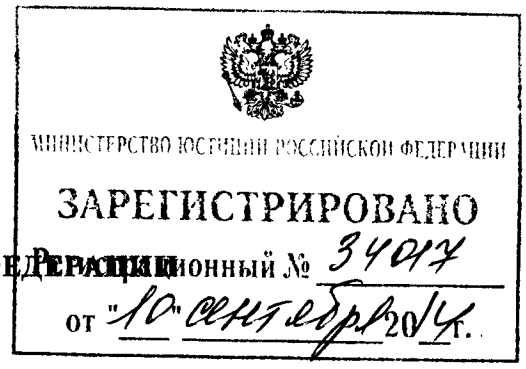

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

«14 »августа 2014 г. № 3361-У

г. Москва

УКАЗАНИЕ

О внесении изменений в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»

1. Внести в Положение Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», зарегистрированное Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930 («Вестник Банка России» от 22 июня 2012 года № 32, от 10 июля 2013 года № 37), следующие изменения.

1.1. В пункте 2.2:

абзац шестой изложить в следующей редакции:

«требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»);»;

дополнить абзацами следующего содержания:

«Требования к обеспечению защиты информации при осуществлении переводов денежных средств помимо требований, указанных в абзацах втором – пятнадцатом настоящего пункта, включают в себя:

требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов;

требования к обеспечению защиты информации при осуществлении переводов денежных средств с применением платежных карт.».

1.2. В пункте 2.3:

абзац первый изложить в следующей редакции:

«2.3. Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается с учетом параметров и статистики выполняемых операций, связанных с осуществлением переводов денежных средств, количества и характера выявленных инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, путем:»;

дополнить подпунктом 2.3.3 следующего содержания:

«2.3.3. применения объектов информационной инфраструктуры, обладающих функциональными и конструктивными особенностями, связанными с обеспечением защиты информации при осуществлении переводов денежных средств и реализации контроля за их функционированием.».

1.3. Пункт 2.5 дополнить подпунктами 2.5.7 – 2.5.10 следующего содержания:

«2.5.7. При разработке программного обеспечения, предназначенного для использования клиентом при осуществлении

переводов денежных средств, самостоятельно или с привлечением сторонних организаций, а также при разработке изменений указанного программного обеспечения оператор по переводу денежных средств обеспечивает реализацию в указанном программном обеспечении функций, связанных:

с выполнением требований к защите информации при осуществлении переводов денежных средств;

с предотвращением несанкционированного доступа к защищаемой информации, передаваемой по информационно-телекоммуникационным сетям, в частности, по сети «Интернет».

Оператор по переводу денежных средств контролирует реализацию указанных функций при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию без дополнительной доработки программного обеспечения.

2.5.8. В случае если программное обеспечение, используемое клиентом при осуществлении переводов денежных средств, разрабатывалось оператором по переводу денежных средств самостоятельно или с привлечением сторонних организаций:

оператор по переводу денежных средств обеспечивает распространение изменений, вносимых в указанное программное обеспечение, направленных на устранение ставших известными оператору по переводу денежных средств уязвимостей указанного программного обеспечения;

оператор по переводу денежных средств определяет являющиеся актуальными версии указанного программного обеспечения и обеспечивает контроль использования клиентом актуальных версий указанного программного обеспечения.

2.5.9. В случае распространения программного обеспечения, используемого клиентом при осуществлении переводов денежных

средств, оператор по переводу денежных средств доводит до клиента инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения и информацию об условиях его эксплуатации либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях эксплуатации данного программного обеспечения.

В случае распространения изменений указанного программного обеспечения оператор по переводу денежных средств вносит соответствующие им изменения в инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения.

2.5.10. Оператор по переводу денежных средств регламентирует и контролирует внесение изменений в программное обеспечение, средства вычислительной техники в составе объектов информационной инфраструктуры, а также в программное обеспечение, используемое клиентом при осуществлении переводов денежных средств; при этом в обязательном порядке должны вноситься изменения, направленные на устранение ставших известными оператору по переводу денежных средств уязвимостей программного обеспечения, средств вычислительной техники.».

1.4. Подпункт 2.6.7 пункта 2.6 признать утратившим силу.

1.5. Пункт 2.8 изложить в следующей редакции:

«2.8. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств с использованием сети «Интернет» включаются следующие требования.

2.8.1. При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают:

применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации, передаваемой по сети «Интернет»;

применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети «Интернет»;

применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения;

минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе объекта информационной инфраструктуры;

фильтрацию сетевых пакетов при обмене информацией между информационно-телекоммуникационными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью «Интернет» с целью защиты от негативного внешнего воздействия из сети «Интернет».

2.8.2. Оператор по переводу денежных средств обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети «Интернет», в частности, в следующих системах (далее при совместном упоминании – системы Интернет-банкинга):

сайтах в сети «Интернет», используемых клиентом на основании договора с оператором по переводу денежных средств в целях формирования и передачи распоряжений о переводе денежных средств;

системах клиент-серверной архитектуры, передающих информацию через сеть «Интернет» и используемых клиентом в целях формирования и передачи распоряжений о переводе денежных средств (за исключением банкоматов, платежных терминалов и электронных устройств, предназначенных для совершения операций с использованием платежных карт и конструкция которых не предусматривает прием (выдачу) наличных денежных средств).

Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости использования пароля многоразового действия и одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга.

В случае принятия соответствующего решения оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, или одноразовый код подтверждения, который:

действителен на протяжении ограниченного периода времени, установленного оператором по переводу денежных средств;

используется для подтверждения клиентом права доступа к системе Интернет-банкинга или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением (договором) условий;

однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору),

подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга;

доводится до клиента по альтернативному системе Интернет-банкинга каналу связи, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения.

Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости направления клиенту по альтернативному системе Интернет-банкинга каналу связи сообщения, содержащего сведения о сформированном с использованием системы Интернет-банкинга распоряжении о переводе денежных средств, включая сумму и получателя денежных средств, до подтверждения клиентом указанного распоряжения с использованием одноразового кода подтверждения.

2.8.3. Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, определяет параметры операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе устанавливает:

максимальную сумму перевода денежных средств с использованием системы Интернет-банкинга за одну операцию и (или) за определенный период времени (например, один день, один месяц);

перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга;

перечень устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга с целью

осуществления переводов денежных средств, на основе идентификаторов указанных устройств;

перечень услуг, предоставляемых с использованием системы Интернет-банкинга;

временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга.

2.8.4. Оператор по переводу денежных средств при передаче клиенту, являющемуся юридическим лицом, программного обеспечения, предназначенного для осуществления переводов денежных средств с использованием системы Интернет-банкинга, доводит до клиента программное средство контроля целостности указанного программного обеспечения и инструкцию по эксплуатации (эксплуатационную документацию) такого программного средства либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию).

2.8.5. При разработке программного обеспечения, используемого клиентом при осуществлении переводов денежных средств с использованием системы Интернет-банкинга и предназначенного для установки на мобильные устройства клиента (далее – система мобильного банкинга), самостоятельно или с привлечением сторонних организаций, а также при разработке изменений указанного программного обеспечения оператор по переводу денежных средств обеспечивает реализацию функций указанного программного обеспечения, связанных с предотвращением несанкционированного доступа к защищаемой информации, хранимой на мобильном устройстве и обрабатываемой в процессе использования системы мобильного банкинга, либо обеспечивает программную реализацию запрета на запись такой информации в мобильное устройство и ее

хранение в мобильном устройстве по окончании сеанса использования системы мобильного банкинга.

2.8.6. Оператор по переводу денежных средств при распространении систем мобильного банкинга с использованием информационных систем (ресурсов), предназначенных, в том числе, для размещения, хранения и распространения с использованием сети «Интернет» программного обеспечения для мобильных устройств (далее – репозитории):

осуществляет размещение установочных файлов системы мобильного банкинга в репозитории с указанием в качестве разработчика данной системы оператора по переводу денежных средств либо уполномоченного им разработчика (при этом оператор по переводу денежных средств обеспечивает информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию);

обеспечивает выявление в репозитории систем мобильного банкинга, размещенных со ссылкой на оператора по переводу денежных средств без получения согласия оператора по переводу денежных средств, и оперативное уведомление клиентов и лиц, обладающих правами на управление репозиторием, о выявленных случаях размещения указанных систем в соответствии с подпунктом 2.12.3 пункта 2.12 настоящего Положения.

2.8.7. Оператор по переводу денежных средств обеспечивает возможность оперативной блокировки доступа (прекращения использования с целью осуществления переводов денежных средств) клиента к системам Интернет-банкинга на основании уведомления, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, например, на основании:

письменного уведомления клиента;

устного уведомления клиента, переданного в соответствии с порядком, установленным оператором по переводу денежных средств;

сообщения (команды), переданного с использованием системы Интернет-банкинга.

2.8.8. Оператор по переводу денежных средств обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу денежных средств стало известно о признаках, указывающих на изменение:

получателя информации, направленной оператором по переводу денежных средств и используемой при аутентификации клиента;

отправителя сообщений (кодов) с номера телефона, указанного в договоре с клиентом, на основании которых осуществляется перевод денежных средств.

К указанным признакам может быть отнесена информация о замене SIM-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре с клиентом.».

1.6. Подпункт 2.12.3 пункта 2.12 изложить в следующей редакции:

«2.12.3. Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе информации о:

рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств;

рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;

появлении в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.».

1.7. Главу 2 дополнить пунктами 2.18 и 2.19 следующего содержания:

«2.18. В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств с применением банкоматов и платежных терминалов включаются следующие требования.

2.18.1. Оператор по переводу денежных средств обеспечивает проведение классификации терминальных устройств дистанционного банковского обслуживания, к которым относятся банкоматы и платежные терминалы, используемые при осуществлении переводов денежных средств (далее при совместном упоминании – ТУ ДБО), с учетом следующего:

возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств;

возможностей осуществления воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО;

особенностей конструкции ТУ ДБО;

места установки ТУ ДБО.

Оператор по переводу денежных средств фиксирует во внутренних документах отнесение каждого ТУ ДБО к одному из определенных в ходе классификации типов (далее – результаты классификации ТУ ДБО) и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО.

Оператор по переводу денежных средств, наряду с факторами, указанными в абзаце первом пункта 2.3 настоящего Положения, учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, с целью выполнения требований подпунктов 2.18.3 – 2.18.8 настоящего пункта.

2.18.2. Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного оборудования.

2.18.3. Оператор по переводу денежных средств обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи.

2.18.4. Оператор по переводу денежных средств обеспечивает размещение на лицевой панели ТУ ДБО или в непосредственной близости от ТУ ДБО сведений, включающих:

наименование оператора по переводу денежных средств, которому принадлежит ТУ ДБО на правах собственности, аренды, лизинга;

идентификатор ТУ ДБО;

телефонный номер (телефонные номера), адреса электронной почты, предназначенные для связи клиентов, использующих данное ТУ ДБО, с оператором по переводу денежных средств, банковским платежным агентом (субагентом) по вопросам, связанным с использованием данного ТУ ДБО;

порядок действий клиента в случае возникновения подозрения о нарушении порядка штатного функционирования ТУ ДБО, а также в случае выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО.

Оператор по переводу денежных средств определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка.

2.18.5. Оператор по переводу денежных средств определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка.

2.18.6. Оператор по переводу денежных средств обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся:

несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода;

несанкционированное внесение изменений в аппаратное обеспечение ТУ ДБО (установка несанкционированного оборудования

на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов;

сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств).

В случае выявления событий, указанных в настоящем подпункте, оператор по переводу денежных средств обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО.

2.18.7. Оператор по переводу денежных средств определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, предусмотренного подпунктом 2.18.6 настоящего пункта, включая его периодичность, в зависимости от факторов, указанных в абзаце первом пункта 2.3 настоящего Положения, а также в зависимости от:

использования систем удаленного мониторинга состояния ТУ ДБО, применения в соответствии с подпунктом 2.18.2 настоящего пункта технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного на (в) ТУ ДБО оборудования;

результатов классификации ТУ ДБО в соответствии с подпунктом 2.18.1 настоящего пункта.

2.18.8. Оператор по переводу денежных средств определяет требования к обеспечению привлеченными к деятельности по оказанию услуг по переводу денежных средств банковскими платежными

агентами (субагентами) защиты информации при использовании ТУ ДБО. Банковский платежный агент (субагент) обеспечивает выполнение указанных требований.

2.19. Оператор по переводу денежных средств осуществляет переводы денежных средств с применением расчетных (дебетовых), кредитных карт:

оснащенных микропроцессором, оснащенных микропроцессором и магнитной полосой, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается после 1 июля 2015 года;

оснащенных магнитной полосой и (или) микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается до 1 июля 2015 года.».

1.8. Абзац второй пункта 5 приложения 1 изложить в следующей редакции:

«обобщающий показатель $EV1_{ПС}$ – характеризующий выполнение группы требований к обеспечению защиты информации при осуществлении переводов денежных средств, определенных в пунктах 2.4 – 2.10, 2.18 и 2.19 настоящего Положения, и вычисляемый как среднее арифметическое оценок выполнения указанных требований, умноженное на корректирующий коэффициент k_1;».

1.9. В приложении 2:

после строки П.18 дополнить строками П.18.1 – П.18.6 следующего содержания:

«

П.18.1	2.5.7	При разработке программного обеспечения, предназначенного для использования клиентом при осуществлении переводов денежных средств, самостоятельно или с привлечением сторонних организаций, а	Требование категории проверки 1

		также при разработке изменений указанного программного обеспечения оператор по переводу денежных средств обеспечивает реализацию в указанном программном обеспечении функций, связанных: с выполнением требований к защите информации при осуществлении переводов денежных средств; с предотвращением несанкционированного доступа к защищаемой информации, передаваемой по информационно-телекоммуникационным сетям, в частности, по сети «Интернет»	
П.18.2	2.5.7	Оператор по переводу денежных средств контролирует реализацию функций, указанных в подпункте 2.5.7 пункта 2.5 настоящего Положения, при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию без дополнительной доработки программного обеспечения	Требование категории проверки 1
П.18.3	2.5.8	В случае если программное обеспечение, используемое клиентом при осуществлении переводов денежных средств, разрабатывалось оператором по переводу денежных средств самостоятельно или с привлечением сторонних организаций: оператор по переводу денежных средств обеспечивает распространение изменений, вносимых в указанное	Требование категории проверки 1

		программное обеспечение, направленных на устранение ставших известными оператору по переводу денежных средств уязвимостей указанного программного обеспечения; оператор по переводу денежных средств определяет являющиеся актуальными версии указанного программного обеспечения и обеспечивает контроль использования клиентом актуальных версий указанного программного обеспечения	
П.18.4	2.5.9	В случае распространения программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, оператор по переводу денежных средств доводит до клиента инструкцию по эксплуатации (эксплуатационную документацию) данного программного обеспечения и информацию об условиях его эксплуатации либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях эксплуатации данного программного обеспечения	Требование категории проверки 1
П.18.5	2.5.9	В случае распространения изменений программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, оператор по переводу денежных средств вносит соответствующие им изменения в инструкцию по эксплуатации	Требование категории проверки 1

		(эксплуатационную документацию) данного программного обеспечения	
П.18.6	2.5.10	Оператор по переводу денежных средств регламентирует и контролирует внесение изменений в программное обеспечение, средства вычислительной техники в составе объектов информационной инфраструктуры, а также в программное обеспечение, используемое клиентом при осуществлении переводов денежных средств; при этом в обязательном порядке должны вноситься изменения, направленные на устранение ставших известными оператору по переводу денежных средств уязвимостей программного обеспечения, средств вычислительной техники	Требование категории проверки 1

»;

строку П.37 признать утратившей силу;

строки П.52 – П.57 изложить в следующей редакции:

«

П.52	2.8.1	При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации, передаваемой	Требование категории проверки 1

		по сети «Интернет»	
П.53	2.8.1	При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети «Интернет»	Требование категории проверки 1
П.54	2.8.1	При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения	Требование категории проверки 1
П.55	2.8.1	При использовании сети «Интернет» для осуществления переводов денежных	Требование категории

		средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе объекта информационной инфраструктуры	проверки 1
П.56	2.8.1	При использовании сети «Интернет» для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают фильтрацию сетевых пакетов при обмене информацией между информационно-телекоммуникационными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью «Интернет» с целью защиты от негативного внешнего воздействия из сети «Интернет»	Требование категории проверки 1
П.57	2.8.2	Оператор по переводу денежных средств обеспечивает идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче распоряжений в целях осуществления переводов денежных средств с использованием сети «Интернет», в частности, в системах Интернет-банкинга	Требование категории проверки 1

»;

после строки П.57 дополнить строками П.57.1 – П.57.10 следующего содержания:

«

П.57.1	2.8.2	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости использования пароля многоразового действия и одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга	Требование категории проверки 3
П.57.2	2.8.2	В случае принятия решения о необходимости использования одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга, оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, или одноразовый код подтверждения, который: действителен на протяжении ограниченного периода времени, установленного оператором по переводу денежных средств; используется для подтверждения клиентом права доступа к системе	Требование категории проверки 3

		Интернет-банкинга или для подтверждения распоряжения (нескольких распоряжений) о разовом переводе (разовых переводах) денежных средств или распоряжения (договора) о периодических переводах денежных средств в определенную дату и (или) период, при наступлении определенных распоряжением (договором) условий; однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга; доводится до клиента по альтернативному системе Интернет-банкинга каналу связи, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения	
П.57.3	2.8.2	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости направления клиенту по альтернативному системе Интернет-банкинга каналу связи сообщения, содержащего сведения о сформированном с использованием	Требование категории проверки 2

		системы Интернет-банкинга распоряжении о переводе денежных средств, включая сумму и получателя денежных средств, до подтверждения клиентом указанного распоряжения с использованием одноразового кода подтверждения	
П.57.4	2.8.3	Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, определяет параметры операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе устанавливает: максимальную сумму перевода денежных средств с использованием системы Интернет-банкинга за одну операцию и (или) за определенный период времени (например, один день, один месяц); перечень возможных получателей денежных средств, в адрес которых могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга; перечень устройств, с использованием которых может осуществляться доступ к системе Интернет-банкинга с целью осуществления переводов денежных средств, на основе идентификаторов указанных устройств;	Требование категории проверки 1

		перечень услуг, предоставляемых с использованием системы Интернет-банкинга; временной период, в который могут быть совершены переводы денежных средств с использованием системы Интернет-банкинга	
П.57.5	2.8.4	Оператор по переводу денежных средств при передаче клиенту, являющемуся юридическим лицом, программного обеспечения, предназначенного для осуществления переводов денежных средств с использованием системы Интернет-банкинга, доводит до клиента программное средство контроля целостности указанного программного обеспечения и инструкцию по эксплуатации (эксплуатационную документацию) такого программного средства либо указывает общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию)	Требование категории проверки 3
П.57.6	2.8.5	При разработке системы мобильного банкинга самостоятельно или с привлечением сторонних организаций, а также при разработке изменений системы мобильного банкинга оператор по переводу денежных средств обеспечивает реализацию функций системы мобильного банкинга, связанных с предотвращением несанкционированного доступа к защищаемой информации,	Требование категории проверки 1

		хранимой на мобильном устройстве и обрабатываемой в процессе использования системы мобильного банкинга, либо обеспечивает программную реализацию запрета на запись такой информации в мобильное устройство и ее хранение в мобильном устройстве по окончании сеанса использования системы мобильного банкинга	
П.57.7	2.8.6	Оператор по переводу денежных средств при распространении систем мобильного банкинга с использованием репозиториев осуществляет размещение установочных файлов системы мобильного банкинга в репозитории с указанием в качестве разработчика данной системы оператора по переводу денежных средств либо уполномоченного им разработчика (при этом оператор по переводу денежных средств обеспечивает информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию) .	Требование категории проверки 1
П.57.8	2.8.6	Оператор по переводу денежных средств при распространении систем мобильного банкинга с использованием репозиториев обеспечивает выявление в репозитории систем мобильного банкинга, размещенных со ссылкой на оператора по переводу денежных средств без получения согласия оператора по переводу денежных средств, и оперативное уведомление клиентов и лиц,	Требование категории проверки 1

		обладающих правами на управление репозиторием, о выявленных случаях размещения указанных систем в соответствии с подпунктом 2.12.3 пункта 2.12 настоящего Положения	
П.57.9	2.8.7	Оператор по переводу денежных средств обеспечивает возможность оперативной блокировки доступа (прекращения использования с целью осуществления переводов денежных средств) клиента к системам Интернет-банкинга на основании уведомления, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, например, на основании: письменного уведомления клиента; устного уведомления клиента, переданного в соответствии с порядком, установленным оператором по переводу денежных средств; сообщения (команды), переданного с использованием системы Интернет-банкинга	Требование категории проверки 3
П.57.10	2.8.8	Оператор по переводу денежных средств обеспечивает приостановление пересылки клиенту извещений (подтверждений) о принятии к исполнению распоряжений и иной защищаемой информации и осуществления перевода денежных средств на основании сообщений (кодов), отправленных с номера телефона, указанного в договоре с клиентом, в случае если оператору по переводу	Требование категории проверки 3

		денежных средств стало известно о признаках, указывающих на изменение: получателя информации, направленной оператором по переводу денежных средств и используемой при аутентификации клиента; отправителя сообщений (кодов) с номера телефона, указанного в договоре с клиентом, на основании которых осуществляется перевод денежных средств. К указанным признакам может быть отнесена информация о замене SIM-карты клиента, прекращении обслуживания или смене номера телефона, указанного в договоре с клиентом	

»;

строку П.96 изложить в следующей редакции:

«

П.96	2.12.3	Оператор по переводу денежных средств обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе информации о: о рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении)	Требование категории проверки 3

		устройства, с использованием которого клиентом осуществлялся перевод денежных средств; о рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода; о появлении в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения	

»;

дополнить строками П.130 – П.142 следующего содержания:

«

П.130	2.18.1	Оператор по переводу денежных средств обеспечивает проведение классификации ТУ ДБО, с учетом следующего: возможностей несанкционированного получения информации, необходимой для осуществления переводов денежных средств; возможностей осуществления	Требование категории проверки 1

		воздействия, приводящего к сбоям, отказам, повреждению ТУ ДБО; особенностей конструкции ТУ ДБО; места установки ТУ ДБО	
П.131	2.18.1	Оператор по переводу денежных средств фиксирует во внутренних документах результаты классификации ТУ ДБО и проводит пересмотр результатов классификации ТУ ДБО при изменении факторов, влияющих на классификацию ТУ ДБО	Требование категории проверки 1
П.132	2.18.1	Оператор по переводу денежных средств, наряду с факторами, указанными в абзаце первом пункта 2.3 настоящего Положения, учитывает результаты классификации ТУ ДБО при выборе организационных мер защиты информации, технических средств защиты информации, а также функциональных и конструктивных особенностей ТУ ДБО, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, с целью выполнения требований подпунктов 2.18.3 – 2.18.8 пункта 2.18 настоящего Положения	Требование категории проверки 1
П.133	2.18.2	Оператор по переводу денежных средств принимает и фиксирует во внутренних документах решения о необходимости установки на (в) ТУ ДБО технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно	Требование категории проверки 2

		установленного оборудования	
П.134	2.18.3	Оператор по переводу денежных средств обеспечивает контроль состава объектов информационной инфраструктуры в сегментах информационно-телекоммуникационных сетей, в составе которых присутствуют ТУ ДБО, за исключением случая использования услуг радиотелефонной подвижной связи	Требование категории проверки 1
П.135	2.18.4	Оператор по переводу денежных средств обеспечивает размещение на лицевой панели ТУ ДБО или в непосредственной близости от ТУ ДБО сведений, включающих: наименование оператора по переводу денежных средств, которому принадлежит ТУ ДБО на правах собственности, аренды, лизинга; идентификатор ТУ ДБО; телефонный номер (телефонные номера), адреса электронной почты, предназначенные для связи клиентов, использующих данное ТУ ДБО, с оператором по переводу денежных средств, банковским платежным агентом (субагентом) по вопросам, связанным с использованием данного ТУ ДБО; порядок действий клиента в случае возникновения подозрения о нарушении порядка штатного функционирования ТУ ДБО, а также в случае выявления признаков событий, связанных с нарушением обеспечения защиты информации при осуществлении	Требование категории проверки 3

		переводов денежных средств с применением ТУ ДБО	
П.136	2.18.4	Оператор по переводу денежных средств определяет во внутренних документах порядок работы с заявлениями клиентов о выявленных событиях, связанных с нарушением обеспечения защиты информации при осуществлении переводов денежных средств с применением ТУ ДБО, и обеспечивает выполнение указанного порядка	Требование категории проверки 1
П.137	2.18.5	Оператор по переводу денежных средств определяет порядок настройки программного обеспечения, средств вычислительной техники в составе ТУ ДБО, включая информацию о конфигурации, определяющей параметры работы технических средств защиты информации, и обеспечивает выполнение указанного порядка	Требование категории проверки 1
П.138	2.18.6	Оператор по переводу денежных средств обеспечивает периодический контроль состояния ТУ ДБО с целью выявления событий, влияющих на обеспечение защиты информации при осуществлении переводов денежных средств. К таким событиям, в том числе, относятся: несанкционированное внесение изменений в программное обеспечение ТУ ДБО, включая внедрение вредоносного кода; несанкционированное внесение изменений в аппаратное обеспечение ТУ	Требование категории проверки 1

		ДБО (установка несанкционированного оборудования на (в) ТУ ДБО), включая несанкционированное использование коммуникационных портов; сбои и отказы в работе технических средств защиты информации, устройств приема платежных карт (при наличии данных устройств), устройств приема наличных денежных средств (при наличии данных устройств), устройств выдачи наличных денежных средств (при наличии данных устройств)	
П.139	2.18.6	В случае выявления событий, указанных в подпункте 2.18.6 пункта 2.18 настоящего Положения, оператор по переводу денежных средств обеспечивает приведение ТУ ДБО в такое состояние, при котором обслуживание клиентов невозможно, до минимизации возможности наступления негативных последствий выявленных событий или устранения несанкционированных изменений в программном и аппаратном обеспечении ТУ ДБО	Требование категории проверки 3
П.140	2.18.7	Оператор по переводу денежных средств определяет во внутренних документах и обеспечивает выполнение порядка проведения контроля, предусмотренного подпунктом 2.18.6 пункта 2.18 настоящего Положения, включая его периодичность, в зависимости от факторов, указанных в абзаце первом пункта 2.3 настоящего Положения, а также в зависимости от: использования систем удаленного мониторинга состояния ТУ ДБО,	Требование категории проверки 1

		применения в соответствии с подпунктом 2.18.2 пункта 2.18 настоящего Положения технических средств, предназначенных для обнаружения и (или) предотвращения (затруднения) работы несанкционированно установленного на (в) ТУ ДБО оборудования; результатов классификации ТУ ДБО в соответствии с подпунктом 2.18.1 пункта 2.18 настоящего Положения	
П.141	2.18.8	Оператор по переводу денежных средств определяет требования к обеспечению привлеченными к деятельности по оказанию услуг по переводу денежных средств банковскими платежными агентами (субагентами) защиты информации при использовании ТУ ДБО	Требование категории проверки 2
П.142	2.19	Оператор по переводу денежных средств осуществляет переводы денежных средств с применением расчетных (дебетовых), кредитных карт: оснащенных микропроцессором, оснащенных микропроцессором и магнитной полосой, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается после 1 июля 2015 года; оснащенных магнитной полосой и (или) микропроцессором, выданных (эмитированных) кредитными организациями на территории Российской Федерации, срок действия которых начинается до 1 июля 2015 года	Требование категории проверки 3

».

2. Настоящее Указание в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 16 июня 2014 года № 18) вступает в силу по истечении 180 дней со дня его официального опубликования в «Вестнике Банка России».

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

СОГЛАСОВАНО

Директор
Федеральной службы безопасности
Российской Федерации А.В. Бортников

Директор
Федеральной службы
по техническому и экспортному контролю В.В. Селин

Верно
Главный экономист
Департамента национальной платежной системы
Банка России
Д.С. Кутнов
14.08.2014

Центральный банк Российской Федерации (Банк России)
Административный департамент
Для документов
№ 4