Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

«____» _____ 2017 г. № _____

г. Москва

У К А З А Н И Е

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. На основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2012, № 53, ст. 7592; 2013, № 27, ст. 3477; № 30, ст. 4084; № 52, ст. 6968; 2014, № 19, ст. 2315, ст. 2317; № 43, ст. 5803; 2015, № 1, ст. 8, ст. 14; 2016, № 27, ст. 4221, ст. 4223; 2017, № 15, ст. 2134; № 18, ст. 2665) 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, 10 сентября 2014 года № 34017, следующие изменения.

1.1. В пункте 2.2:

абзац шестнадцатый изложить в следующей редакции:

«Оператор по переводу денежных средств, оператор платежной системы, оператор услуг платежной инфраструктуры к инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, относят события, которые возникли вследствие нарушения или попыток нарушения целостности, конфиденциальности и (или) доступности защищаемой информации, в том числе включенные в перечень инцидентов, размещаемый Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – перечень инцидентов).»;

абзацы семнадцатый – девятнадцатый признать утратившими силу.

1.2. Пункт 2.5 дополнить подпунктом $2.5.5^{1}$ следующего содержания:

«$2.5.5^{1}$. Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры на стадиях создания и эксплуатации объектов информационной инфраструктуры обеспечивают:

использование для осуществления переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст

«Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014) (далее – ГОСТ Р ИСО/МЭК 15408-3-2013);

ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений оператор по переводу денежных средств, оператор услуг платежной инфраструктуры привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) (далее – Постановление Правительства Российской Федерации № 79).

При модернизации объектов информационной инфраструктуры по решению оператора по переводу денежных средств, оператора услуг платежной инфраструктуры проводится анализ уязвимостей только объектов информационной инфраструктуры, подвергнутых модернизации.».

1.3. Подпункт 2.8.3 пункта 2.8 изложить в следующей редакции:

«2.8.3. Оператор по переводу денежных средств на основании заявления клиента, переданного способом, определенным договором оператора по переводу денежных средств с клиентом, определяет ограничения по параметрам операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе указанные в подпункте 2.10.7 пункта 2.10 настоящего Положения.».

1.4. Абзац первый подпункта 2.9.1 пункта 2.9 изложить в следующей редакции:

«2.9.1. Обеспечение защиты информации с помощью СКЗИ осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2012, № 29, ст. 3988; 2013, № 14, ст. 1668, № 27; ст. 3463, ст. 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65; № 26, ст. 3889), Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350, и технической документацией на СКЗИ. Обеспечение защиты персональных данных с помощью СКЗИ дополнительно осуществляется в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении состава и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620.».

1.5. Пункт 2.10 дополнить подпунктами 2.10.5–2.10.7 следующего содержания:

«2.10.5. При осуществлении переводов денежных средств с использованием информационно-телекоммуникационной сети «Интернет» и размещении программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых оператором по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от

воздействия вредоносного кода, оператор по переводу денежных средств обеспечивает реализацию технологических мер по разделению контуров подготовки и подтверждения клиентом электронных сообщений (далее – разделение контуров) и (или) реализует ограничения по параметрам операций по осуществлению переводов денежных средств, определяемые договором оператора по переводу денежных средств с клиентом, а также обеспечивает возможность установления указанных ограничений по инициативе клиента.

2.10.6. Реализуемые оператором по переводу денежных средств технологические меры разделения контуров обеспечивают:

идентификацию и аутентификацию клиента при подготовке клиентом и при подтверждении клиентом электронных сообщений;

возможность использования клиентом независимых программных сред для подготовки и подтверждения электронных сообщений;

возможность контроля клиентом реквизитов распоряжений о переводе денежных средств при подготовке электронных сообщений (пакета электронных сообщений) и их подтверждении;

аутентификацию входных электронных сообщений (пакета электронных сообщений) путем использования и сравнения (сверки) аутентификационных данных, сформированных на основе информации о реквизитах распоряжений о переводе денежных средств при подготовке клиентом электронных сообщений (пакета электронных сообщений) и подтверждении клиентом электронных сообщений;

удостоверение оператором по переводу денежных средств в праве клиента распоряжаться денежными средствами только в случае положительных результатов аутентификации входных электронных сообщений (пакета электронных сообщений).

В зависимости от 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, реализуемые технологические меры по разделению контуров могут дополнительно обеспечивать:

возможность выполнения подтверждения клиентом электронных сообщений вне операционной системы, используемой для подготовки электронных сообщений;

установление временных ограничений на выполнение клиентом подтверждения электронных сообщений.

2.10.7. При реализации ограничений по параметрам операций по осуществлению переводов денежных средств могут применяться следующие ограничения на:

максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени;

перечень возможных получателей денежных средств;

временной период, в который могут быть совершены переводы денежных средств;

географическое местоположение устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;

перечень идентификаторов устройств, с использованием которых может осуществляться подготовка и (или) подтверждение клиентом электронных сообщений;

перечень предоставляемых услуг, связанных с осуществлением переводов денежных средств;

иные ограничения по параметрам операций по осуществлению переводов денежных средств.».

1.6. Дополнить пунктом 2.13^{1} следующего содержания:

«$2.13.^{1}$ Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры осуществляют информирование Банка России:

о выявленных инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе включенных в перечень инцидентов;

о планируемых мероприятиях по раскрытию информации о инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая размещение информации на официальных сайтах в информационно-телекоммуникационной сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до проведения мероприятия.

Информирование осуществляется в форме электронных сообщений. Информация о технологиях подготовки, направлении и форматах электронных сообщений, согласованных с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, размещается на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».».

1.7. Абзац шестой подпункта 2.15.1 пункта 2.15 изложить в следующей редакции:

«Оценка соответствия осуществляется оператором по переводу денежных средств, оператором платежной системы, оператором услуг платежной инфраструктуры с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства Российской Федерации № 79.».

1.8. Подпункт 2.16.1 пункта 2.16 дополнить абзацем следующего содержания:

«Оператор национально значимой платежной системы уведомляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, об установленных требованиях к содержанию, форме и периодичности представления указанной в абзаце первом настоящего подпункта информации в части применения СКЗИ.».

1.19. В приложении 2:

после строки П.14 дополнить строками П.14.1 и П.14.2 следующего содержания:

«

П.14.1	2.5.5[1]	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры на стадии создания и эксплуатации объектов информационной инфраструктуры обеспечивают использование для осуществления переводов денежных средств прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже чем ОУД 4 в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3-2013	Требование категории проверки 3
П.14.2	2.5.5[1]	Оператор по переводу денежных средств, оператор услуг платежной инфраструктуры на стадии создания и эксплуатации объектов информационной инфраструктуры обеспечивают проведение ежегодного тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры	Требование категории проверки 3

»;

строку П.57.4 изложить в следующей редакции:

«

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 ограничения по параметрам операций, которые могут осуществляться клиентом с использованием системы Интернет-банкинга, в том числе указанные в подпункте 2.10.7 пункта 2.10 настоящего Положения	Требование категории проверки 1

»;

строку П.58 изложить в следующей редакции:

«

П.58	2.9.1	Обеспечение защиты информации с помощью СКЗИ осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, и технической документацией на СКЗИ. Обеспечение защиты персональных данных с помощью СКЗИ дополнительно осуществляется в соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении состава и содержании организационных и технических мер по обеспечению безопасности персональных данных при их	Требование категории проверки 3

		обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»	

»;

после строки П.81 дополнить строками П.81.1 и П.81.2 следующего содержания:

«

П.81.1	2.10.5	При осуществлении переводов денежных средств с использованием информационно-телекоммуникационной сети «Интернет» и (или) размещении программного обеспечения, используемого клиентом при осуществлении переводов денежных средств, на средствах вычислительной техники, для которых оператором по переводу денежных средств не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, оператор по переводу денежных средств обеспечивает реализацию технологических мер по разделению контуров подготовки и подтверждения клиентом электронных сообщений и (или) реализует ограничения по параметрам операций по осуществлению переводов денежных средств, определяемых договором оператора по переводу денежных средств с клиентом, а также обеспечивает возможность установления указанных ограничений по инициативе клиента	Требование категории проверки 1
П.81.2	2.10.6	Реализуемые оператором по переводу	Требование

		денежных средств технологические меры разделения контуров обеспечивают: идентификацию и аутентификацию клиента при подготовке клиентом и при подтверждении клиентом электронных сообщений; возможность использования клиентом независимых программных сред для подготовки и подтверждения электронных сообщений; возможность контроля клиентом реквизитов распоряжений о переводе денежных средств при подготовке электронных сообщений (пакета электронных сообщений) и их подтверждении; аутентификацию входных электронных сообщений (пакета электронных сообщений) путем использования и сравнения (сверки) аутентификационных данных, сформированных на основе информации о реквизитах распоряжений о переводе денежных средств при подготовке клиентом электронных сообщений (пакета электронных сообщений) и подтверждении клиентом электронных сообщений; удостоверение оператором по переводу денежных средств распоряжений о переводе денежных средств только в случае положительных результатов аутентификации входных электронных сообщений (пакета электронных сообщений)	категории проверки 1

»;

после строки П.115 дополнить строкой П.115.1 следующего содержания:

«

П.115.1	2.16.1	Оператор национально значимой платежной системы уведомляет федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, об установленных требованиях к содержанию, форме и периодичности представления указанной в абзаце первом подпункта 2.16.1 пункта 2.16 настоящего Положения информации в части применения СКЗИ	Требование категории проверки 3

».

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от __ _____ 2017 года № _____) вступает в силу с 1 июля 2018 года, за исключением абзаца третьего подпункта 1.2 и подпункта 1.5 пункта 1 настоящего Указания.

Абзац третий подпункта 1.2 и подпункт 1.5 пункта 1 настоящего Указания вступают в силу с 1 июля 2019 года.

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