Предложения участников финансового рынка
по устранению устаревших и избыточных регуляторных требований в нормативных актах по вопросам,
относящимся к компетенции Банка России
Подгруппа 14 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

№	Ссылка на пункт нормативного акта*	Суть устаревшей/избыточной нормы	Краткое обоснование для устранения устаревших требований
14-1	**Приказ ФСФР России от 08.12.2005 № 05-77/пз-н** "Об утверждении Положения о требованиях к осуществлению деятельности участников финансовых рынков при использовании электронных документов"	Не соответствует действующему законодательству, т.к. предъявляет требования к сертифицированным средствам электронной подписи, что формально лишает участника финансового рынка применять современные средства коммуникации с клиентами.	Устаревший нормативный акт. В соответствии с п. 2 участники финансового рынка при взаимодействии между собой и со своими клиентами с использованием электронных документов должны применять только сертифицированные средства электронной подписи. Указанное требование значительно ограничивает возможность использовать современные средства коммуникации в отношениях профессиональных участников и управляющих компаний с клиентами (подтверждение отправки сообщения вводом кодов доступа со специальной индивидуальной карты, SMS-подтверждения, использования мобильных приложений и др.). С учетом утверждения Банком России 17.04.2019 Положения № 684-П перестает нести какую-либо защитную функцию в сфере обмена информацией между участником рынка и клиентом. В соответствии с разъяснением Службы Банка России по финансовым рынкам от 16.09.2013 г. № 13-ОП-10/1143, регулятор подтверждал НАУФОР целесообразность прекратить действие Приказа ФСФР России от 08.12.2005 № 05-77/пз-н в связи с неактуальностью и противоречием действующему законодательству.
		Должны применяться только сертифицированные средства	Делает невозможным использованием простой электронной подписи (кодов из смс, паролей,

* *действующий нормативный документ ФКЦБ, ФСФР, ЦБ РФ.*

		электронной подписи при обмене электронными документами с проф.участниками.	иное), в то время как ФЗ «Об электронной подписи» не ограничивает в праве выбора любой технологии и вида ЭП
	Пункт 2, Пункт 6	Необходимость предварительного уведомления федерального органа исполнительной власти по рынку ценных бумаг о начале использования ими электронных документов. Настоящее Положение определяет порядок использования документов, в которых информация представлена в электронно-цифровой форме с электронной подписью.	Полностью устарел
14-2	**Положение Банка России от 17.04.2019 №684-П** «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия	Распространение стандартных требований практически на все некредитные финансовые организации.	Учитывая, что затраты на реализацию мероприятий в соответствии с требованиями Положения 684-П в ряде случаев превышают риски, которые принимает на себя некредитная финансовая организация[1], предлагается установить для некредитных финансовых организаций (профессиональных участников рынка ценных бумаг и специализированных депозитариев) минимальные требования к уровню защиты информации. Стандартный уровень защиты информации, по нашему мнению, необходимо применять в отношении некредитной финансовой организации,

[1] ПАРТАД совместно с СРО НФА в период с 07 по 17 июня 2019 года был проведен опрос своих членов на предмет определения возможных последствий применения Положения №684-П, в котором приняло участие 23 организации. При этом более половины участников опроса (15 организаций) высказали мнение о том, что предполагаемые затраты на защиту информации, предусмотренные требованиями данного нормативного акта, существенно превосходят реальный уровень рисков в их деятельности.

	осуществлению незаконных финансовых операций»		только, если она входит в группу компаний с участием кредитной организации, в рамках которой используются единые объекты информационной инфраструктуры. Вместе с тем, некредитная финансовая организация может по своему усмотрению определить для себя соответствие требованиям по стандартному уровню защиты информации с учетом принятой политики управления рисками.
14-3	**Положение Банка России №684-П «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» от 17 апреля 2019 г.**	В соответствии с Положением к ломбардам предъявляются требования об обеспечении стандартного уровня защиты информации, установленного ГОСТ Р 57580.1-2017. Требования ГОСТ необходимо реализовать до 01.01.2021 года, при этом к ломбардам применимо 96 требований, которые реализуются с помощью технических мер, и 108 требований, которые можно реализовать как технически, так и организационно.	Выдержать исполнение указанных требований смогут только самые крупные сетевые ломбарды, что касается мелких и средних участников рынка, то для них это будет не просто затруднительным, а невозможным. На примере данного Положения можно увидеть, что нормативное регулирование не соответствует текущим реалиям ломбардного рынка, абсолютно не учитывает интересы его участников, не оценивает последствия регуляторного воздействия принимаемых нормативных актов на различные сектора ломбардного рынка. На наш взгляд, необходимо снизить уровень требований к ломбардам в отношении информационной безопасности до минимального.
14-4	Целиком **Приказ ФСФР России от 08.12.2005 N 05-77/пз-н** "Об утверждении Положения о требованиях к осуществлению деятельности участников финансовых рынков при использовании	1) Устарел по части формулировок, терминов; 2) Избыточно требование об уведомлении о начале использования ими электронных документов.	1) Требуется терминологическая актуализация; 2) В условиях развития информационных технологий такое уведомление нецелесообразно.

	электронных документов"		
14-5	**Положение Банка России от 09.06.2012 N 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»	Отменить или актуализировать регулирование, предусмотренное абзацем 2 подпункта 2.5.5.1 Положения № 382-П: «Оператору по переводу денежных средств, оператору услуг платежной инфраструктуры на стадиях создания и эксплуатации объектов информационной инфраструктуры необходимо обеспечить: 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	Положение Банка России от 09.06.2012 N 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» в части сертификации автоматизированных систем и приложений в системе сертификации ФСТЭК России не может быть выполнено. В соответствии с Информационным сообщением ФСТЭК России от 29.03.2019 № 240/24/1525 ФСТЭК России более не осуществляет сертификацию на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей.

		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)	
14-6	**Методические рекомендации** по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (**утв. Банком России 14.02.2019 N 4-МР**)	Отменить или актуализировать регулирование, предусмотренное абзацем 9 пп. 2.3.8.1 Методических рекомендаций: «2.3.8.1. В случае функционирования объектов информационной инфраструктуры с использованием собственного решения для выполнения действий, указанных в подпункте 2.3.7 настоящего пункта, рекомендуется обеспечить: … использованием прикладного программного обеспечения, применяемого в доверенной среде, прошедшего проверку на отсутствие недекларированных возможностей и соответствующего 4-му уровню контроля отсутствия	Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утв. Банком России 14.02.2019 №4-МР) в части сертификации автоматизированных систем и приложений в системе сертификации ФСТЭК России не может быть выполнено. В соответствии с Информационным сообщением ФСТЭК России от 29.03.2019 № 240/24/1525 ФСТЭК России более не осуществляет сертификацию на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей.

		недекларированных возможностей согласно Руководящему документу "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей", утвержденному приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. №114, или сертифицированного в системе сертификации ФСТЭК России 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 (ОУД) 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 Росстандарта от 8 ноября 2013 года №1340-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2014)	
14-7	**Положение Банка России от 17.04.2019 N 683-П** «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»	Отменить или актуализировать регулирование, предусмотренное п. 4.1 Положения № 683-П: «4.1. Кредитные организации должны обеспечить использование для осуществления банковских операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема 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	"Положение Банка России от 17.04.2019 №683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» в части сертификации автоматизированных систем и приложений в системе сертификации ФСТЭК России не может быть выполнено. В соответствии с Информационным сообщением ФСТЭК России от 29.03.2019 № 240/24/1525 ФСТЭК России более не осуществляет сертификацию на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей.

		экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями 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 №1340-ст "Об утверждении национального стандарта" (М., ФГУП "Стандартинформ", 2014). В отношении прикладного программного обеспечения автоматизированных систем и приложений, не указанных в абзаце первом настоящего подпункта, кредитные организации должны самостоятельно определять необходимость сертификации или	

		анализа уязвимостей и контроля отсутствия недекларированных возможностей.	
14-8	Абз. 2 п. 2.5.5.1. **Положения Банка России от 09.06.2012 № 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»	Требования по использованию 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	Требование избыточное, т.к. сертификация программного обеспечения не может подтвердить отсутствие уязвимостей (например, уязвимостей нулевого дня).
14-9	п. 4.1. **Положения Банка России 17.04.2019 № 683-П** «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»	Требования по использованию для осуществления банковских операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией клиентам для совершения действий в целях осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений, к исполнению в автоматизированных	Требование избыточное, т.к. сертификация программного обеспечения не может подтвердить отсутствие уязвимостей (например, уязвимостей нулевого дня).

		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, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4	
14-10	п.9 **Положения Банка России от 17.04.2019 № 684-П** «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»	Требование к использованию 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	Требование избыточное, т.к. сертификация программного обеспечения не может подтвердить отсутствие уязвимостей (например, уязвимостей нулевого дня).

		«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, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (ОУД)	
14-11	**Требования к Правилам** защиты информации центрального депозитария, утвержденные **Приказом ФСФР России от 03.07.2012 г**. «Об утверждении требований к некоторым внутренним документам центрального депозитария» **№ 12-53/пз-н.**	Требования к правилам защиты информации центрального депозитария, которые являются внутренним документом центрального депозитария	Требования обязывают утверждать дополнительные документы по защите информации, по сути своей дублирующие уже имеющиеся документы, разрабатываемые для соблюдения 382-П/672-П/683-П/684-П, что усложняет методологическую работу.
14-12	**Стандарт Банка России** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» **СТО БР ИББС-1.0-2014** (принят и введен в действие Распоряжением Банка России от	Признать утратившим силу.	Приведенные Стандарты Банка России носят для кредитных организаций рекомендательный характер, но после присоединения к ним становятся обязательными для исполнения. При этом требования указанных Стандартов Банка России перешли в Стандарт Банка России ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» являющийся обязательным для всех кредитных организаций.

	17.05.2014 № Р-399); **Стандарт Банка России** «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014» **СТО БР ИББС-1.2-2014** (принят и введен в действие Распоряжением Банка России от 17.05.2014 № Р-399)		Вместе с тем, кредитные организации, ранее присоединившиеся к указанным Стандартам Банка России, обязаны на периодической основе отчитываться перед Банком России о проведенных мероприятиях внешнего аудита, самооценки, что не является целесообразным по причине трудозатратности и снижения операционной и финансовой эффективности кредитной организации. Учитывая издание обязательного Стандарта Банка России ГОСТ Р 57580.1-2017, содержащего требования для всех кредитных организаций, предлагаем отменить указанные Стандарты Банка России.
14-13	**Положение Банка России от 09.06.2012 № 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»	Актуализировать норму абзаца 2 подпункта 2.5.5.1 пункта 2.5 Положения № 382-П в части использования кредитными организациями 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	В соответствии с информационным сообщением ФСТЭК России от 29.03.2019 № 240/24/1525 в связи с утверждением Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (далее – Требования к уровням доверия), с 1 июня 2019 года ФСТЭК России не принимаются к рассмотрению заявки на сертификацию средств защиты информации на соответствие требованиям руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных

		по анализу уязвимостей и контролю отсутствия недекларированных возможностей.	возможностей». Учитывая изложенное, ФСТЭК России указала, что разработчикам и производителям сертифицированных средств защиты информации рекомендуется с привлечением испытательных лабораторий провести оценку соответствия средств защиты информации Требованиям к уровням доверия и представить результаты в ФСТЭК России для переоформления соответствующих сертификатов соответствия. В этой связи норма абзаца 2 подпункта 2.5.5.1 пункта 2.5 Положения № 382-П устарела, не может быть фактически выполнена и нуждается в доработке в соответствии с последними изменениями в актах ФСТЭК России.
14-14	**Положение Банка России от 17.04.2019 № 683-П** «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»	Актуализировать норму подпункта 4.1 пункта 4 Положения № 683-П в части использования кредитными организациями прикладного программного обеспечения автоматизированных систем и приложений, сертифицированного в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей.	В соответствии с информационным сообщением ФСТЭК России от 29.03.2019 № 240/24/1525 в связи с утверждением Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (далее – Требования к уровням доверия), с 1 июня 2019 года ФСТЭК России не принимаются к рассмотрению заявки на сертификацию средств защиты информации на соответствие требованиям руководящего документа «Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Учитывая изложенное, ФСТЭК России указала, что разработчикам и производителям сертифицированных средств защиты информации рекомендуется с привлечением испытательных

			лабораторий провести оценку соответствия средств защиты информации Требованиям к уровням доверия и представить результаты в ФСТЭК России для переоформления соответствующих сертификатов соответствия. В этой связи норма подпункта 4.1 пункта 4 Положения № 683-П устарела, не может быть фактически выполнена и нуждается в доработке в соответствии с последними изменениями в актах ФСТЭК России.
14-15	**ст.27, ч.7 Федерального закона от № 161-ФЗ «О национальной платежной системе»**	Установлено, что банками направляется информация обо всех случаях или попытках осуществления переводов денежных средств без согласия клиентов через АСОИ ФинЦерт. Однако при этом обязаны отправлять ежеквартально две отчетности: 1. **Отчетность по форме 0409258** «Сведения о несанкционированных операциях, совершенных с использованием платежных карт» **2. Отчетность по форме 0403203** «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств»	Поскольку данные из указанных отчетностей уже имеются в Банке России (АСОИ ФинЦерт), то **отчетность могла бы формироваться автоматически на стороне Банка России.**
14-16	**ч. 7. ст. 27 Федерального закона от № 161-ФЗ** «О национальной платежной системе»	Установлено, что признаками совершения операций без согласия клиента, установленными Банком России, банки должны приостанавливать и связываться с	На практике видно, что большое количество переводов на эти реквизиты являются легитимными, но при этом у банка нет возможности, не нарушая законодательство, одобрять эти операции без связи с клиентом.

		клиентом по каждой операции, которая выполняется на реквизит из списка сомнительных реквизитов. Банками направляется информация обо всех случаях или попытках осуществления переводов денежных средств без согласия клиентов через АСОИ ФинЦерт. Однако при этом обязаны отправлять ежеквартально две отчетности: • Отчетность по форме 0409258 «Сведения о несанкционированных операциях, совершенных с использованием платежных карт» • Отчетность по форме 0403203 «Сведения о выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств» Поскольку данные из указанных отчетностей уже имеются в Банке России (АСОИ ФинЦерт), то отчетность могла бы формироваться автоматически на стороне Банка России.	**Механизма предоставления обратной связи в АСОИ ФинЦерт так же не предусмотрено**. Это вызывает негативный отклик со стороны клиентов.
14-17	Пункты 1.4, 1.5, 1.10, 1.13 **Указания Банка России от 08.10.2018 № 4926-У**	Указание № 4926-У содержит требования по предоставлению следующих типов уведомлений:	Данные нормы не соответствуют предоставленным АСОИ ФИНЦЕРТ средствам автоматизации, которые содержат одну единую форму для

	«О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»	первичное, промежуточное, окончательное)	направления информации.