PARITETBANK

Рекомендации по безопасному использованию банковских платежных карточек

1. Общие рекомендации

1.1. При получении карточки распишитесь на ее оборотной стороне в специальном поле. Наличие вашей подписи на карточке снизит риск использования ее другими лицами в случае утери или кражи карточки. При отсутствии подписи на карточке либо несоответствии подписей на карточке и карт-чеке держателю карточки может быть отказано в проведении операции с ее использованием. Сохраните номер карточки и номер телефона службы клиентской поддержки банка, выдавшего карточку. Эта информация может понадобиться вам для блокировки карточки в случае ее утери либо кражи. Храните номер телефона службы клиентской поддержки банка, выдавшего карточку в легкодоступном месте (например, в памяти мобильного телефона или записной книжке).

1.2. Обеспечивайте условия хранения карточки, которые исключают всякую возможность ее утери, порчи, копирования данных, несанкционированного и незаконного использования. Не допускайте механических повреждений карточки, ее деформации, загрязнения, воздействия высоких и низких температур, электромагнитных полей, прямых солнечных лучей, влаги, красителей, растворителей, вредных химических веществ и других неблагоприятных факторов, которые могут привести к утрате карточкой работоспособности.

1.3. Используйте разные карточки для осуществления ежедневных платежей, платежей в сети Интернет, а также в зарубежных поездках: для каждого типа платежей стоит оформить отдельный счет и выпустить к нему карточку.

Для осуществления платежей за рубежом желательно оформить к одному счету несколько карточек различных платежных систем и хранить их отдельно друг от друга, это сможет уберечь вас от неприятных ”сюрпризов“ в местах, где принимаются карточки не всех платежных систем. Помните, что не стоит хранить большие суммы денег на карточках, которыми вы пользуетесь нерегулярно: например, карточку для оплаты в сети Интернет стоит пополнять именно на ту сумму, которую планируете потратить, и непосредственно перед совершением платежа.

1.4. Право пользования карточкой имеет только держатель. Карточку нельзя передавать другим лицам. При необходимости предоставления доступа к счету иным лицам нужно обратиться в банк, выдавший карточку, для оформления дополнительной карточки.

1.5. Храните втайне от других лиц конфиденциальные данные карточки: номер и срок действия карточки, указанный на оборотной стороне трехзначный код проверки подлинности карточки (при его наличии), ПИН-код, который желательно запомнить. В случае если это является

затруднительным, ПИН-код необходимо хранить отдельно от карточки в неявном виде (например, переписав его на листок бумаги среди прочих групп цифр или любой другой информации) или изменить его на более удобный (при наличии такой услуги у банка, выдавшего карточку). Никогда не сообщайте ПИН-код другим лицам, включая родственников, знакомых, работников банков, организаций торговли (сервиса), представителей правоохранительных органов. Не передавайте ПИН-код ни по телефону, ни по электронной почте. Только держатель карточки должен знать свой ПИН-код.

1.6. Целесообразно пользоваться услугой SMS-информирования (оповещения) или аналогичной (например, оповещения с применением push-технологии или e-mail-оповещения). Данная услуга посредством SMS-сообщений обеспечивает оперативное уведомление о совершенных по карточке операциях, изменении остатка по счету. Использование услуги SMS-информирования позволит не только незамедлительно узнать о несанкционированной вами операции, но и предпринять необходимые меры для своевременной блокировки карточки.

В случае если при наличии у вас подключенной услуги SMS-информирования сообщения от банка о проводимых вами операциях перестали поступать на ваш мобильный телефон, необходимо связаться с банком для уточнения причин.

При получении информационного сообщения о подозрительной операции, которую вы не совершали, а также, если полученное от банка сообщение вызывает какие-либо сомнения или опасения, необходимо заблокировать карточку любым из доступных вам способов, обратиться в службу клиентской поддержки банка, выдавшего карточку, по телефонам, указанным на обратной стороне карточки или полученным непосредственно в банке, и следовать указаниям специалиста.

1.7. Для взаимодействия с банком, выдавшим карточку, используйте только реквизиты средств связи (мобильных и стационарных телефонов, факсов, интернет-сайтов, обычной и электронной почты), которые получены из надежных проверенных источников (например, на странице интернет-банкинга) или непосредственно в этом банке.

1.8. При обнаружении утери (кражи) карточки, оставлении ее в банкомате или ином устройстве самообслуживания, изъятии кассиром организации торговли (сервиса), ее компрометации (если конфиденциальные данные карточки стали известны посторонним лицам) либо при возникновении подозрений в ее компрометации необходимо немедленно заблокировать карточку (например, позвонив в службу клиентской поддержки или посредством систем дистанционного банковского обслуживания) и обратиться в банк, выдавший карточку.

1.9. При получении сообщения с просьбой позвонить в банк по указанным в сообщении телефонам рекомендуется связаться со службой поддержки клиентов банка по достоверно известному вам номеру телефона и

сообщить о факте получения такого сообщения. Также будьте внимательными, отвечая на телефонные звонки и сообщения, поступающие якобы от банка: если работника банка интересует ваш ПИН-код, **полный** номер карточки, срок ее действия или что-то, что вызывает у вас подозрения, необходимо прервать звонок и самостоятельно связаться со службой поддержки банка по достоверно известному вам номеру телефона.

1.10. При наличии у банка, выдавшего карточку, возможности установить ограничения (лимиты) на снятие наличных денежных средств и безналичные операции как на территории Республики Беларусь, так и за ее пределами, желательно, ознакомившись с условиями предоставления услуги и изменения базовых лимитов, установить приемлемые для вас ограничения. При отсутствии необходимости в совершении таких платежей в ближайшее время не рекомендуется подключать возможности оплаты карточкой в сети Интернет, а также за рубежом.

1.11. Старайтесь регулярно проверять состояние своего счета (предпочтительно не реже чем раз в месяц), а также после заграничных поездок, в которых использовалась карточка. При выявлении расхождений между фактически совершенными и отраженными в выписке операциями обратитесь в банк, выдавший карточку, для уточнения обоснованности операций.

1.12. При смене номера вашего контактного телефона, свяжитесь с банком для актуализации ваших данных.

2. Проведение операций с использованием карточки в банкоматах и других устройствах самообслуживания.

2.1. При выборе банкомата или другого устройства самообслуживания, в котором вы собираетесь провести операцию с использованием карточки, желательно избегать плохо освещенных и безлюдных мест. Наиболее безопасными местами для совершения операций являются помещения банковских офисов.

2.2. Для совершения регулярных операций старайтесь пользоваться одним и тем же банкоматом или другим устройством самообслуживания, расположенным в хорошо освещенном месте. В случае если вы заметили, что с банкоматом произошли какие-либо изменения (например, появилась накладка на картоприемнике), позвоните в службу поддержки банка, который обслуживает банкомат, по номеру телефона, указанному на экране банкомата, и сообщите о ваших подозрениях.

2.3. Перед началом совершения операции осмотрите лицевую панель банкомата или другого устройства самообслуживания. Особое внимание обратите на основные элементы банкомата: картоприемник, ПИН-клавиатуру, устройство для выдачи денежных средств. Некоторые банкоматы, устройства самообслуживания банков предлагают сверить изображение устройства, размещенное на мониторе, с тем, которое вы видите

перед собой: если вы заметили разницу, сообщите об этом в банк и воздержитесь от использования такого устройства. Обратите особое внимание на щель картоприемника: мошенники могут установить поверх картоприемника или непосредственно в картоприемник непредусмотренную конструкцией банкомата накладку. Зачастую мошенники оставляют заметные следы: щели, клеевые подтеки и сколы. Лучше не использовать банкомат, картоприемник которого выглядит так, будто кто-то ковырял его отверткой или облил клеем.

Порой мошенники делают поддельные панели с видеокамерами, которые затем крепятся к банкомату: на диспенсер для денег, под козырек, под экран или даже в стенде для рекламных брошюр. Эти камеры издалека могут выглядеть как черные точки.

Если у вас возникли подозрения о наличии подобных устройств, не пользуйтесь данным банкоматом или другим устройством самообслуживания и по возможности сообщите о подозрениях в банк, обслуживающий данное устройство, по телефону, указанному на экране устройства.

Если какие-либо детали банкомата или другого устройства самообслуживания не закреплены, шатаются или выглядят неестественно – это также повод отказаться от использования такого устройства.

2.4. При обнаружении постороннего оборудования (например, накладки) не пытайтесь снять его самостоятельно, воздержитесь от совершения операций, а о выявленном постороннем оборудовании сообщите в банк, обслуживающий устройство. Если сомнения относительно корректной работы банкомата, устройства самообслуживания возникли после того, как карточка помещена в картоприемник, не вводите ПИН-код, нажмите кнопку для отмены операции и заберите карточку. Если вы заметили постороннее оборудование уже после окончания обслуживания, обязательно сразу же заблокируйте карточку любым доступным вам способом.

2.5. Убедитесь, что выбранный вами банкомат или другое устройство самообслуживания принимает имеющуюся у вас карточку. Логотип платежной системы на вашей карточке и на экране программно-технического устройства и (или) на его корпусе должны быть одинаковы. Если вы вставили в банкомат или другое устройство самообслуживания карточку, не обслуживающуюся в данном устройстве, карточка будет вам возвращена, при этом на экране должна появиться информация о невозможности совершения операции с использованием данной карточки.

2.6. Не применяйте чрезмерную физическую силу, чтобы вставить карточку в банкомат или другое устройство самообслуживания.

2.7. Обращайте внимание на людей, стоящих за вами в очереди у банкомата или другого устройства самообслуживания, в случае необходимости попросите их отойти на расстояние, с которого они не смогут увидеть вводимый вами ПИН-код. При вводе ПИН-кода находитесь как

можно ближе к банкомату или устройству самообслуживания, при этом прикрывайте клавиатуру ладонью свободной руки.

2.8. В случае если поблизости от банкомата или другого устройства самообслуживания находятся люди, вызывающие у вас подозрение, следует выбрать другое время для использования данного устройства или воспользоваться другим банкоматом или устройством самообслуживания.

2.9. Будьте особенно осторожны, если незнакомые люди предлагают вам помощь в использовании карточки в банкомате или другом устройстве самообслуживания. В случае затруднений, возникших при использовании карточки, не прислушивайтесь к советам посторонних лиц, а для связи с банком, выдавшим карточку, пользуйтесь только номерами телефонов, которые указаны непосредственно на карточке либо получены вами из надежных проверенных источников или непосредственно в банке.

2.10. При неоднократном (как правило, трехкратном) некорректном вводе ПИН-кода карточка блокируется и может быть изъята банкоматом или другим устройством самообслуживания. В случае изъятия карточки (независимо от причины) банкоматом или другим устройством самообслуживания немедленно заблокируйте ее (например, связавшись со службой поддержки клиентов банка или с использованием систем дистанционного банковского обслуживания).

2.11. При использовании карточки внимательно изучайте информацию, выводимую на экран банкомата или другого устройства самообслуживания, и проверяйте правильность вводимых данных.

2.12. Не позволяйте никому отвлекать вас во время проведения операции, поскольку вы можете случайно совершить некорректную операцию. Кроме того, при отсутствии каких-либо действий с вашей стороны в течение установленного для данного устройства времени оно может изъять вашу карточку и (или) деньги.

2.13. После получения наличных денежных средств в банкомате следует убедиться в том, что карточка была возвращена устройством, дождаться выдачи карт-чека (при его запросе) и только после этого отходить от банкомата. Следует помнить, что последовательность выдачи наличных денежных средств и возврата карточки в банкоматах разных банков может отличаться: банкомат может сначала вернуть карточку, а затем выдать запрошенную сумму денежных средств. Необходимо учитывать данную специфику работы банкоматов и не отходить от устройства до момента получения карточки, карт-чека (при его запросе) и денег.

2.14. В случае если банкомат или другое устройство самообслуживания работает некорректно (например, долгое время находится в режиме ожидания, самопроизвольно перезагружается), следует отказаться от использования такого устройства, отменить совершаемую операцию, нажав на клавиатуре соответствующую кнопку, и дождаться возврата карточки. Если устройство не возвращает карточку, следует незамедлительно

заблокировать карточку любым доступным вам способом и обратиться в банк, выдавший карточку.

2.15. Если при проведении операции в банкомате или другом устройстве самообслуживания что-нибудь вызвало у вас настороженность или подозрения, нажмите кнопку
для отмены операции, заберите карточку и при первой же возможности сообщите в банк, выдавший карточку, о ваших подозрениях.

2.16. Не оставляйте запрошенный вами карт-чек в банкомате или другом устройстве самообслуживания, так как в чеке могут быть указаны сумма операции, остаток денежных средств. Это может привлечь грабителя или мошенника.

3. Получение наличных денежных средств и проведение операций безналичной оплаты с использованием карточки в отделении банка

3.1. Все действия работника банка с вашей карточкой должны проходить под вашим наблюдением. Не разрешайте работнику банка уходить с вашей карточкой в другое помещение.

3.2. При получении наличных денежных средств либо проведении безналичной оплаты особое внимание обращайте на соответствие указанной вами суммы и валюты операции сумме и валюте, содержащейся в карт-чеке.

3.3. Работник банка вправе потребовать у вас предъявления документа, удостоверяющего личность (паспорта), для идентификации держателя карточки и оформления операции.

3.4. При проведении операций в пунктах выдачи наличных обращайте особое внимание на действия работника банка, если он пытается провести вашу карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение несанкционированных вами операций. Обязательно поинтересуйтесь причиной, по которой работнику необходимо повторно провести карточку через считывающее устройство оборудования.

3.5. Перед вводом ПИН-кода убедитесь, что сумма и валюта совершаемой операции верны.

3.6. Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам банка.

3.7. Перед тем как подписать карт-чек (в случае, если это необходимо), убедитесь, что сумма, валюта операции, дата операции, тип операции и другие данные, указанные в карт-чеке, верны.

4. Проведение операций безналичной оплаты с использованием карточки в организациях торговли (сервиса)

4.1. При проведении операций в ресторанах, барах, магазинах, отдавая карточку обслуживающему персоналу, не выпускайте ее из поля зрения. При необходимости проследуйте вместе с работником организации торговли (сервиса) к терминалу. Это позволит предотвратить неправомерное копирование информации с карточки.

4.2. При совершении операции с использованием платежного терминала (POS-терминала) кассир может потребовать у вас ввести ПИН-код или подписать карт-чек в соответствии с требованиями, установленными правилами платежных систем, а также предоставить паспорт в целях установления личности держателя карточки.

4.3. При проведении операции оплаты в организациях торговли (сервиса) обращайте особое внимание на действия кассира, если он пытается провести вашу карточку через считывающее устройство оборудования больше одного раза. Это позволит предотвратить проведение несанкционированных вами операций. Обязательно поинтересуйтесь причиной, по которой кассиру необходимо повторно провести карточку через считывающее устройство оборудования. Если вследствие неуспешного проведения операции по карточке вы оплатили покупку иным способом (например, наличными деньгами или другой карточкой), сохраните документ, подтверждающий, что оплата не была успешно произведена, и проверьте, списались ли со счета денежные средства по операции, завершенной неуспешно.

4.4. Вводите ПИН-код, прикрывая клавиатуру ладонью свободной руки. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости от вас, не смогут его увидеть. Никогда и ни при каких обстоятельствах не сообщайте ПИН-код работникам организаций торговли (сервиса).

4.5. Перед вводом ПИН-кода убедитесь, что сумма и валюта совершаемой операции
верны.

4.6. Перед тем как подписать карт-чек, убедитесь, что сумма, валюта, дата операции, тип операции, название организации торговли (сервиса) и другие данные, указанные в карт-чеке, верны.

4.7. Если вы решили отказаться от покупки после успешного завершения операции, потребуйте отменить операцию. Обязательно сохраняйте карт-чек по операции отмены до момента сверки выписки по счету, к которому выпущена карточка.

4.8. В случае отказа по какой-либо причине от использования услуг гостиницы, пункта проката и т. п. требуйте отмены блокировки залоговой суммы.

4.9. Бесконтактные операции совершаются в режиме ”самообслуживания“ – держатель не передает карточку или другой платежный инструмент, используемый для оплаты (например, браслет, брелок, мобильный телефон или другое устройство), кассиру, а

самостоятельно прикладывает карточку или другой платежный инструмент к считывающему устройству терминала для проведения операции.

4.10. Перед оплатой за товары или услуги в устройствах самообслуживания организаций торговли (сервиса) (например, на автозаправочной станции) изучите имеющуюся информацию о правилах совершения платежей, размещенную на экране устройства или рядом с ним, и следуйте инструкциям системы самообслуживания. При вводе ПИН-кода прикрывайте клавиатуру ладонью свободной руки.

5. Проведение операций безналичной оплаты с использованием карточки в сети Интернет

5.1. Для оплаты товаров в сети Интернет лучше использовать отдельную карточку (к отдельному счету и с ограниченной суммой денежных средств на нем), предназначенную только для данной цели. Совершайте покупки только в тех интернет-магазинах, которые вызывают у вас доверие.

5.2. Не отвечайте на электронные письма, в которых от имени банка или иных организаций, а также граждан вас просят предоставить персональную информацию, в том числе реквизиты вашей карточки, в целях их обновления или для регистрации. Постарайтесь выяснить правомерность таких предложений, связавшись с банком по достоверно известному номеру телефона (например, полученному вами непосредственно от банка, выдавшего карточку).

5.3. Злоумышленники часто распространяют вирусные программы через различные интернет-ресурсы (от социальных сетей до обычных новостных сайтов), посредством электронной почты, программ обмена сообщениями. Клиент, компьютер которого заражен, при попытке войти в личный кабинет может незаметно перенаправляться на ”фишинговый“ сайт, который внешне практически не отличается от подлинных сайтов интернет-банков. Чтобы этого избежать, старайтесь максимально использовать возможности вашего браузера и почтового клиента по обеспечению безопасности. Для этого в опциях браузера и почтового клиента необходимо включить дополнительные функции.

Например, ”Блокировка всплывающих окон“, ”Защита от фишинга и вредоносного ПО“, ”Открывать файлы на основе содержимого, а не расширения“ и др. Также не стоит пользоваться окном предварительного просмотра в используемом вами почтовом клиенте.

Кроме того, рекомендуется всегда самостоятельно вводить веб-адрес банка (интернет-банкинга) в адресную строку браузера вместо использования любых гиперссылок, тем более из подозрительных сообщений.

5.4. Проверяйте правильность адресов интернет-сайтов, к которым подключаетесь для совершения покупки, так как похожие адреса могут

использоваться для осуществления неправомерных действий. Если у вас появились какие-либо подозрения относительно интернет-страницы или вы не хотите предоставлять персональные данные или данные карточки, то покиньте страницу и совершите покупку в другом месте.

5.5. Перед совершением операции оплаты товара (услуги) внимательно изучите условия предлагаемого соглашения, в частности, все правила предоставления услуг, условия доставки, возврата, замены товара, а также процедуру отмены заказа. Особенно внимательно читайте условия совершения операций, связанных с азартными играми (казино, лотереи), так как они могут предусматривать автоматическую подписку, что повлечет списание денежных средств на регулярной основе.

5.6. Сохраняйте любые электронные документы, переписку по электронной почте, касающуюся попыток разрешения спорной ситуации с организацией торговли (сервиса), так как эти сведения могут оказаться важны для защиты ваших прав потребителя. При невозможности самостоятельно разрешить спорную ситуацию обратитесь в банк, выдавший карточку. В случае если условия для вас непонятны, откажитесь от платежа. Помните, что возврат денежных средств по совершенным вами операциям возможен далеко не во всех случаях.

5.7. Если вами было произведено бронирование гостиницы через интернет-сайт, но
по каким-то причинам вы не планируете воспользоваться ею, обязательно проведите отмену бронирования через тот же интернет-сайт согласно указанным на нем процедурам. Получение клиентом кода отмены бронирования отеля является доказательством того, что бронь действительно отменена. В ином случае за несвоевременную отмену брони гостиница имеет право представить к списанию с вашего счета сумму денежных средств в установленном ею размере.

5.8. Никогда не сообщайте свой ПИН-код при заказе товаров по телефону или почте и не вводите его в форму заказа на сайте торговой точки. При совершении удаленных операций ввод ПИН-кода никогда не требуется.

5.9. Совершайте покупки только со своих устройств, не пользуйтесь интернет-кафе и другими общедоступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые вами конфиденциальные данные.

5.10. Если банком, выдавшим карточку, поддерживается технология дополнительного подтверждения операций, совершаемых держателями карточек с использованием их реквизитов в сети Интернет (например, Verified by Visa или MasterCard SecureCode), рекомендуется подключить такую услугу для обеспечения более высокого уровня безопасности интернет-платежей.

5.11. Устанавливайте на свои устройства лицензионное программное обеспечение,

в том числе антивирусное, межсетевые экраны (фаерволы/брандмауэры), и регулярно производите их обновление. Это поможет защитить ваши устройства от вирусов и других деструктивных программ, а также от несанкционированного доступа к вашим конфиденциальным данным. Даже если вы уверены в своем программном обеспечении, не стоит открывать или загружать вложения электронных писем от незнакомых и сомнительных адресатов.

5.12. Не стоит позволять браузерам сохранять данные карточки ”для упрощения совершения покупок в будущем“.

6. Особенности проведения операций с использованием карточки

6.1. Необходимо учитывать, что специфика совершения операций с использованием
карточки предполагает наличие временного разрыва между датой совершения операции и отражением данной операции по счету. Продолжительность периода между днем совершения операции и днем отражения операции по счету зависит от места осуществления операции (на территории Республики Беларусь или за границей), принадлежности технической инфраструктуры (банку, выдавшему карточку, или другому банку), времени осуществления операции (ночное или дневное время, рабочие или выходные, праздничные дни).

6.2. При заключении договора об использовании карточки (кредитного договора) особое внимание следует обратить на положения, касающиеся операций конверсии (покупки-продажи) с использованием карточки и применяемого банком, выдавшим карточку, обменного курса. Если валюта счета не совпадает с валютой операции, курс конверсии (покупки-продажи валюты), используемый для отражения операций по счету, применяется банком, выдавшим карточку, согласно договору об использовании карточки (кредитному договору), заключенному между вами и банком. Например, банк может применить курс конверсии (покупки-продажи) не на дату совершения держателем операции с использованием карточки, а на дату отражения операции по счету.

6.3. Внимательно ознакомьтесь с размером комиссионного вознаграждения, взимаемого банком, выдавшим карточку, за операции, совершаемые с использованием карточки. Размер взимаемого комиссионного вознаграждения при проведении одной и той же операции может быть различным у банка, выдавшего карточку, и у других банков.

6.4. В зависимости от страны пребывания при проведении операции с использованием карточки может удерживаться дополнительная комиссия, о размерах которой целесообразно поинтересоваться у обслуживающего вас работника перед совершением операции. Также такая информация может быть отображена на экране банкомата или устройства самообслуживания при совершении операции.

6.5. При проведении операций без вашего физического присутствия во время и (или) в месте проведения оплаты (например, посредством почты, факса, телефона и т. п.) сообщайте (вносите в соответствующие поля) необходимые реквизиты карточки только для проведения операции, которую вы сами инициировали и считаете правомерной.

6.6. В случае если вы все же пострадали от мошенничества: необходимо немедленно обратиться в службу клиентской поддержки банка, выдавшего карточку, для блокировки карточки и следовать рекомендациям специалиста. По факту мошенничества рекомендуется подать заявление в правоохранительные органы.

6.7. При оплате товаров (услуг) за границей стоит обращать внимание на наличие сервиса Dynamic currency conversion (DCC), что в переводе означает ”динамический обмен валюты“. Этот сервис предлагает дополнительный этап конверсии, что, как правило, приводит к уплате дополнительной комиссии: сумма к оплате пересчитывается в белорусские рубли по курсу, установленному банком, предлагающим услугу DCC. Необходимо внимательно следить за информацией, представленной на экране терминала, а также проверять указанные в карт-чеке условия проведения операции (в частности, стоит обращать внимание на наличие аббревиатуры DCC). В случае несогласия с условиями проведения операции не подтверждайте ее подписью на карт-чеке или вводом ПИН-кода, настаивайте на отмене операции и ее проведении без применения динамической конверсии.

При наличии у банка, выдавшего карточку, такой возможности, вы можете запретить осуществление операций с использованием услуги DCC (например, через интернет-банкинг или обратившись непосредственно в банк).

7. Использование систем дистанционного банковского обслуживания

7.1. При использовании интернет-банкинга обращайте внимание на наличие на странице сервиса защищенного протокола HTTPS. Перед входом в систему рекомендуется удостовериться в подлинности сертификата и сайта. Как правило, для этого необходимо кликнуть в поле адресной строки Интернет (как правило, это поле с пиктограммой замка или листа бумаги) и сверить имеющуюся в блоке информацию. В случае несоответствия присутствующих данных с реальными сведениями о банке стоит немедленно покинуть страницу.

7.2. При наличии на странице интернет-банкинга функции ввода данных с помощью виртуальной клавиатуры, стоит использовать эту возможность для защиты от программ ”клавиатурных шпионов“.

7.3. Не забывайте периодически (а также в случае, если пароль стал известен посторонним лицам) менять свой пароль. Старайтесь сделать его максимально сложным и уникальным. Для этого используйте в пароле

прописные и строчные буквы, цифры и символы. Не используйте один и тот же пароль в разных системах (электронная почта, системы интернет-банкинга других банков, социальные сети и т. п.). Постарайтесь избегать в пароле даты своего рождения, имени и других доступных о вас данных. Ни при каких обстоятельствах не разглашайте свой пароль никому, включая сотрудников банка.

7.4. Будьте осторожны, посещая сайты с сомнительным содержанием: именно они, как правило, являются источником самых новых вирусов, работа которых может быть направлена на хищение ваших данных (в том числе, логинов и паролей).

7.5. Не стоит позволять браузерам запоминать логины и пароли для входа в системы дистанционного банковского обслуживания: это ускорит ваш вход в систему, но существенно снизит ее безопасность.

7.6. По окончании сеанса работы с системой интернет-банкинга обязательно корректно выходите из системы, используя соответствующую опцию.

8. Мобильный банкинг

8.1. Устанавливайте мобильные приложения (в том числе и приложения банков) только из известных источников (Google Play Market, Windows Store, App Store).

8.2. Необходимо использовать мобильные устройства с работающими системами защиты, такими как: ограничение доступа к устройству, активное антивирусное программное обеспечение с обновленными базами данных, система обновления операционной системы.

8.3. Не устанавливайте мобильные приложения банков на мобильный телефон (устройство), на котором получены root-права (права суперпользователя). Такие телефоны и устройства также не рекомендуется использовать для получения сообщений от банка (например, SMS с кодом (одноразовым паролем) для прохождения аутентификации).

8.4. При утрате мобильного телефона (устройства), на котором установлено мобильное приложение банка (приходят SMS-сообщения с подтверждающими одноразовыми паролями) или неожиданным прекращением работы SIM-карты, следует как можно быстрей заблокировать SIM-карту.

8.5. Никогда не оставляйте открытым мобильное приложение: всегда пользуйтесь кнопкой для завершения работы.