Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

« » _____ 2018 г. № -П

г. Москва

П О Л О Ж Е Н И Е

Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности

1. На основании статьи 57.4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2004, № 31, ст. 3233; 2005, № 25, ст. 2426; 2007, № 1, ст. 10; 2008, № 42, ст. 4696; № 44, ст. 4982; 2009, № 1, ст. 25; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 48, ст. 6728; 2012, № 53, ст. 7591; 2013, № 27, ст. 3438; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695; № 52, ст. 6975; 2014, № 30, ст. 4219; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, 37; № 27, ст. 3958; № 29, ст. 4348, 4357; 2016, № 1, ст. 46, 50; № 26, ст. 3891; № 27, ст. 4225, 4295; 2017, № 18, ст. 2661, 2669; № 30, ст. 4456; № 31, ст. 4830; 2018, № 11, ст. 1584, 1588; 2018, № 24, ст. 3400; 2018, № 27, ст. 3950) настоящее Положение устанавливает

обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента (далее – требования к защите информации при осуществлении банковской деятельности), за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами.

2. Требования к защите информации при осуществлении банковской деятельности, связанной с осуществлением переводов денежных средств, применяются с учетом Положения 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», зарегистрированным Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930, 10 сентября 2014 года № 34017, 22 июня 2018 года № 51411 (далее – Положение Банка России от 9 июня 2012 года №382-П).

Термины, используемые в настоящем Положении, применяются в значениях, установленных Положением Банка России от 9 июня 2012 года №382-П.

3. Для проведения работ по обеспечению защиты информации при осуществлении банковской деятельности кредитные организации могут привлекать организации, которые должны иметь лицензии на осуществление деятельности по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

4. Требования к защите информации при осуществлении банковской деятельности применяются для обеспечения защиты следующей информации (далее – защищаемая информация):

информации, подготавливаемой, обрабатываемой и хранимой в целях осуществления банковских операций, определенных в статье 5 Федерального закона от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности» (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, №27, ст. 357; Собрание законодательства Российской Федерации, 1996, №6, ст. 492; 2001, №33, ст. 3424; 2003, № 27, ст. 2700; № 52, ст. 5033; 2004, № 27, ст. 2711; 2005, № 1, ст. 45; 2007, №31, ст. 4011; №41, ст. 4845; 2009, №23, ст. 2776; №30, ст. 3739; 2010, №31, ст. 4193; №47, ст. 6028; 2011, №7, ст. 905; №27, ст. 3873; №48, ст. 6730; №50, ст. 7351; 2012, №27, ст. 3588; №50, ст. 6954; №53, ст. 7605; 2013, №11, ст. 1076; №19, ст. 2329; №26, ст. 3207; №27, ст. 3438; №30, ст. 4084; №51, ст. 6699; 2014, №26, ст. 3395; №52, ст. 7543; 2015, №27, ст. 3950; №29, ст. 4357; 2017, №18, ст. 2661)(далее – осуществление банковских операций);

информации об осуществленных банковских операциях;

информации, содержащейся в первичных документах на осуществление банковских операций, формируемых работниками кредитных организаций (далее – работники) и (или) клиентами кредитных организаций (далее – клиенты);

информации, необходимой для идентификации и аутентификации клиентов при осуществлении банковских операций и удостоверения клиентами права на осуществление банковских операций;

ключевой информации средств криптографической защиты информации (далее – СКЗИ), используемой при подготовке и осуществлении банковских операций;

информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, используемых для осуществления банковской деятельности в целях обработки защищаемой информации;

информации о конфигурации, определяющей параметры работы

технических средств защиты информации, используемых для осуществления банковской деятельности в целях обработки защищаемой информации;

информации, подлежащей обязательной защите в соответствии с пунктом 2.1 Положения Банка России от 9 июня 2012 года №382-П.

5. Для объектов информационной инфраструктуры, а также автоматизированных систем, используемых для осуществления банковских операций в целях обработки, передачи, хранения защищаемой информации, кредитные организации обеспечивают следующие уровни защиты информации, определенные национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Росстандарта от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2017).

5.1. Усиленный уровень защиты информации реализуется системно значимыми кредитными организациями, кредитными организациями, выполняющими функции оператора услуг платежной инфраструктуры значимых платежных систем, кредитными организациями, значимыми на рынке платежных услуг, при условии достижения показателя среднедневного (по отношению к числу календарных дней в году) количества осуществляемых банковских операций более 3 млн. единиц.

5.2. Стандартный уровень защиты информации реализуется кредитными организациями, не относящимися к кредитным организациям, указанным в подпункте 5.1 настоящего пункта.

6. Кредитные организации на стадиях создания и эксплуатации объектов информационной инфраструктуры обеспечивают:

использование для осуществления банковских операций 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);

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

Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений кредитные организации могут привлекать 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 кредитной организации проводится анализ уязвимостей только объектов информационной инфраструктуры, подвергнутых модернизации.

Кредитные организации обеспечивают обработку защищаемой информации с использованием автоматизированных систем, создаваемых (модернизируемых) кредитной организацией самостоятельно и (или) с привлечением сторонних организаций.

7. Кредитные организации при разработке программного обеспечения, используемого клиентом при осуществлении банковских операций, в том числе при разработке изменений указанного программного обеспечения, обеспечивают реализацию в указанном программном обеспечении функций, связанных:

с выполнением требований к защите информации при осуществлении банковских операций;

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

Кредитные организации контролируют реализацию указанных функций при разработке программного обеспечения с привлечением сторонней организации, а также при закупке готового к использованию программного обеспечения без дополнительной доработки.

7.1. Кредитные организации:

обеспечивают распространение изменений, вносимых в программное обеспечение, используемое клиентом при осуществлении банковских операций, направленных на устранение ставших известными кредитной организации уязвимостей указанного программного обеспечения;

определяют являющиеся актуальными версии программного обеспечения, используемого клиентом при осуществлении банковских операций, и обеспечивают контроль использования клиентом актуальных версий указанного программного обеспечения.

7.2. Кредитные организации доводят до клиента инструкцию по безопасной эксплуатации (эксплуатационную документацию) программного обеспечения, используемого клиентом при осуществлении банковских

операций, и информацию об условиях его безопасной эксплуатации либо указывают общедоступный ресурс, с использованием которого клиент имеет возможность получить указанную инструкцию (эксплуатационную документацию) и информацию об условиях безопасной эксплуатации данного программного обеспечения.

7.3. В случае распространения изменений указанного программного обеспечения кредитные организации вносят соответствующие им изменения в инструкцию по безопасной эксплуатации (эксплуатационную документацию) данного программного обеспечения.

7.4. Кредитные организации при распространении программного обеспечения, используемого клиентом при осуществлении банковских операций с использованием сети «Интернет» и предназначенного для установки на устройства подвижной радиотелефонной связи (далее – мобильное программное обеспечение), в рамках информационных систем (ресурсов), предназначенных, в том числе, для размещения, хранения и распространения с использованием сети «Интернет» мобильного программного обеспечения (далее - репозитории):

осуществляют размещение установочных файлов мобильного программного обеспечения в репозитории с указанием в качестве разработчика данной системы кредитной организации либо уполномоченного им разработчика (при этом кредитные организации обеспечивают информирование клиентов об уполномоченных им разработчиках по каналу, альтернативному репозиторию);

обеспечивают выявление в репозитории мобильного программного обеспечения, размещенного со ссылкой на кредитную организацию без получения согласия кредитной организации, и оперативное уведомление клиентов и лиц, обладающих правами на управление репозиторием, о выявленных случаях размещения указанного программного обеспечения.

8. Кредитные организации обеспечивают регистрацию лиц, обладающих правами:

по осуществлению доступа к защищаемой информации;

по управлению криптографическими ключами;

по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению банковских операций.

Кредитные организации обеспечивают регистрацию своих работников, обладающих правами по формированию электронных сообщений, содержащих первичные документы на осуществление банковских операций (далее – электронные сообщения).

9. Кредитные организации обеспечивают формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода на объектах информационной инфраструктуры, а также на автоматизированных системах, используемых для осуществления банковских операций, кредитные организации обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

Кредитные организации приостанавливают при необходимости осуществление банковской деятельности на период устранения последствий заражения вредоносным кодом.

10. Обеспечение защиты информации с помощью СКЗИ при осуществлении банковской деятельности 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.

10.1. В случае если кредитная организация применяет СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

10.2. Криптографические ключи изготавливаются клиентом (самостоятельно) и (или) кредитной организацией.

Безопасность процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

11. Кредитные организации обеспечивают удостоверение первичных документов на осуществление банковских операций, содержащихся в электронных сообщениях, электронной подписью или иным аналогом собственноручной подписи, кодами, паролями и иными средствами, позволяющими обеспечить целостность и подтвердить составление

указанного первичного документа уполномоченным на это лицом.

12. Кредитные организации при осуществлении банковской деятельности с использованием сети «Интернет» и размещении программного обеспечения, используемого клиентом при осуществлении банковских операций на средствах вычислительной техники, для которых кредитными организациями не обеспечивается непосредственный контроль защиты информации от воздействия вредоносного кода, обеспечивают реализацию технологических мер по использованию раздельных информационно-коммуникационных технологий для подготовки электронных сообщений и передачи клиентами подтверждений об исполнении первичных документов на осуществление банковских операций (далее – технологические меры по использованию раздельных технологий) и (или) реализовывают ограничения по параметрам банковских операций, определяемые договором кредитной организации с клиентом, а также обеспечивают возможность установления указанных ограничений по инициативе клиента.

12.1. Реализуемые кредитными организациями технологические меры по использованию раздельных технологий должны обеспечивать:

идентификацию и аутентификацию клиента при подготовке клиентом и при подтверждении клиентом электронных сообщений в соответствии с требованиями законодательства Российской Федерации;

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

возможность контроля клиентом реквизитов первичных документов на осуществление банковских операций 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 первичных документов на осуществление банковских операций

при подготовке клиентом электронных сообщений (пакета электронных сообщений) и подтверждении клиентом электронных сообщений;

удостоверение кредитной организацией в праве клиента осуществлять банковские операции только в случае положительных результатов аутентификации входных электронных сообщений (пакета электронных сообщений).

В зависимости от параметров и статистики выполняемых банковских операций, количества и характера выявленных инцидентов, связанных с нарушением требований к защите информации при осуществлении указанных банковских операций, реализуемые технологические меры по использованию раздельных технологий 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.

12.2. При реализации ограничений по параметрам банковских операций могут применяться следующие ограничения:

на максимальную сумму за одну банковскую операцию и (или) за определенный период времени;

на перечень возможных получателей банковских операций;

на временной период, в который могут быть осуществлены банковские операции;

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 банковских операций.

Кредитные организации могут применить иные ограничения по параметрам банковских операций.

12.3. Кредитные организации при осуществлении банковских операций с использованием сети «Интернет» на основании заявления (уведомления) клиента, переданного способом, определенным договором кредитной организации с клиентом, обеспечивают:

установление ограничения по параметрам банковских операций, которые могут осуществляться клиентом;

возможность оперативной блокировки доступа клиента с целью осуществления банковской операции.

13. Кредитные организации обеспечивают регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной в абзацах втором, третьем, четвертом пункта 4 настоящего Положения, в том числе содержащейся в электронных сообщениях, на следующих этапах осуществления банковских операций:

формирование (подготовка) защищаемой информации, в том числе содержащейся в электронных сообщениях;

передача защищаемой информации, в том числе содержащейся в электронных сообщениях;

идентификация, аутентификация и авторизация клиентов при осуществлении банковских операций;

получение подтверждения клиента об исполнении первичных документов на осуществление банковских операций;

уведомление клиента об осуществленных банковских операциях;

обработка защищаемой информации, в том числе содержащейся в электронных сообщениях;

хранение электронных сообщений.

13.1 Технология безопасной обработки защищаемой информации, применяемая на всех этапах осуществления банковских операций, указанных в настоящем пункте, должна обеспечивать защиту защищаемой информации,

в том числе содержащейся в электронных сообщениях, от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе:

формирование уникального идентификатора, присваиваемого каждой банковской операции, используемого для ее идентификации, на всех этапах осуществления банковских операций, указанных в настоящем пункте;

реализацию технологических мер по использованию раздельных технологий, указанных в пункте 12 настоящего Положения;

защиту защищаемой информации, в том числе содержащейся в электронных сообщениях, при ее передаче по каналам связи;

аутентификацию входных электронных сообщений;

взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями;

идентификацию, аутентификацию и авторизацию клиента при составлении, удостоверении и передаче электронных сообщений с использованием сети «Интернет»;

сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении банковских операций;

выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании программного обеспечения, и осуществление банковских операций злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации;

восстановление информации, содержащейся в первичных документах на осуществление банковских операций в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.

13.2 Кредитные организации обеспечивают регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой

информации, в том числе содержащейся в электронных сообщениях, на всех этапах осуществления банковских операций, указанных в настоящем пункте, в том числе регистрацию действий своих работников, а также регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения.

Регистрации подлежат, в том числе следующие результаты выполнения действий:

дата (день, месяц, год) и время (часы, минуты, секунды) осуществления банковской операции;

уникальный идентификатор банковской операции;

код, соответствующий этапу осуществления банковской операции;

результат осуществления действия.

13.2.1. Регистрации подлежат, в том числе следующие данные о действиях работников, выполняемых с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) осуществления работником банковской операции;

набор символов, присвоенный работнику и позволяющий идентифицировать его в автоматизированной системе, программном обеспечении;

уникальный идентификатор банковской операции;

код, соответствующий этапу осуществления банковской операции;

результат осуществления работником банковской операции (успешная или неуспешная);

идентификационная информация объекта информационной инфраструктуры, в отношении которого выполнена банковская операция, в том числе используемая для адресации устройства, с использованием которого осуществлен доступ.

13.2.2. Регистрации подлежат, в том числе следующие данные о действиях клиентов, выполняемых с использованием автоматизированных

систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) осуществления клиентом банковской операции;

набор символов, присвоенный клиенту и позволяющий идентифицировать его в автоматизированной системе, программном обеспечении;

уникальный идентификатор банковской операции;

код, соответствующий этапу осуществления банковской операции;

результат осуществления клиентом банковской операции (успешная или неуспешная);

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций, которой в зависимости от технической возможности является IP-адрес, MAC-адрес, номер SIM-карты, номер телефона и (или) иной идентификатор устройства.

13.3 Кредитные организации обеспечивают регистрацию инцидентов, связанных с нарушениями требований к защите информации при осуществлении банковской деятельности, в том числе событий, которые привели или могут привести к осуществлению банковских операций без согласия клиента, неоказанию услуг по осуществлению банковских операций.

По каждому инциденту, указанному в настоящем подпункте, кредитные организации обеспечивают регистрацию, в том числе:

уникального идентификатора осуществления банковской операции без согласия клиента;

этапа (этапов) осуществления банковской операции, на котором(ых) произошел несанкционированный доступ к защищаемой информации;

результата реагирования на инцидент, связанный с осуществлением банковской операции без согласия клиента, в том числе по возврату

денежных средств или электронных денежных средств.

13.4 Кредитные организации обеспечивают хранение следующей информации:

информация, содержащаяся во входных и выходных электронных сообщениях;

информация, указанная в подпунктах 13.2.1, 13.2.2 подпункта 13.2. настоящего пункта;

информация, указанная в подпункте 13.3 настоящего пункта.

Кредитные организации обеспечивают целостность и доступность указанной в настоящем подпункте информации не менее пяти лет, начиная с даты ее формирования (поступления).

14. Кредитные организации:

обеспечивают формирование подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации (далее – служба информационной безопасности), а также определяют во внутренних документах цели и задачи деятельности этой службы;

предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач.

Кредитные организации осуществляют планирование и контроль обеспечения защиты информации при осуществлении банковской деятельности, наделяя следующими полномочиями службу информационной безопасности:

определять требования к средствам и системам защиты информации и организационным мерам защиты информации при осуществлении банковской деятельности;

осуществлять контроль (мониторинг) обеспечения защиты информации при осуществлении банковской деятельности;

контролировать выполнение работниками требований к защите

информации при осуществлении банковской деятельности;

контролировать организацию работ по защите информации в автоматизированных системах при осуществлении банковской деятельности;

участвовать в разбирательствах инцидентов, связанных с нарушениями требований к защите информации при осуществлении банковской деятельности, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;

участвовать в действиях, связанных с восстановлением предоставления услуг автоматизированных систем после сбоев и (или) отказов в работе объектов информационной инфраструктуры.

15. Кредитные организации обеспечивают доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления, 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 осуществлялась банковская операция;

рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется банковская операция, и своевременному обнаружению воздействия вредоносного кода.

16. Кредитные организации к инцидентам, связанным с нарушениями требований к защите информации при осуществлении банковской деятельности, должны относить события, которые привели или могут привести к осуществлению банковских операций без согласия клиента, неоказанию услуг по осуществлению банковских операций, в том числе включенные в перечень инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения

и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и размещаемый Банком России на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – перечень инцидентов).

Кредитные организации осуществляют информирование Банка России:

о выявленных инцидентах, связанных с нарушением требований к защите информации при осуществлении банковской деятельности, в том числе включенных в перечень инцидентов;

о планируемых мероприятиях по раскрытию информации об инцидентах, связанных с нарушением требований к защите информации при осуществлении банковской деятельности, 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 предоставления кредитной организацией в Банк России сведений, указанных в абзацах третьем и четвертом настоящего пункта. Информация о форме и сроке предоставления указанных сведений подлежит согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации согласно части 6 статьи 5 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), и размещается на официальном сайте Банка России в сети «Интернет».

17. Кредитные организации обеспечивают проведение оценки соответствия уровню защиты информации, установленному в пункте 5 настоящего Положения (далее – оценка соответствия защиты информации) не реже одного раза в два года. Оценка соответствия защиты информации

осуществляется с привлечением сторонних организаций, имеющих лицензию 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 (далее – проверяющая организация).

17.1. Оценка соответствия защиты информации осуществляется в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Росстандарта от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2–2018).

17.2. По результатам оценки соответствия защиты информации проверяющая организация готовит отчет, оформляемый в соответствии с разделом 8 ГОСТ Р 57580.2–2018.

Кредитные организации обеспечивают хранение отчета по результатам оценки соответствия защиты информации не менее пяти лет, начиная с даты его выдачи проверяющей организацией.

18. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от __ _____ 201_ года № __) вступает в силу с «____» _____года, за исключением пункта 5, пункта 6, пункта 12, подпунктов 17.1, 17.2 пункта 17 настоящего Положения.

Пункт 6, пункт 12 настоящего Положения вступают в силу с 1 января 2020 года.

Пункт 5, подпункты 17.1, 17.2 пункта 17 настоящего Положения вступают в силу с 1 января 2021 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