении на телефон Уполномоченного лица SMS-сообщений, свидетельствующих о попытке входа в Систему «Клиент-Банк» или подтверждения отправки документов, которых данное лицо не совершало, немедленно обратиться в Банк и инициировать блокировку доступа к Системе «Клиент-Банк» в порядке, установленном Договором.

Требования, установленные настоящим Приложением, в случае использования Клиентом модуля «Интеграционный Клиент-Банк» распространяются на стороне Клиента на все АРМ Клиента, которые участвуют в обмене ЭД с Банком с использованием модуля «Интеграционный Клиент-Банк».

При невыполнении или неполном выполнении требований настоящего Приложения к Правилам по обеспечению информационной безопасности АРМ принимаю на себя риски возможных потерь (ущерба)

