ПРАВИЛА
информационной безопасности при работе в Системе интернет-банкинга

Содержание

Страницы

1. Цель

1.1. Настоящий стандарт устанавливает общие правила, а также защитные меры, направленные на предотвращение нарушений информационной безопасности при использовании клиентами Банка Системы интернет-банкинга.

2. Основные термины и определения

2.1. **Злоумышленник** - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

2.2. **Злоумышленные действия** – любые действия, совершаемые Злоумышленником в Системе интернет-банкинга.

2.3. **Угроза** - опасность, предполагающая возможность потерь (ущерба).

2.4. **Риск** - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.

2.5. **Информационная безопасность** - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

2.6. **Защитная мера** - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе интернет-банкинга.

2.7. **Инцидент** - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности

2.8. **Риск нарушения информационной безопасности** - Риск, связанный с Угрозой Информационной безопасности.

2.9. **Обработка риска нарушения информационной безопасности** - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска.

3. Общие положения

3.1. Правила информационной безопасности при работе в Системе интернет-банкинга (далее - Правила) составлены в соответствии с требованиями законодательства Российской Федерации, Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014, иными нормативными правовыми актами Банка России, а также действующей в ЗАО «Экономбанк» (далее – Банк) Политикой информационной безопасности и являются обязательными к исполнению Клиентами, заключившими Договор.

3.2. Настоящие Правила определяют защитные меры по обработке Рисков нарушения информационной безопасности при использовании клиентами Системы интернет-банкинга. При этом клиент обязан учитывать то, что:

3.1.1. информационно-телекоммуникационная сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) информационно-телекоммуникационной сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;

3.1.2. существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством информационно-телекоммуникационной сети Интернет;

3.1.3. существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из информационно-телекоммуникационной сети Интернет;

3.1.4. гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;

3.1.5. меры по нейтрализации злоумышленных действий могут быть эффективными только в течение первых часов после инцидента;

3.1.6. расследованием злоумышленных действий и поиском злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему интернет-банкинга, для проведения экспертизы.

4. Ограничение ответственности Банка

4.1. В связи с тем, что для доступа в Систему интернет-банкинга клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе злоумышленные действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся клиентом.

4.2. За пользование нелицензированным программным обеспечением клиент несет уголовную ответственность в соответствии со статьей 146 Уголовного кодекса Российской Федерации.

4.3. В случае обнаружения несанкционированных действий со средствами, находящимися на счетах клиента, клиент осуществляет действия в соответствии с Памяткой для клиентов о действиях в случае обнаружения несанкционированного списания денежных средств с их счетов (Приложение А к настоящим Правилам).

4.4. Окончательное решение об использовании защитных мер, предлагаемых Банком (см. раздел 5 настоящих Правил) принимает клиент.

4.5. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы интернет-банкинга. Содержимое журнала Системы интернет-банкинга используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования злоумышленных действий.

5. Защитные меры, реализуемые в Банке

5.1. Доступ в Систему интернет-банкинга осуществляется клиентами с использованием уникальных учетных записей, с индивидуальными логинами и паролями многоразового действия.

5.2. Для усовершенствования защитных мер при использовании Системы интернет-банкинга при осуществлении доступа, а также при подтверждении операции клиентами могут использоваться одноразовые коды и (или) электронная подпись.

5.3. Одноразовый код доводится до клиента путем отправки SMS-сообщения на указанный клиентом номер телефона.

5.4. Одноразовый код однозначно соответствует сеансу связи или подтверждаемой операции и не может быть использован повторно.

5.5. Время действия одноразового кода составляет 360 с.

5.6. Сообщение, содержащее одноразовый код подтверждения операции, включает в себя информация об операции. Клиент получает данные о сумме подтверждаемого перевода и получателе денежных средств до ввода одноразового кода.

5.7. В случае если Банку стало известно о признаках, указывающих на изменение получателя SMS-сообщений, отправка сообщений прекращается до установки актуального номера телефона клиента.

5.8. На основании заявления Клиента Банк устанавливает ограничения по параметрам операций, которые может осуществлять Клиент в системе Интернет-банк:

- на максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени;
- на перечень возможных получателей денежных средств;
- на временной период, в который могут быть совершены переводы денежных средств;
- на географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение Клиентом электронных сообщений;
- на перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;
- на перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств.

6. Защитные меры предлагаемые клиентам Банка

6.1. Не сообщайте посторонним лицам, а также кому бы то ни было через сеть Интернет, логины и пароли доступа к ресурсам Банка, историю операций, контактные и учетные данные, так как эти данные могут быть перехвачены злоумышленником и использованы для получения доступа к Вашим счетам.

6.2. Не записывайте логин и пароль на бумаге, мониторе или клавиатуре.

6.3. Не используйте функцию запоминания логина и пароля в браузерах.

6.4. Не используйте одинаковые логин и пароль для доступа к различным системам.

6.5. Всегда явным образом завершайте сеанс работы с Системой интернет-банкинга, используя пункт меню «Выход».

6.6. В случае если доступ к Системе интернет-банкинга осуществляется с использованием постороннего компьютера, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно смените логин и пароль.

6.7. Если Вы получили на электронную почту письмо с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Банк по телефону (8452) 427-000, 8 800-100-1319 и сообщите о письме. Банк никогда не просит передать данные по электронной почте. Обновление данных осуществляется только сотрудником Банка в присутствии Клиента/представителя Клиента, предъявившего документ, удостоверяющего личность. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах и не отвечайте на них.

6.8. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносные компьютерные программы), способные украсть ваши идентификационные данные для входа в Систему интернет-банкинга и ключи ЭП.

6.9. Регулярно, не реже одного раза в месяц, производите смену пароля.

6.10. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] < >. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.

6.11. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

6.12. Не позволяйте третьим лицам производить за Вас генерацию ключей ЭП.

6.13. Присоединяйте USB-токен к компьютеру непосредственно перед началом работы с Системой интернет-банкинга. По окончании работы извлекайте USB-токен из компьютера.

6.14. Храните USB-токены в местах, исключающих несанкционированный доступ к ним. В случае утери USB-токенов немедленно обратитесь в Банк с требованием блокировки Вашей учетной записи в Системе интернет-банкинга.

6.15. Используйте лицензированное программное обеспечение. Помните: помимо того, что Вы несете уголовную ответственность за пользование нелицензированным программным обеспечением в соответствии со статьей 146 Уголовного кодекса Российской Федерации, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

6.16. Регулярно (не реже раза в неделю) проводите проверку на наличие новых версий программного обеспечения, установленного на компьютере, производите установку обновлений операционной системы и пакета JAVA.

6.17. Обеспечьте регулярное автоматическое обновление антивирусных баз настройками антивирусного программного обеспечения. В случае обнаружения вирусов (вредоносных компьютерных программ) на компьютере, после его удаления незамедлительно смените пароль в Системе интернет-банкинга и произведите замену сертификатов ЭП.

6.18. Четко регламентируйте порядок использования компьютера, с которого

осуществляется взаимодействие с Системой интернет-банкинга, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.

6.19. Не устанавливайте на компьютере, который используется для взаимодействия с Системой интернет-банкинга, постороннее программное обеспечение, например, программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.

6.20. Не запускайте на своем компьютере программы, полученные из источников, не заслуживающих доверия.

6.21. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

6.22. Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.

6.23. Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены злоумышленником и использованы для получения доступа к Вашим счетам.

6.24. Перед вводом своего пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официального сайта Банка, просьба сообщить об этом по телефону (8452)427-000, 8 800-100-1319.

6.25. Подключайтесь к услуге «SMS-банкинга», предоставляемой Банком и позволяющей дополнительно подтверждать ЭПД путем ввода в Систему интернет-банкинга кода одноразового пароля, полученного Клиентом из Банка в виде текстового SMS-сообщения. Регулярно проверяйте журнал операций Системы интернет-банкинга. Поддерживайте свою контактную информацию в Системе интернет-банкинга в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

6.26. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе интернет-банкинга, незамедлительно смените пароль, сообщите об инциденте в Банк и произведите смену ключей и сертификатов ЭП.

6.27. Банк располагает техническими средствами мониторинга вредоносных компьютерных программ при работе клиента с Системой интернет-банкинга. В случае выявления этими средствами подозрений на наличие на компьютере Клиента вредоносных компьютерных программ учетная запись Клиента может быть заблокирована.

6.28. При получении информации из Банка об указанной причине блокировки необходимо произвести полную проверку компьютера, используемого для работы с Системой интернет-банкинга, на наличие вирусов. Рекомендуется использовать антивирусные программы разных производителей, т.к. одна антивирусная программа может пропускать некоторые типы вирусов. В случае если после такой проверки вирусы не будут обнаружены, рекомендуется произвести полную переустановку операционной системы на компьютере, используемом для работы в Системе интернет-банкинга.

Приложение А

ПАМЯТКА ДЛЯ КЛИЕНТОВ
о действиях в случае обнаружения несанкционированного списания денежных средств с их счетов в АО «Экономбанк»

В случае обнаружения несанкционированного списания денежных средств со счета Банк рекомендует клиенту осуществить следующие действия:

1. Незамедлительно представить письменное заявление в Банк, заверенное печатью и подписью руководителя, по возможности, на бланке организации о факте несанкционированного списания с указанием даты, суммы платежа, других известных клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств.
2. Для проведения расследования указанного инцидента необходимо оперативно заполнить полученный из Банка опросный лист и направить его в Банк, а также согласовать дату и время выезда к Вам специалиста Банка.
3. Решение о выезде специалиста Банка для проведения расследования клиент принимает самостоятельно. Для проведения расследования необходимо предоставить специалисту Банка файлы протоколов (системных журналов), подтверждающие установку обновлений операционной системы персонального компьютера и антивирусного программного обеспечения, документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения, а также иные документы, которые клиент сочтет необходимыми для рассмотрения инцидента, по существу. Необоснованный отказ в предоставлении требуемых документов может являться основанием для отказа в удовлетворении заявленных Клиентом требований.
4. С момента выявления списания денежных средств с банковского счета не использовать компьютеры, которые эксплуатировались для работы в Системе интернет-банкинга. Их необходимо отключить от сети и обесточить. С высокой долей вероятности они заражены специализированными вредоносными компьютерными программами, поэтому этот шаг позволит предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.
5. Произвести смену ключей и сертификатов электронной подписи (далее – ЭП), используемых для работы с Системой интернет-банкинга в соответствии с действующим Договором. До момента смены ключей работа в Системе интернет-банкинга будет прекращена Банком в связи с компрометацией действующих средств доступа.
6. По факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 272 и 273 Уголовного кодекса Российской Федерации в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим неправомерный доступ неустановленных лиц к Вашей компьютерной информации, что, в свою очередь, привело к несанкционированному клиентом переводу денежных средств клиента.
7. С копией указанного заявления с приложением копии талона правоохранительного органа о приеме заявления, обратиться в Арбитражный суд с исковым заявлением в отношение банка получателя о возврате неосновательного обогащения с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (глава 60 Гражданского кодекса Российской Федерации) Если известны полные реквизиты получателя–физического лица, указанный иск подается в суд общей юрисдикции.

8. Решение об обращении в правоохранительные органы клиент принимает самостоятельно.
9. Срок для предоставления Банку претензий по несанкционированному списанию средств со счета клиента составляет 30 (тридцати) календарных дней с даты осуществления операции. По каждой операции предоставляется отдельная претензия.
10. Решение по претензии принимается Банком в течение 30 (тридцати) рабочих дней со дня подачи заявления в Банк и предоставления клиентом необходимого пакета документов.

    По истечении 30 (тридцати) календарных дней с даты осуществления операции претензии по несанкционированному списанию средств со счета клиента Банком не принимаются.