Приложение 1
К Правилам
выпуска и обслуживания виртуальных карт

Требования Банка по информационной безопасности при использовании виртуальной карты

Несоблюдении Клиентом требований Банка по информационной безопасности при использовании виртуальной карты является нарушением Клиентом настоящих Правил. В этом случае Клиент принимает на себя все риски осуществления несанкционированного доступа к банковским счетам Клиента при использовании Карты, а Банк освобождается от какой-либо ответственности и не обязан возмещать Клиенту убытки, включая, но не ограничиваясь, возвратом суммы операции, совершенной без согласия Клиента.

Для обеспечения безопасности при выпуске и обслуживании Карты в системе «Интернет-банк» применяются:

- шифрование канала связи с использованием протокола SSL и сертификата, подписанного доверенным удостоверяющим центром;
- идентификация и аутентификация Клиента;
- сеансовые ключи для подтверждения операций с использованием Системы;
- рассылка уведомлений о совершенных операциях в Системе и с использованием Карты на Абонентский номер Клиента
- изменение статуса ЭД в Системе по мере осуществления операций;
- предоставление выписки по счетам с использованием Системы по мере осуществления операций.

1. Требования при организации рабочего места при осуществлении расчетов по Карте

1.1. На компьютере или мобильном устройстве (мобильный телефон, планшетный компьютер и т.п.), используемом Клиентом для расчетов по Карте должно быть установлено только лицензионное программное обеспечение, включая операционную систему и средства защиты. Клиент обязан использовать операционные системы и программное обеспечение, на которые разработчик регулярно выпускает обновления, в том числе связанные с повышением уровня безопасности.

1.2. Компьютер (мобильное устройство), используемый Клиентом для расчетов по Карте, не должен быть заражен вирусами. Клиент обязан установить и активировать антивирусное программное обеспечение. Антивирусные средства защиты должны соответствовать классу “Internet Security”. Клиент обязан регулярно (автоматически) обновлять антивирусные базы и проверять компьютер или мобильное устройство на вирусы. Обращаем внимание, что действие вирусов может быть направлено на запоминание и передачу третьим лицам информации о Реквизитах Карты.

1.3. Клиент обязан установить автоматическое обновление операционной системы, средств защиты и интернет-браузера, которое будет устанавливать последние исправления, тем самым ликвидируя уязвимости обновляемых систем.

1.4. Клиент обязан установить на компьютер или мобильное устройство и настроить межсетевой экран (брандмауэр, файервóл) с «Белым списком», в котором будут указаны только необходимые адреса (сервер Системы, сервера обновлений операционной системы, средств защиты, интернет-браузера и других необходимых приложений). Это позволит предотвратить несанкционированный доступ к информации на компьютере (мобильном устройстве).

1.5. Клиент обязан устанавливать программное обеспечение только с доверенных источников (рекомендуемых производителем или поставщиком программного обеспечения) и использовать широко известные браузеры.

1.6. Работа на компьютере или мобильном устройстве должна производиться под ограниченными в правах учетными записями (без прав администратора).

1.7. Функция «Автоматическое выполнение» для подсоединяемых к компьютеру или мобильному устройству внешних носителей (компакт-дисков, флэш-карт и т.д.) должна быть отключена.

1.8. Чужие компьютеры или «недоверенные» компьютеры (интернет-кафе, киоски и т.д.) не должны использоваться для расчетов по Карте. При использовании недоверенных компьютеров (мобильных устройств) значительно возрастает риск кражи Реквизитов Карты.

1.9. Компьютер или мобильное устройство для расчетов по Карте не должно использоваться для посещения сайтов, отличных от сайта Системы.

1.10. Доступ посторонних лиц к компьютеру и мобильному устройству, с которого осуществляются расчеты с использованием Реквизитов Карты, должен быть ограничен.

2. Требования к действиям клиентов при осуществлении расчетов по Карте

2.1. Клиент обязан использовать отдельную виртуальную карту для заказа товаров и услуг через сеть Интернет. Устанавливать максимальный Платежный лимит по Карте в таком размере денежных средств, которое необходимо для заказа товаров и услуг через сеть Интернет.

2.2. Для осуществления покупок Клиент обязан пользоваться интернет-сайтами только известных и проверенных организаций торговли и услуг, которые применяют специальные программные средства для защиты информации о банковской карте. Безопасные интернет-сайты используют шифрование канала связи с использованием протокола SSL и сертификата. До совершения операции Клиент обязан убедиться, что:

- в адресной строке используемого браузера действительно указан адрес требуемого интернет-сайта;
- соединение действительно происходит в защищенном режиме SSL, при этом интернет-браузер должен показывать значок закрытого замка, в адресной строке браузера присутствует наименование протокола соединения «https».
- сертификат сайта выдан удостоверяющим центром и соответствует сайту. Для этого, откройте информацию о сертификате;
- за клиентом не ведется наблюдение, в том числе с использованием технических средств.

2.3. Клиент обязан убедиться в правильности адресов интернет-сайтов, к которым подключается и на которых собирается совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий. Необходимо вручную, с помощью клавиатуры компьютера (мобильного устройства), вводить в адресной строке браузера адрес интернет-сайтов, на которых планируется совершить покупку или заказ товаров и услуг.

2.4. Запрещается сообщать информацию о Реквизитах Карты любым лицам, включая сотрудников Банка, родственников и иных третьих лиц. Запрещается сообщать Реквизиты Карты по телефону в публичных местах и в присутствии посторонних лиц, которые могут услышать эту информацию и в дальнейшем использовать ее в своих целях. Запрещается оставлять документы, содержащие Реквизиты Карты, без присмотра в публичных местах: в том числе в офисе, гостинице, аэропорту – везде, где они могут стать доступными посторонним лицам. Запрещается записывать Реквизиты Карты таким образом, чтобы можно было определить, к чему эти Реквизиты Карты относятся, не сохраняйте их в электронном виде, в том числе в

специальных программах для хранения паролей

2.5. Запрещается сохранять Реквизиты Карты на любых носителях, включая компьютер (мобильное устройство). Запрещается сохранять ключевую информацию на жестких/сетевых дисках компьютера, в реестре операционной системы.

2.6. С целью контроля проведенных по Карте операций Клиент обязан сообщить Абонентский номер для информирования о совершении операций по Карте с использованием СМС-сообщений.

2.7. Клиент обязан не реже одного раза в 14 (Четырнадцать) календарных дней осуществлять доступ в Систему, в том числе для ознакомления с информацией, публикуемой Банком в соответствии с п. 2.4. настоящих Правил. Клиент обязан внимательно контролировать все операции, совершенные с использованием Карты.

2.8. Клиент обязан блокировать компьютер или мобильное устройство при отсутствии за ним визуального контроля со стороны Клиента.

2.9. При любом неадекватном (отличающемся от обычного) поведении компьютера (мобильного устройства), используемом для расчетов по Карте:

подозрительная активность на компьютере или подозрительная работа мобильного устройства, с которого осуществляются расчеты по Карте (самопроизвольные движения мышью, открытие/закрытие окон, набор текста и т.п.), а также при возникновении опасений, что Реквизиты Карты стали известны посторонним лицам, или Клиент получил СМС-сообщение или выписку Банка об операциях, которые не совершал, необходимо выполнить следующие действия:

- *закрыть интернет-сайт, на котором осуществлялись расчеты по Карте;*
- *заблокировать технические средства (в том числе, выключить компьютер или мобильное устройство), используемые для расчетов по Карте;*
- *немедленно обратиться в Единую справочную службу Банка для приостановления расчетов по Карте по реквизитам, указанным на официальном сайте Банка.*