**Комментарии на вопросы (предложения) кредитных организаций (КО), поступившие в рамках предстоящей встречи руководителей КО с руководством Банка России по вопросам «Регулирования Банком России деятельности коммерческих банков» в адрес заместителя Председателя Банка России Г.А. Зубарева**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вопрос (предложения) КО** | **Комментарии** |
| ***Темы и вопросы по направлению информационная безопасность и противодействие мошенничеству*** | | |
| 1 | В период пандемии кредитные организации перенесли значительное число операций в цифровые каналы, что неизбежно повысило не только зависимость от технологий, но и значимость безопасности данных для банковского бизнеса. Каковы планы регулятора в области обеспечения качества технологий для банков и их защиты от внешних и внутренних угроз? В частности, какова позиция Банка России относительно использования кредитными организациями облачной инфраструктуры? Планируется ли нормативная регламентация требований к обеспечению информационной безопасности в облачной инфраструктуре? | Если рассматривать вопрос об использовании сторонней облачной инфраструктуры, то в целом позиция Банка России отражена в Стандарте Банка России СТО БР ИББС-1.4-2018 «Обеспечение информационной безопасности банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге».  В настоящий момент в рамках работ по риск-профилированию проводится сбор информации о зависимости кредитных организаций от поставщиков облачной инфраструктуры.  В рамках полномочий Банка России по установлению требований по операционной надежности планируется дополнительно установить требования к обеспечению информационной безопасности при использовании облачной инфраструктуры. |
| 2 | Что планирует предпринимать Банк России для нормализации обстановки в области кибермошенничества? Поддерживает ли регулятор инициативы по усилению уголовной ответственности за преступления в сфере информационно-коммуникационных технологий, в том числе в части хищения сведений, составляющих банковскую тайну, и телефонного мошенничества? | Банк России поддерживает инициативы по внесению изменений в Уголовный кодекс Российской Федерации, направленных на усиление ответственности за разглашение сведений, составляющих банковскую тайну. Кроме того, Банк России предлагает рассмотреть возможность выделения из статьи 183 Уголовного кодекса Российской Федерации самостоятельного состава преступлений – незаконное получение и разглашение сведений, составляющих банковскую тайну. Учитывая то, что данное преступное деяние наносит существенный социальный вред, одновременно с выделением данного состава преступления в отдельную норму Уголовного кодекса Российской Федерации предлагаем также рассмотреть возможность увеличения ответственности за данное деяние.  Также сообщаем, что Государственной Думой Федерального Собрания Российской Федерации принят в первом чтении проект федерального закона № 605945-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Гражданский процессуальный кодекс Российской Федерации» (далее – законопроект  № 605945-7). Законопроект № 605945-7 направлен на предоставление Банку России полномочий по обращению в Генеральную прокуратуру Российской Федерации для внесудебной «блокировки сайтов», используемых с нарушением законодательства о финансовом рынке, а также в суд для осуществления «блокировки сайтов», с использованием которых распространяется вредоносное программное обеспечение на финансовом рынке. Создаваемый в рамках законопроекта механизм позволит принимать оперативные меры в отношении мошеннических (фишинговых) сайтов, что снизит риски наступления негативных последствий (в том числе связанных с хищением денежных средств) для клиентов кредитных организаций.  Подготовленная ко второму чтению редакция законопроекта № 605945-7 концептуально поддержана ФСБ России и Генеральной прокуратурой Российской Федерации, Роскомнадзором и Минцифры России.  В настоящее время Банк России совместно с Генеральной прокуратурой Российской Федерации проводит эксперимент по взаимодействию по вопросу ограничения доступа к сайтам (в рамках эксперимента в Генеральную прокуратуру Российской Федерации для принятия мер по ограничению доступа направляется информация о сайтах, на которых выявлены признаки, предусмотренные законопроектом № 605945-7, и которые расположены в иностранных доменных зонах (например, .COM,.ORG и т.д.).  Одновременно сообщаем, что Банк России не возражает против усиления ответственности операторов связи за несоблюдение требований, предъявляемых к использованию персональных данных и обороту идентификационных модулей абонентов в части обязательного заключения договора на оказание услуг связи с конкретным абонентом, и блокирования операторами связи (в том числе по требованию правоохранительных органов) абонентских терминалов сетей подвижной радиотелефонной связи с неподлинными и (или) неуникальными идентификационными номерами мобильного оборудования.  Кроме того, сообщаем, что Государственной Думой Федерального Собрания Российской Федерации принят в первом чтении проект федерального закона № 514780-7 «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и иные законодательные акты Российской Федерации» (в части создания Единой информационной системы проверки сведений об абоненте и пользователях услугами связи абонента) направлен на совершенствование обмена информацией между операторами связи и финансовыми организациями и предусматривает создание Единой информационной системы проверки сведений об абоненте и пользователях услугами связи абонента. Создаваемый в рамках законопроекта механизм позволит осуществлять идентификацию клиентов кредитной организации через вышеуказанную систему, тем самым минимизировав риски совершения несанкционированных операций с денежными средствами граждан. Доступ к данной системе будет предоставлен организациям кредитно-финансовой сферы, Банку России, а также органам исполнительной власти в соответствии с их компетенцией и полномочиями. В настоящее время в Банк России поступили замечания и предложения от заинтересованных лиц (операторы связи, Минцифры России, Ассоциация российских банков, комитетов Государственной думы Российской Федерации и так далее). Банк России в настоящее время рассматривает поступающие предложения, проводит их обсуждения, по результатам которых приступит к подготовке предложений по внесению изменений в действующую редакцию законопроекта в рамках компетенции. |
| 3 | Каковы планы Банка России по участию в деятельности межведомственной рабочей группы Минцифры России по рассмотрению вопросов противодействия мошенничеству, совершаемому с использованием телефонных номеров? Кредитными организациями отмечается необходимость повышения эффективности деятельности этой рабочей группы, активизации взаимодействия с операторами сотовой связи и принятия значимых решений, способных существенно изменить ситуацию с телефонным мошенничеством (в том числе с подменой номеров). Какие иные меры планирует реализовать Банк России в части противодействия мошенничеству с использованием методов социальной инженерии? | В рамках противодействия мобильному мошенничеству по инициативе Банка России совместно с операторами связи, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Роскомнадзором проводится отдельная работа по противодействию мошенничеству, совершаемому посредством подмены телефонного номера. В целях минимизации рисков хищений денежных средств Банк России осуществляет сбор и формирование перечней номеров телефонов, используемых организациями кредитно-финансовой сферы исключительно для входящей связи, то есть только для приема звонков от клиентов организаций. Информация об актуализированных перечнях номеров телефонов ежемесячно (в случае корректировки перечня) направляется Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации операторам связи в целях обеспечения ограничения пропуска входящего трафика на номера телефонов своих абонентов при указании в качестве номера А номеров телефонов, содержащихся в перечне. На основании указанного перечня за 2020 год операторами связи было заблокировано свыше 1,5 млн нелегитимных вызовов.  В конце 2019 года основным трендом атак на организации финансовой сферы стали хищения персональных данных физических и юридических лиц с целью дальнейшего использования их в противоправных целях. Основной пик утечек пришелся на октябрь 2019 года. Резкий рост утечек персональных данных коррелирует с увеличением количества атак, связанных с использованием методов «социальной инженерии», «фишинга».  В рамках взаимодействия с операторами связи за 2020 год Департамент информационной безопасности Банка России направил информацию о 26397 телефонных номерах для их блокировки, что превышает показатель предыдущего года на 86%.  В 2020 году Банк России совместно с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, операторами связи продолжает активную работу в рамках межведомственной рабочей группы по рассмотрению вопросов противодействия мошенничеству, совершаемому с использованием телефонных номеров. |
| 4 | Кредитные организации отмечают несовершенство межбанковского взаимодействия по вопросам информационной безопасности через ФинЦЕРТ[[1]](#footnote-1) Банка России. Каковы планы Банка России по повышению эффективности такого взаимодействия, в том числе АСОИ[[2]](#footnote-2)? Будут ли вноситься изменения в процесс взаимодействия Банка России с коммерческими банками по вопросам информационной безопасности, повышаться степень автоматизации этого взаимодействия? | Да, есть планы по совершенствованию процесса организации взаимодействия, в частности разработка нового проекта стандарта Банка Росси СТО БР ИББС 1.5.  Для улучшения взаимодействия участников с ФинЦЕРТ при развитии АСОИ ФинЦЕРТ предполагается в первую очередь рассмотреть следующие возможности:  - улучшить производительность и интерфейс личного кабинета;  - предусмотреть в АСОИ ФинЦЕРТ оперативное взаимодействие участников информационного обмена в рамках обработки выявленных инцидентов;  - расширить перечень функций АСОИ ФинЦЕРТ, доступных через API.. |
| 5 | Планируется ли изменение требований к построению процесса безопасной разработки программного обеспечения (ПО) с учетом повсеместного использования современных методик разработки ПО (Agile, Scrum, Kanban, DevSecOps и т.д.)? | Да, планируется. Банком России совместно рабочей группой, состоящей из участников кредитно-финансовой сферы, в настоящий момент производится доработка методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций» в части формирования раздела с требованиями к гибкой безопасной разработке и тестированию программного обеспечения. |
| 6 | Будет ли Банк России развивать практику киберучений среди кредитных организаций? | Банк России будет развивать практику киберучений среди кредитных организаций.  В 2020 году была проведена апробация подходов на двух десятках кредитных организаций.  В 2021 году запланировано проведение киберучений с организациями, входящими в состав финансовых объединений, как кредитными, так и некредитными финансовыми организациями. Всего будет задействовано около 200 организаций.  Результаты киберучений будут учитываться Департаментом информационной безопасности при подготовке плана мероприятий в рамках консультативного надзора и/или в рамках контактных проверок. |
| 7 | Планируется ли введение специализированных требований к сотрудникам служб информационной безопасности кредитных организаций или их сертификация со стороны Банка России? | Обеспечение информационной безопасности в кредитно-финансовой сфере требует соответствующих кадровых ресурсов. Особое внимание уделяется системе своевременной и эффективной подготовки квалифицированных кадров, способных обеспечить на должном уровне выполнение требований и стандартов по информационной безопасности. Формирование качественных программ профессиональной подготовки должно основываться на положения профессионального стандарта.  В целях оптимизации организационной среды и совершенствования кадрового обеспечения в области информационной безопасности Банком России при участии ряда финансовых организаций и образовательных учреждений разработан проект профессионального стандарта «Специалист по информационной безопасности кредитно-финансовой сферы». Принятие профессионального стандарта является одним из этапов формирования нового образа специалиста по информационной безопасности в кредитно-финансовой сфере в соответствии с современными вызовами и угрозами в сфере обеспечения информационной безопасности. |
| 8 | Каким образом регулятор предполагает обеспечить достаточные требования к информационной безопасности цифровой валюты Центрального банка Российской Федерации? | При реализации проектов по введению цифровой валюты Центрального Банка (ЦВЦБ) фокус внимания со стороны Банка России в области информационной безопасности направлен, в первую очередь, на создание доверенной среды, которая будет обеспечиваться за счет применения безопасных технологий и своевременного выявления и устранения возможных уязвимостей в технологии обращения ЦВЦБ и компонентах инфраструктуры ЦВЦБ. Главной целью при управлении рисками информационной безопасности необходимо считать обеспечение доверия потребителей к используемым технологиям.  При этом необходимый уровень доверия должен быть обеспечен на всех этапах жизненного цикла ЦВЦБ: безопасная разработка, проектирование, внедрение, сопровождение и использование технологии конечными потребителями. Кроме того, должна проводиться постоянная актуализация уровней рисков нарушения информационной безопасности для компонентов экосистемы и векторов атак – с последующим совершенствованием механизмов защиты и внедрением новых технологий безопасности. |
| 9 | В соответствии с требованиями Положения № 683-П[[3]](#footnote-3) кредитная организация обязана проводить анализ уязвимостей информационной безопасности объектов информационной инфраструктуры и оценку соответствия защиты информации. Фактически данные анализ и оценка в части тестирования инфраструктуры могут быть проведены одним исполнителем соответствующим комплексом аудитов. Однако ввиду того, что каждая работа проводится по соответствующему национальному стандарту Российской Федерации (ГОСТ Р 57580.1-2017[[4]](#footnote-4) и ГОСТ Р ИСО/МЭК 15408-3-2013[[5]](#footnote-5)), она выполняется по отдельным тарифам, что приводит к существенному росту расходов кредитной организации. Планируется ли Банком России инициирование приведения требований методик указанных национальных стандартов к единообразию с целью оптимизации процесса оценки уязвимости инфраструктуры для кредитных организаций? | Оценка выполнения требований к обеспечению защиты информации, установленных Положением Банка России от 17 апреля 2019 года № 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», осуществляется по следующим направлениям:  - оценка выполнения требований к технологическим мерам защиты информации (направление «технологические меры»);  - оценка выполнения требований к безопасности прикладного программного обеспечения автоматизированных систем и приложений (направление «безопасность программного обеспечения»);  - оценка выполнения требований к обеспечению защиты информации информационной инфраструктуры (направление «безопасность информационной инфраструктуры»).  Необходимо обратить внимание, что объекты оценки выполнения требований для каждого направления отличаются. В связи с этим приведение требований национальных стандартов Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и 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» к единообразию является нецелесообразным.  Одновременно с этим считаем возможным оценку выполнения требований по всем трем направлениям в рамках одного аудита с целью оптимизации расходов на их проведение. |
| 10 | Кредитная организация провела оценку соответствия согласно Положению № 382-П[[6]](#footnote-6) в декабре 2019 года. В соответствии с пунктом 8.2 Положения № 719-П[[7]](#footnote-7) с 01.01.2022 Положение № 382-П признается утратившим силу. В этой связи будет ли оценка соответствия, проведенная в течение двух лет (до декабря 2021 года) согласно Положению № 382-П, отвечать требованиям Положения № 719-П? Если нет, то может ли кредитная организация не проводить оценку соответствия по Положению № 382-П и направить ресурсы в 2022 году на проведение оценки соответствия защиты информации согласно Положению № 719-П? | Аудит на соответствие требованиям Положения №382-П необходимо проводить 1 раз в 2 года. Кредитная организация провела оценку соответствия согласно Положению № 382-П в декабре 2019 года, соответственно в декабре 2021 года организации необходимо провести повторный аудит на соответствие требованиям действующего Положения №382-П.  Положение Банка России от 4 июня 2020 г. № 719-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» (далее – Положение 719-П) вступает в силу с 01.01.2022.  В связи с этим для выполнения требований, указанных в Положении № 719-П считаем целесообразным проведение кредитными организациями в 2021 году самооценки с последующим формированием плана устранения несоответствий и отчета о его исполнении по состоянию не позднее чем на декабрь 2021 года. Указанный подход позволит своевременно привести в соответствие требованиям информационную инфраструктуру кредитной организации.  Вместе с тем оценка соответствия, проведенная в 2022 году с привлечением сторонней организации, имеющей соответствую лицензию, будет свидетельствовать о выполнении кредитной организацией требований, указанных в Положении №719-П. |
| 11 | В связи с вступлением в силу требований Положения  № 716-П[[8]](#footnote-8) становится ли подразделение кредитной организации, отвечающее за информационную безопасность, риск-ориентированным подразделением? То есть подразделением, которое в целях реализации требований Положения № 716-П касательно управления риском информационной безопасности и в соответствии с внутренним нормативным документом по управлению операционным риском будет являться службой информационной безопасности и будет:  - согласно пункту 7.9.2. Положения  № 716-П управлять риском информационной безопасности;  - согласно пункту 7.10. Положения  № 716-П формировать специализированные отчеты по рискам информационной безопасности? | Положение № 716-П устанавливает обязанность кредитной организации (головной кредитной организации банковской группы) с учетом требований, указанных в главе 9, определять выполнение службой информационной безопасности или отдельным структурным подразделением, ответственным за обеспечение информационной безопасности, функций в целях обеспечения информационной безопасности согласно п. 7.9.1, а также функций в целях управления риском информационной безопасности согласно п. 7.9.2.  Положение № 716-П устанавливает требование по формированию службой информационной безопасности специализированных отчетов по рискам информационной безопасности согласно п. 7.10. |
| 12 | Согласно пункту 7.10 Положения № 716-П служба информационной безопасности формирует отчеты в соответствии подпунктом 2.15.3 пункта 2.15 Положения  № 382-П. Согласно Положению № 719-П с 01.01.2022 Положение № 382-П признается утратившим силу. Будут ли вноситься изменения в Положение № 716-П в целях уточнения, в соответствии с каким нормативным документом требуется формировать специализированные отчеты по рискам информационной безопасности? | В связи с вступлением в силу Положения Банка России №719-П планируется внесение изменений в Положение №716-П. |
| ***Предложения и инициативы кредитных организаций*** | | |
| 13 | Согласно пункту 14.1 Положения № 672-П[[9]](#footnote-9) участники СБП[[10]](#footnote-10) должны обеспечивать удостоверение электронной подписью электронных сообщений при их передаче между участниками СБП и клиентами участников СБП. В настоящее время технологии, используемые банками и их клиентами - юридическими лицами в рамках услуги организации приема платежей через СБП, определяются договорными отношениями. Информация об операции возврата, инициированная на терминале, передается по защищенным каналам связи в банк и позволяет определить клиента - юридическое лицо, совершающее возврат средств покупателю. Однако такой запрос не может быть подписан электронной подписью в ее толковании, определенном Федеральным законом № 63-ФЗ[[11]](#footnote-11). Предлагается рассмотреть возможность внесения изменений в Положение № 672-П, исключив вышеуказанное требование об удостоверении электронной подписью электронных сообщений между банками и их клиентами, и установить процедуру информационного взаимодействия между ними в рамках договорных отношений и в зависимости от применяемой информационно-технологической инфраструктуры. | В целях исполнения требования пункта 14.1 Положения № 672-П в отношении клиентов – юридических лиц считаем целесообразным использовать электронную подпись ответственного лица юридической организации, являющейся клиентом кредитной организации, для удостоверения электронных сообщений при осуществлении переводов денежных средств с использованием СБП. |
| 14 | Предлагается разработать специальные коды запроса/ответа с информацией о несанкционированном списании и оказания содействия в блокировке и возврате денежных средств. Введение кодов предоставит кредитным организациям возможность реализации приоритетной обработки информации и оперативного проведения мероприятий (при определенных условиях) по противодействию зачисления средств, списанных мошенническим путем[[12]](#footnote-12). | Выражаем Вам благодарность за предоставление информации о пользовательском опыте и предложениях при работе с АСОИ ФинЦЕРТ. Постараемся учесть высказанные предложения при развитии системы. |
| 15 | В условиях цифровизации и унификации форматов банки вновь просят рассмотреть возможность внесения уточнения в ст. 26 Федерального закона № 395-1[[13]](#footnote-13) в части определения понятия «справки по операциям и счетам клиентов» и содержания указываемой в данных документах информации, которые кредитные организации обязаны предоставлять по запросам органов предварительного следствия и органов, уполномоченных осуществлять оперативно-розыскную деятельность, поскольку данное понятие трактуется широко не только запрашивающими органами, но и судами, которые дают разрешение на получение таких справок.  Неверное толкование данного понятия ведет к риску разглашения банковской тайны либо несет риск применения к кредитной организации мер ответственности за неисполнение запроса органов предварительного следствия и органов, уполномоченных осуществлять оперативно-розыскную деятельность. | Банк России не наделе правом разъяснять применение норм федеральных законов, вместе с тем полагаем, что перечень банковских операций и сделок, приведенный в ст. 5 Федерального закона№ 395-1, справки о которых могут быть предоставлены в порядке, предусмотренном ст. 26 указанного Федерального закона, является достаточным и не требует дополнительного уточнения.  Кроме того, согласно статье 26 Федерального закона№ 395-1 правоохранительные органы вправе запрашивать информацию, относящуюся к банковской тайне. В этой связи аргумент в пользу разглашения банковской тайны при направлении справок правоохранительным органам некорректен.  Вместе с тем обозначенная Ассоциацией банков России проблематика может быть разрешена путем разработки единого унифицированного подхода к форме и содержанию справок, предоставляемых кредитными организациями, а также конкретизацией направляемых правоохранительными органами запросов, и может быть реализована внутренними нормативными актами и не требует внесения изменений в федеральное законодательство. |
| 16 | Просим прокомментировать законодательную инициативу в области расширения доступа ФНС России к данным о клиентах банков в рамках обмена информацией с Банком России (Федеральный закон «О внесении изменений в статьи 86 и 102 части первой Налогового кодекса Российской Федерации») в разрезе анализа на предмет соблюдения требований по защите банковской тайны и персональных данных, влияния на требования к информационной безопасности. | Указанный в вопросе законопроект действительно рассматривался Банком России и Департаментом информационной безопасности, в частности. Законопроектом действительно предполагается обмен информацией, в том числе относящейся к банковской тайне, между ФНС России и Банком России. Указанный обмен направлен на исполнение полномочий, возложенных законом на указанный орган и Банк России. При этом при указанном информационном обмене требования к защите информации будут соблюдены. |
| 17 | Предлагаем однозначно нормативно закрепить обязанность кредитных организаций осуществлять сбор биометрических персональных данных физических лиц только после проведения их идентификации с целью приема на обслуживание в кредитную организацию и/или в процессе такого обслуживания.  Учитывая существенные риски, присущие информационным технологиям и дистанционному взаимодействию в целом, существует потребность в их минимизации посредством подтверждения клиентами факта получения банковских услуг или совершения банковских операций с использованием биометрических персональных данных.  Кроме того, практика понуждения кредитных организаций к осуществлению сбора биометрических персональных данных физических лиц, не являющихся клиентами, не соответствует нормам законодательства ПОД/ФТ[[14]](#footnote-14). | Проведение банком идентификации в целях сбора биометрических данных в ЕБС, не должно его обязывать получать финансовую услугу в указанном банке. В соответствии со статьей 3 Федерального закона № 115-ФЗ[[15]](#footnote-15) клиентом признается физическое или юридическое лицо, иностранная структура без образования юридического лица, находящиеся на обслуживании организации, осуществляющей операции с денежными средствами или иным имуществом.  Размещение и обновление в ЕБС сведений о клиенте является самостоятельной услугой, оказываемой банком. В связи с этим отсутствие предшествующих договорных отношений с банком, в том числе отсутствие заключенного договора банковского счета, не может являться основанием для отказа в размещении и обновлении в ЕБС сведений о клиенте.  По мнению Банка России, при приеме на обслуживание клиента, обратившегося в банк в целях регистрации в ЕБС, должна быть выполнена его идентификация в соответствии с требованиями Федерального закона  № 115-ФЗ, сведения о нем должны быть внесены в анкету (досье) клиента. При этом банк вправе предложить клиенту – физическому лицу оказание любых иных услуг, предусмотренных статьей 5 Федерального закона «О банках и банковской деятельности». Однако отказ клиента от получения иных услуг не может служить основанием для отказа в размещении и обновлении сведений о нем ЕБС.  Указанные разъяснения представлены в информационном письме Банка России от 13.12.2019 № ИН-06-59/91.  При этом необходимость идентификации гражданина при личной явке перед сбором биометрических данных как в банке, так и в МФЦ закреплено постановлением Правительства РФ от 14.07.2018 № 820. |
| 18 | Кредитные организации предлагают Банку России рекомендовать ФНС России усилить контроль за внесением записей в ЕГРЮЛ и ЕГРИП, которые являются основными источниками информации при проверке документов клиентов для открытия счета и/или внесения изменений в карточки клиентов.  В последние пару лет участились случаи мошенничества, когда в банк приносят поддельные документы высокого качества, не вызывающие вопросов у операционистов, обладающих лишь общими сведениями о вариантах подделок. При этом при просмотре ЕГРЮЛ и ЕГРИП специалисты видят аналогичные изменения, что позволяет принимать положительное решение об открытии счета или смене уполномоченного лица. О мошеннических действиях в таких ситуациях банки узнают уже постфактум, преимущественно – от уже пострадавших юридических или физических лиц, при этом записи в ЕГРЮЛ и ЕГРИП зачастую корректируются значительно позже (либо совсем не корректируются). | Вопрос не относится к компетенции Банка России. Тем не менее проблематика неактуальных сведений, содержащихся в ЕГРЮЛ и ЕГРИП, существенно влияет на деятельность финансовых организаций в том числе, а также на Банк России при реализации ряда полномочий (в частности, планируется использование сведений из ЕГРЮЛ и ЕГРИП удостоверяющим центром Банка России). В этой связи вопрос взят в проработку. |

1. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере. [↑](#footnote-ref-1)
2. Автоматизированная система обработки инцидентов. [↑](#footnote-ref-2)
3. 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». [↑](#footnote-ref-3)
4. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. [↑](#footnote-ref-4)
5. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. [↑](#footnote-ref-5)
6. 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». [↑](#footnote-ref-6)
7. Положение Банка России от 04.06.2020 № 719-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». [↑](#footnote-ref-7)
8. Положение Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе». [↑](#footnote-ref-8)
9. Положение Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России». [↑](#footnote-ref-9)
10. Система быстрых платежей Банка России. [↑](#footnote-ref-10)
11. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи». [↑](#footnote-ref-11)
12. Аналогичное предложение направлено первому заместителю Председателя Банка России О.Н. Скоробогатовой. [↑](#footnote-ref-12)
13. Закон от 02.12.1990 № 395-1 «О банках и банковской деятельности». [↑](#footnote-ref-13)
14. Аналогичное предложение направлено первому заместителю Председателя Банка России О.Н. Скоробогатовой. [↑](#footnote-ref-14)
15. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». [↑](#footnote-ref-15)