Зарегистрировано в Минюсте России 16 мая 2019 г. N 54634

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

17 апреля 2019 г. N 684-П

ПОЛОЖЕНИЕ ОБ УСТАНОВЛЕНИИ ОБЯЗАТЕЛЬНЫХ ДЛЯ НЕКРЕДИТНЫХ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ФИНАНСОВЫХ РЫНКОВ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ НЕЗАКОННЫХ ФИНАНСОВЫХ ОПЕРАЦИЙ

На основании статьи 76.4-1 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" (Собрание законодательства Российской Федерации, 2002, N 28, ст. 2790; 2003, N 2, ст. 157; N 52, ст. 5032; 2004, N 27, ст. 2711; N 31, ст. 3233; 2005, N 25, ст. 2426; N 30, ст. 3101; 2006, N 19, ст. 2061; N 25, ст. 2648; 2007, N 1, ст. 9, ст. 10; N 10, ст. 1151; N 18, ст. 2117; 2008, N 42, ст. 4696, ст. 4699; N 44, ст. 4982; N 52, ст. 6229, ст. 6231; 2009, N 1, ст. 25; N 29, ст. 3629; N 48, ст. 5731; 2010, N 45, ст. 5756; 2011, N 7, ст. 907; N 27, ст. 3873; N 43, ст. 5973; N 48, ст. 6728; 2012, N 50, ст. 6954; N 53, ст. 7591, ст. 7607; 2013, N 11, ст. 1076; N 14, ст. 1649; N 19, ст. 2329; N 27, ст. 3438, ст. 3476, ст. 3477; N 30, ст. 4084; N 49, ст. 6336; N 51, ст. 6695, ст. 6699; N 52, ст. 6975; 2014, N 19, ст. 2311, ст. 2317; N 27, ст. 3634; N 30, ст. 4219; N 40, ст. 5318; N 45, ст. 6154; N 52, ст. 7543; 2015, N 1, ст. 4, ст. 37; N 27, ст. 3958, ст. 4001; N 29, ст. 4348, ст. 4357; N 41, ст. 5639; N 48, ст. 6699; 2016, N 1, ст. 23, ст. 46, ст. 50; N 26, ст. 3891; N 27, ст. 4225, ст. 4273, ст. 4295; 2017, N 1, ст. 46; N 14, ст. 1997; N 18, ст. 2661, ст. 2669; N 27, ст. 3950; N 30, ст. 4456; N 31, ст. 4830; N 50, ст. 7562; 2018, N 1, ст. 66; N 9, ст. 1286; N 11, ст. 1584, ст. 1588; N 18, ст. 2557; N 24, ст. 3400; N 27, ст. 3950; N 31, ст. 4852; N 32, ст. 5115; N 49, ст. 7524; N 53, ст. 8411, ст. 8440) настоящее Положение устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью 1 статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", в целях противодействия осуществлению незаконных финансовых операций.

1. В целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью 1 статьи 76.1 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", некредитные финансовые организации, осуществляющие финансовые операции (далее - некредитные финансовые организации), должны осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых некредитными финансовыми организациями (далее соответственно - автоматизированные системы, защищаемая информация, защита информации):

информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками некредитных финансовых организаций и (или) клиентами некредитных финансовых организаций (далее - электронные сообщения);

информации, необходимой некредитным финансовым организациям для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

информации об осуществленных некредитными финансовыми организациями и их клиентами финансовых операциях;

ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемой некредитными финансовыми организациями и их клиентами при осуществлении финансовых операций (далее - криптографические ключи).

В случае если защищаемая информация содержит персональные данные, некредитные финансовые организации должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2009, N 48, ст. 5716; N 52, ст. 6439; 2010, N 27, ст. 3407; N 31, ст. 4173, ст. 4196; N 49, ст. 6409; 2011, N 23, ст. 3263; N 31, ст. 4701; 2013, N 14, ст. 1651; N 30, ст. 4038; N 51, ст. 6683; 2014, N 23, ст. 2927; N 30, ст. 4217, ст. 4243; 2016, N 27, ст. 4164; 2017, N 9, ст. 1276; N 27, ст. 3945; N 31, ст. 4772; 2018, N 1, ст. 82) (далее - Федеральный закон "О персональных данных").

2. Некредитные финансовые организации должны обеспечивать доведение до своих клиентов рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код), в целях противодействия незаконным финансовым операциям.

Некредитные финансовые организации должны обеспечивать доведение до своих клиентов следующей информации:

о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

3. Обеспечение защиты информации с помощью СКЗИ некредитные финансовые организации должны осуществлять в соответствии с технической документацией на СКЗИ, а также следующими федеральными законами и нормативными правовыми актами Российской Федерации:

Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи" (Собрание законодательства Российской Федерации, 2011, N 15, ст. 2036; N 27, ст. 3880; 2012, N 29, ст. 3988; 2013, N 14, ст. 1668; N 27, ст. 3463, ст. 3477; 2014, N 11, ст. 1098; N 26, ст. 3390; 2016, N 1, ст. 65; N 26, ст. 3889) (далее - Федеральный закон "Об электронной подписи");

Федеральным законом "О персональных данных";

постановлением Правительства Российской Федерации от 1 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257);

приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года N 6382, 25 мая 2010 года N 17350 (далее - Положение ПКЗ-2005);

приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года N 378 "Об утверждении состава и содержания 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 N 33620.

4. В случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований указанная оценка должна проводиться в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

В случае если некредитная финансовая организация применяет СКЗИ российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

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

> КонсультантПлюс: примечание.
> П. 5 вступает в силу с 01.01.2021.

5. Защита информации в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых осуществляется некредитными финансовыми организациями (далее при совместном упоминании - объекты информационной инфраструктуры), должна осуществляться некредитной финансовой организацией в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года N 822-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2017) (далее - ГОСТ Р 57580.1-2017). Требования ГОСТ Р 57580.1-2017 должны применяться по результатам определения некредитной финансовой организацией применимого к ней в течение календарного года уровня защиты информации, предусмотренного ГОСТ Р 57580.1-2017 (далее соответственно - уровень защиты информации, определение уровня защиты информации), с соблюдением следующих требований.

5.1. Определение уровня защиты информации должно осуществляться некредитной финансовой организацией ежегодно не позднее первого рабочего дня календарного года определения уровня защиты информации (далее - дата определения уровня защиты информации).

5.2. Требования ГОСТ Р 57580.1-2017, соответствующие усиленному уровню защиты информации, должны соблюдать центральные контрагенты, центральный депозитарий (далее - некредитные финансовые организации, реализующие усиленный уровень защиты информации).

5.3. Требования ГОСТ Р 57580.1-2017, соответствующие стандартному уровню защиты информации, должны соблюдать следующие некредитные финансовые организации (далее - некредитные финансовые организации, реализующие стандартный уровень защиты информации):

специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;

клиринговые организации;

организаторы торговли;

страховые организации, стоимость активов которых в течение последних шести календарных месяцев подряд по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, превышала 20 миллиардов рублей;

негосударственные пенсионные фонды, осуществляющие деятельность по обязательному пенсионному страхованию;

негосударственные пенсионные фонды, осуществляющие деятельность по негосударственному пенсионному обеспечению, размер средств пенсионных резервов которых в течение последних шести календарных месяцев подряд по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, превышал 10 миллиардов рублей;

репозитарии;

брокеры, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключили сделки купли-продажи ценных бумаг за счет своих клиентов при осуществлении брокерской деятельности в объеме более 100 000 миллионов рублей в квартал и (или) которые в течение трех последних кварталов по состоянию 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли брокерское обслуживание более чем 100 000 лиц;

дилеры, которые в течение последних трех кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключали за свой счет на организованных торгах сделки купли-продажи ценных бумаг в объеме более 200 000 миллионов рублей в квартал;

депозитарии (в том числе расчетные депозитарии), осуществившие в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, учет ценных бумаг на счетах, предусмотренных пунктом 2.1 и абзацами вторым - пятым пункта 2.2 Положения Банка России от 13 ноября 2015 года N 503-П "О порядке открытия и ведения депозитариями счетов депо и иных счетов", зарегистрированного Министерством юстиции Российской Федерации 16 декабря 2015 года N 40137, открытых в депозитарии, стоимость которых превышала 500 000 миллионов рублей;

регистраторы, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, открыли лицевые счета в реестрах владельцев эмиссионных ценных бумаг, инвестиционных паев паевых инвестиционных фондов, ипотечных сертификатов участия более чем 1 000 000 лиц;

управляющие, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, заключали сделки купли-продажи ценных бумаг при осуществлении деятельности по управлению ценными бумагами в объеме более 20 000 миллионов рублей в квартал и (или) которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли доверительное управление ценными бумагами и денежными средствами более чем 2 000 лиц, с которыми заключены договоры доверительного управления.

5.4. Некредитные финансовые организации, реализующие усиленный уровень защиты

информации, и некредитные финансовые организации, реализующие стандартный уровень защиты информации (далее при совместном упоминании - некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации), должны осуществлять тестирование объектов информационной инфраструктуры на предмет проникновений и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

КонсультантПлюс: примечание.
П. 6 вступает в силу с 01.01.2021.

6. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать проведение оценки соответствия определенного ими уровня защиты информации требованиям, предусмотренным пунктом 5 настоящего Положения (далее - оценка определенного уровня защиты информации), с соблюдением следующих требований.

6.1. Оценка определенного уровня защиты информации должна осуществляться 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 от 3 февраля 2012 года N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) (далее - проверяющая организация).

6.2. Оценка определенного уровня защиты информации должна осуществляться в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года N 156-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2018) (далее - ГОСТ Р 57580.2-2018).

6.3. Оценка определенного уровня защиты информации должна осуществляться некредитными финансовыми организациями, реализующими усиленный уровень защиты информации, не реже одного раза в год, некредитными финансовыми организациями, реализующими стандартный уровень защиты информации, - не реже одного раза в три года.

7. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать хранение отчета, составленного проверяющей организацией по результатам оценки определенного уровня защиты информации, в течение не менее чем пяти лет с даты его выдачи проверяющей организацией.

КонсультантПлюс: примечание.
Абз. 1 п. 8 вступает в силу с 01.01.2022 и действует до 30.06.2023 включительно.

8. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить уровень соответствия не ниже третьего уровня соответствия, предусмотренного подпунктом "г" пункта 6.9 ГОСТ Р 57580.2-2018.

КонсультантПлюс: примечание.

Абз. 2 п. 8 вступает в силу с 01.07.2023.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить уровень соответствия не ниже четвертого уровня соответствия, предусмотренного подпунктом "д" пункта 6.9 ГОСТ Р 57580.2-2018.

КонсультантПлюс: примечание.
П. 9 вступает в силу с 01.01.2020.

9. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, в том числе на наличие уязвимостей или недекларированных возможностей (далее - сертификация), или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4, предусмотренного пунктом 7.6 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "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 N 1340-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2014) (далее - анализ уязвимостей).

Некредитные финансовые организации, не указанные в абзаце первом настоящего пункта, должны самостоятельно определять необходимость сертификации или анализа уязвимостей.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего подпункта, некредитные финансовые организации должны самостоятельно определять необходимость сертификации или анализа уязвимостей.

По решению некредитной финансовой организации анализ уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

10. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должно осуществляться в соответствии со статьей 6 Федерального закона "Об электронной подписи".

11. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной в абзацах втором - четвертом пункта 1 настоящего Положения, в рамках идентификации, аутентификации и авторизации своих клиентов при совершении действий в целях осуществления финансовых

операций, формировании (подготовке), передаче и приеме электронных сообщений, удостоверении права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом, осуществлении финансовой операции, учете результатов ее осуществления, хранении электронных сообщений и информации об осуществленных финансовых операциях (далее при совместном упоминании - технологические участки) на основе анализа рисков с соблюдением следующих требований.

11.1. Технология обработки защищаемой информации, применяемая на всех технологических участках, должна обеспечивать целостность и неизменность защищаемой информации.

11.2. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений, должна обеспечивать следующие мероприятия:

проверку правильности формирования (подготовки) электронных сообщений (двойной контроль);

проверку правильности заполнения полей электронного сообщения и прав владельца электронной подписи (входной контроль);

контроль дублирования электронного сообщения;

структурный контроль электронных сообщений;

защиту защищаемой информации при ее передаче по каналам связи.

11.3. Технология обработки защищаемой информации, применяемая при удостоверении права клиентов некредитных финансовых организаций распоряжаться денежными средствами, ценными бумагами или иным имуществом, должна обеспечивать выполнение следующих мероприятий:

получение электронных сообщений клиента, подписанных клиентом способом, указанным в пункте 10 настоящего Положения;

получение от клиента подтверждения совершенной финансовой операции.

11.4. Технология обработки защищаемой информации, применяемая при осуществлении финансовой операции, учете результатов ее осуществления (при наличии учета), должна обеспечивать выполнение следующих мероприятий:

проверку соответствия (сверку) выходных электронных сообщений соответствующим входным электронным сообщениям;

проверку соответствия (сверку) результатов осуществления финансовых операций информации, содержащейся в электронных сообщениях;

направление клиентам некредитных финансовых организаций уведомлений об осуществлении финансовых операций в случае, когда такое уведомление предусмотрено законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций, или договором.

12. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех технологических участках, включая регистрацию действий своих работников и клиентов, выполняемых с

использованием автоматизированных систем, программного обеспечения, с соблюдением следующих требований.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны регистрировать следующую информацию о действиях своих работников и клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

дату (день, месяц, год) и время (часы, минуты, секунды) осуществления финансовой операции, а для клиентов - совершение действий в целях осуществления финансовой операции;

присвоенный работнику (клиенту) идентификатор, позволяющий идентифицировать работника (клиента) в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат осуществления финансовой операции - для работника, совершение действий в целях осуществления финансовой операции - для клиента;

идентификационную информацию, используемую для идентификации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций: для работников (клиентов) - сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) работника (клиента); для клиентов - международный идентификатор абонента-клиента (индивидуальный номер абонента клиента - физического лица), международный идентификатор пользовательского оборудования (оконечного оборудования) клиента - физического лица, номер телефона и (или) иной идентификатор устройства клиента.

13. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны осуществлять регистрацию инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков (далее - инциденты защиты информации), а также представлять сведения о выявленных инцидентах защиты информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками, при наличии указанного должностного лица (отдельного структурного подразделения) в соответствии с внутренними документами указанных некредитных финансовых организаций при соблюдении следующих требований.

13.1. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, к инцидентам защиты информации должны относить события, которые привели или могут по оценке указанных некредитных финансовых организаций привести к осуществлению финансовых операций без согласия клиента некредитной финансовой организации, неоказанию услуг, связанных с осуществлением финансовых операций, в том числе события, включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в сети "Интернет" (далее - перечень типов инцидентов).

13.2. По каждому инциденту защиты информации некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны осуществлять регистрацию следующей информации:

защищаемой информации на технологических участках, на которых произошел несанкционированный доступ к защищаемой информации;

результата реагирования на инцидент защиты информации, в том числе совершенных действий по возврату денежных средств, ценных бумаг и иного имущества клиента некредитной

финансовой организации.

14. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать:

хранение информации, указанной в абзацах втором и четвертом пункта 1 настоящего Положения, информации о регистрации данных, указанных в пункте 12 настоящего Положения, и информации об инцидентах защиты информации;

целостность и доступность информации, указанной в абзаце первом настоящего пункта, в течение не менее чем пяти лет с даты ее формирования некредитной финансовой организацией (даты поступления в некредитную финансовую организацию), а в случае если законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций, установлен иной срок - на срок, установленный законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций.

15. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны информировать Банк России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов;

о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети "Интернет", в отношении инцидентов защиты информации не позднее одного рабочего дня до дня проведения мероприятия.

16. В случае если некредитная финансовая организация, не относящаяся к некредитным финансовым организациям, реализующим усиленный и стандартный уровни защиты информации, выявила соответствие требованиям, указанным в подпункте 5.3 пункта 5 настоящего Положения, такая некредитная финансовая организация должна обеспечить соответствие требованиям, указанным в подпунктах 5.3 и 5.4 пункта 5 и пунктах 6 - 15 настоящего Положения, в срок не позднее девяти месяцев со дня выявления соответствия требованиям, указанным в подпункте 5.3 пункта 5 настоящего Положения.

17. В случае совмещения некредитной финансовой организацией видов деятельности в сфере финансовых рынков, осуществление которых обусловливает необходимость реализации одновременно двух уровней защиты информации, такая некредитная финансовая организация должна обеспечить соблюдение требований, предъявляемых к более высокому уровню защиты информации, при условии, что при совмещении деятельности она использует единые объекты информационной инфраструктуры.

18. Настоящее Положение не распространяется на отношения, регулируемые Федеральным законом от 26 июля 2017 года N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736).

19. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 21 декабря 2018 года N 39) вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Пункт 9 настоящего Положения вступает в силу с 1 января 2020 года.

Пункты 5 и 6 настоящего Положения вступают в силу с 1 января 2021 года.

Абзац первый пункта 8 настоящего Положения вступает в силу с 1 января 2022 года и

действует по 30 июня 2023 года включительно.

Абзац второй пункта 8 настоящего Положения вступает в силу с 1 июля 2023 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