Письмо Банка России от 05.08.2013 № 146-Т "О рекомендациях по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети "Интернет"

Банк России направляет рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет» (далее - Рекомендации).

Территориальным учреждениям Банка России довести настоящее письмо до сведения кредитных организаций.

Настоящее письмо подлежит официальному опубликованию в «Вестнике Банка России».

Заместитель
Председателя Банка России
Т.Н. Чугунова

Рекомендации по повышению уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети "Интернет"

Приложение
к письму Банка России
от 05.08.2013 № 146-Т
«О рекомендациях
по повышению уровня безопасности
при предоставлении розничных
платежных услуг с использованием
информационно-телекоммуникационной
сети «Интернет»

Настоящие Рекомендации предназначены для использования кредитными организациями, являющимися операторами по переводу денежных средств (далее - операторы по переводу денежных средств), и привлекаемыми ими банковскими платежными агентами в целях повышения уровня безопасности при предоставлении розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет».

1. Операторам по переводу денежных средств в рамках систем управления рисками рекомендуется проводить анализ рисков нарушения защиты информации, связанных с предоставлением розничных платежных услуг с использованием информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), учитывающий в том числе такие факторы, как:
угрозы нарушения защиты информации при предоставлении розничных платежных услуг с использованием сети «Интернет»;
результаты оценки выявленных уязвимостей программного и аппаратного обеспечения и технологий, применяемых при предоставлении клиентам услуг с использованием сети «Интернет»;
совокупность организационных мер защиты информации, программного и аппаратного обеспечения и технологий, а также связанного с обеспечением защиты информации функционала электронных средств платежа (характеристик и возможностей электронных средств платежа, способных предотвратить или затруднить совершение несанкционированных операций), применяемых при предоставлении розничных платежных услуг с использованием сети «Интернет» (далее - меры защиты информации) оператором по переводу денежных средств;
меры защиты информации, необходимость применения которых установлена оператором по переводу денежных средств и доведена до клиента (например, средства аутентификации, предоставленные клиенту оператором по переводу денежных средств);
передачу функций оператора по переводу денежных средств на аутсорсинг[1)];
данные опросов общественного мнения, иных исследований, направленных на получение информации об осведомленности клиентов о мерах обеспечения защиты информации при потреблении услуг с использованием сети «Интернет».

2. Операторам по переводу денежных средств рекомендуется пересматривать результаты анализа рисков: на регулярной основе в полном объеме (не реже, чем один раз в два года);
при изменении или появлении факторов, влияющих на анализ рисков, например, при внесении изменений в процесс предоставления розничных платежных услуг с использованием сети «Интернет»;
по решению руководителя оператора по переводу денежных средств и лиц, ответственных за обеспечение защиты информации при осуществлении переводов денежных средств;
при внесении существенных изменений в состав организационных мер защиты информации, состав или конфигурацию технических средств защиты информации, программного и аппаратного обеспечения, применяемых при предоставлении розничных платежных услуг с использованием сети «Интернет».

3. Операторам по переводу денежных средств рекомендуется учитывать результаты анализа рисков при определении периодичности контроля применения мер защиты информации.

Операторам по переводу денежных средств рекомендуется при необходимости по результатам анализа рисков вносить изменения в используемые меры защиты информации. Если внесение изменений в состав применяемых мер защиты информации не может обеспечить необходимый уровень безопасности при предоставлении розничных платежных услуг или указанные изменения не могут быть внесены по техническим или экономическим причинам, рекомендуется внедрять компенсационные меры защиты информации (например, использовать технологии с другим набором характерных для них рисков и пр.) и проводить анализ рисков для подтверждения того, что необходимый уровень безопасности обеспечивается.

4. Операторам по переводу денежных средств рекомендуется проводить работу, направленную на повышение финансовой грамотности клиентов, в том числе доводить до клиентов информацию о мерах, способствующих повышению уровня безопасности при получении розничных платежных услуг с использованием сети «Интернет», включая использование программно-технических или организационных мер (например, антивирусного программного обеспечения, персональных идентификаторов и пр.).

Указанная работа может осуществляться на регулярной основе (не реже, чем один раз в два года) и (или) при появлении факторов, указанных в п. 2 настоящих Рекомендаций, в том числе на этапе заключения договора между клиентом и оператором по переводу денежных средств.

5. Операторам по переводу денежных средств рекомендуется в случае предоставления клиенту технических средств защиты информации для получения розничных платежных услуг с использованием сети «Интернет» обеспечить применение мер, гарантирующих целостность и подлинность указанных средств при их передаче.

6. Операторам по переводу денежных средств рекомендуется при предоставлении клиентам розничных платежных услуг с использованием сети «Интернет» использовать в том числе: многофакторную аутентификацию[2)];
динамическую аутентификацию клиента (то есть аутентификацию, при которой на одном из этапов используется пароль (код подтверждения), имеющий ограниченный срок действия и ограничение на число использований);
подтверждение операций с помощью одноразовых паролей (кодов подтверждения), при этом пароли (коды подтверждения) должны доводиться до клиента в совокупности с информацией о совершаемой операции (например, сумма операции, получатель и пр.) и доставляться до клиента по альтернативному каналу связи, например, через SMS-сообщения.

7. Операторам по переводу денежных средств рекомендуется информировать клиента обо всех неудачных попытках получения доступа к розничным платежным услугам с использованием сети «Интернет», предоставлять клиенту возможность приостанавливать или иным образом ограничивать доступ к указанным услугам.

8. Операторам по переводу денежных средств рекомендуется информировать клиента о возможной приостановке получения розничных платежных услуг с использованием сети «Интернет», происходящей по инициативе кредитной организации, с пояснением причин, а также о способах и сроках возобновления.

9. Операторам по переводу денежных средств рекомендуется устанавливать период времени, в течение которого пользователь не производит действий, связанных с розничными платежными услугами с использованием сети «Интернет», с момента последнего подтверждения клиентом права получения розничных платежных услуг с использованием сети «Интернет» (период «бездействия»), по истечении которого доступ в систему или возможность осуществления операций блокируется и необходим повторный вход в систему.

10. Операторам по переводу денежных средств рекомендуется использовать механизмы мониторинга[3)] розничных платежных услуг с использованием сети «Интернет», в том числе в целях анализа рисков, например, определять критерии повышенного внимания к операциям (частоту, порядок, сумму, место совершения операции, получателя и пр.).

11. Операторам по переводу денежных средств рекомендуется включать в договор, предоставляющий клиенту возможность получать розничные платежные услуги с использованием сети «Интернет», положение, устанавливающее лимиты операций с использованием сети «Интернет».

12. Операторам по переводу денежных средств рекомендуется предоставлять клиенту возможность управлять лимитами на совершение операций с использованием сети «Интернет» (например, устанавливать максимальный размер операции, совершаемой с использованием сети «Интернет», определять список возможных получателей денежных средств, запрещать совершение операции с использованием сети «Интернет» с отдельными счетами и пр.) и при предоставлении указанной возможности проводить аутентификацию для подтверждения применения/отмены применения указанных лимитов.

13. Операторам по переводу денежных средств рекомендуется использовать различные лимиты операций (например, в зависимости от используемого электронного средства платежа, лимитов, установленных самим клиентом, страны совершения операции и пр.).

14. Операторам по переводу денежных средств рекомендуется информировать клиентов о способах страхования рисков, связанных с совершением операций с использованием сети «Интернет», о способах и порядке получения информации об условиях страхования.

15. Операторам по переводу денежных средств рекомендуется учитывать настоящие Рекомендации при составлении договоров с банковскими платежными агентами (субагентами), предоставляющими электронные средства платежа, позволяющие получить розничные платежные услуги с использованием сети «Интернет», а также доводить Рекомендации до их сведения.

16. Операторам по переводу денежных средств рекомендуется при предоставлении клиентам возможности получения розничных платежных услуг с использованием сети «Интернет» доводить до их сведения соответствующие письма Банка России[4)].

защита информации в национальной платежной системе

[1)] В рамках данных Рекомендаций под аутсорсингом следует понимать передачу на договорной основе выполнения отдельных функций оператора по переводу денежных средств сторонним организациям, например, функции системного администрирования или колл-центра.
[2)] В рамках данных Рекомендаций под многофакторной аутентификацией следует понимать аутентификацию, при которой используется два или более факторов аутентификации. К факторам аутентификации относятся: обладание предметом или устройством (например, персональным идентификатором), знание определенной информации (например, пароля), обладание определенными постоянными неотъемлемыми свойствами (например, отпечатками пальцев).
[3)] В рамках данных Рекомендаций под мониторингом следует понимать сбор, организацию хранения, систематизацию и анализ информации о предоставленных розничных платежных услугах и используемых электронных средствах платежа.
[4)] В рамках данных Рекомендаций к письмам Банка России относятся письма, содержащие рекомендации по дистанционному банковскому обслуживанию, например, письмо Банка России от 07.12.2007 № 197-Т «О рисках при дистанционном банковском обслуживании», письмо Банка России от 31.03.2008 № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга», письмо Банка России от 02.10.2009 № 120-Т «О памятке «О мерах безопасного использования банковских карт», письмо Банка России от 22.11.2010 № 154-Т «О рекомендациях по раскрытию информации об основных условиях использования банковской карты и о порядке урегулирования конфликтных ситуаций, связанных с ее использованием» и другие.