Вопросы безопасности
Правильная ссылка на статью:
Горян Э.В. — Определение факторов безопасности цифровой инфраструктуры в финансово-банковском секторе: подход Сингапура // Вопросы безопасности. – 2022. – № 4. DOI: 10.25136/2409-7543.2022.4.39060 EDN: KFAHYQ URL: https://nbpublish.com/library_read_article.php?id=39060

Определение факторов безопасности цифровой инфраструктуры в финансово-банковском секторе: подход Сингапура

Горян Элла Владимировна

ORCID: 0000-0002-5962-3929

кандидат юридических наук

доцент, Владивостокский государственный университет

690014, Россия, Приморский край, г. Владивосток, ул. Гоголя, 41, каб. 5502

ella-gorjan@yandex.ru

Статья из рубрики ""

DOI:

10.25136/2409-7543.2022.4.39060

EDN:

KFAHYQ

Дата направления статьи в редакцию:

29-10-2022

Дата публикации:

23-11-2022

Аннотация: Объектом исследования являются отношения в сфере обеспечения безопасности цифровых инфраструктур в финансово-банковском секторе. Предмет исследования представлен нормативно-правовыми актами и источниками «мягкого права» Сингапура, устанавливающими требования к информационным системам, персональным и конфиденциальным данным. Определяются особенности сингапурского подхода к регулированию отношений в рассматриваемой сфере. Рассматриваются требования Валютного управления Сингапура к безопасности цифровых инфраструктур как в государственном, так и в частном секторе. Характеризуются особенности обеспечения безопасности ключевых компонентов цифровых инфраструктур: цифровой идентичности; авторизации и согласия; функциональной совместимости платежных систем и обмена данными. Исследуется роль финансового регулятора в обеспечении безопасности цифровых инфраструктур. Основными факторами безопасности цифровой инфраструктуры финансово-банковского сектора Сингапур определил целостный подход

к разработке политики регулирования, равно как и определяющую роль финансового регулятора в создании цифровой инфраструктуры. Техническая сторона является лишь одним из элементов цифровой инфраструктуры: необходимо сбалансировать нормативные, технические и деловые стандарты. Выделенные Валютным управлением Сингапура ключевые компоненты цифровой инфраструктуры определяют уровень безопасности производственных процессов финансовых институтов. Внимание должно быть сфокусировано на укреплении доверия конечного пользователя. Защищенность цифровой инфраструктуры финансовых институтов от угроз повышает степень доверия к этим институтам со стороны инвесторов. Поэтому финансовые институты Сингапура имеют высокую инвестиционную привлекательность.

Ключевые слова:

финансово-банковский сектор, информационная безопасность, персональные данные, цифровая инфраструктура, финансовый регулятор, финтех, авторизация, цифровая идентичность, обмен данными, интероперабельность платежных систем

Актуальность. Финансовые институты развитых экономик мира становятся мишенями серьезных кибератак. Сингапур не является исключением: будучи самым развитым с точки зрения информационных технологий в мире государством, он является также ключевым международным финансовым и торговым центром. Это делает его идеальной мишенью для кибератак, последствия которых гораздо серьезнее, чем обычное нарушение общественного и экономического благополучия Сингапура – под удар попадает вся цепочка международных поставок и банковская сфера, а в перспективе – и международная экономика. Поэтому законодатель этого города-государства оперативно реагирует на возникающие вызовы и совершенствует нормативно-правовую базу. Например, в 1993 году Сингапур первым из государств Юго-восточной Азии принял Акт о злоупотреблениях в компьютерных сетях и кибербезопасности (Computer Misuse and Cybersecurity Act). Вторая декада XXI века ознаменовалась бурным ростом цифровой экономики, на что Сингапур отреагировал Актом о защите персональных данных (Personal Data Protection Act 2012), Национальным планом действий в отношении киберпреступности (National Cybercrime Action Plan 2016), Стратегией национальной кибербезопасности (National Cybersecurity Strategy 2016) и Актом о кибербезопасности (Cybersecurity Act 2018) [1, с. 105]. В своей Стратегии кибербезопасности Сингапур выделил четыре основных направления тесного сотрудничества частного и публичного секторов по обеспечению кибербезопасности: (i) построение устойчивой инфраструктуры; (ii) создание безопасного киберпространства с привлечением гражданского общества; (iii) развитие динамичной экосистемы кибербезопасности за счет увеличения количества специалистов в результате сотрудничества с образовательными заведениями; (iv) усиление международного сотрудничества, особенно в рамках АСЕАН (Singapore's Cybersecurity Strategy 2016, URL: https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy).

Сингапур одним из первых осознал, что следующим этапом цифровой революции является переход от фрагментированных цифровых решений к цифровым инфраструктурам. Они будут стимулировать более широкое внедрение цифровых технологий в экономике и обществе [2, p. 2]. Цифровые инфраструктуры обеспечивают совместимость решений и бесперебойность услуг, что позволяет охватить большее число людей и предприятий при меньших затратах и большем удобстве. Государственные

фундаментальные цифровые инфраструктуры имеют решающее значение для всеохватывающего экономического и социального развития. Подобно тому, как физическая инфраструктура стимулировала появление промышленной экономики, фундаментальные государственные цифровые инфраструктуры ускоряют рост цифровой экономики.

Постановка проблемы исследования. Финансово-банковский сектор одним из первых экономических секторов перешел в цифровую среду. Цифровая инфраструктура финансовых институтов обеспечивает непрерывность торгово-экономических процессов, поэтому её безопасность – залог стабильности кредитно-финансовых и товарно-денежных отношений. Безопасность финансово-банковского сектора имеет информационную природу, поскольку по своей сути он представляет собой совокупность данных, отражающих движение капиталов и работу инструментов. А данные существуют в цифровом формате, они обрабатываются в информационных системах, уязвимых к физическому (техническому) и человеческому влиянию. Противодействовать информационным угрозам можно при условии их определенности, то есть известности тех показателей (факторов), которые определяют саму сущность существования объекта. В связи с этим необходимость определения таких факторов является насущным вопросом, стоящим перед регулятором. Защищенность цифровой инфраструктуры финансовых институтов от угроз влияет на степень доверия к этим институтам как со стороны контрагентов, так и со стороны инвесторов, доверяющих им свои капиталы. Высокая волатильность цифровых активов привлекает большое количество непрофессиональных инвесторов, желающих приумножить свои капиталы. Поэтому перед лицом сохранения притока инвестиций финансовые институты вынуждены повышать расходы на обеспечение безопасности цифровых инфраструктур.

Цель исследования – охарактеризовать подход Сингапура по определению факторов безопасности цифровой инфраструктуры в финансово-банковском секторе.

Методология. Для получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный и формально-логический методы) и специальных юридических методов познания (сравнительно-правовой и формально-юридический методы).

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования составляют основные нормативно-правовые акты в сфере обеспечения безопасности цифровой инфраструктуры Сингапура. Выбранная нами для исследования тема еще не достаточно изучена в российской научной литературе и является логическим продолжением нашего исследования в рамках гранта РФФИ «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект». Однако следует отметить работу О.М Махалиной и В.Н. Махалина, в которой они доказывают необходимость рассмотрения затрат на информационную безопасность в качестве «стратегических инвестиций, обеспечивающих непрерывность их бизнес-процессов и, которые, создают преимущества в эпоху стремительно развивающихся киберугроз» [3, с. 136].

Основная часть. Валютное управление Сингапура (Monetary Authority of Singapore) в 2021 году определило четыре ключевых компонента базовой цифровой инфраструктуры: 1) цифровую идентичность (digital identity), 2) авторизацию и согласие (authorization and consent), 3) функциональную совместимость платежных систем (payments interoperability) и 4) обмен данными (data exchange) [2, p. 2-3]. Уровень безопасности

этих основных компонентов влияет на возможность осуществления цифровых операций, в своей совокупности они обеспечивают фундамент цифровой экономики. В науке принято выделять несколько факторов безопасности информационных систем [4, с. 30]: когнитивный, социальный, информационно-технический и организационно-административный. Следовательно и цифровые инфраструктуры, будучи комплексными информационными объектами, могут быть подвержены влиянию процессов и явлений, негативно сказывающихся на их функциональности. По своей сути цифровая инфраструктура – это комплекс технологий и построенных на их основе цифровых продуктов, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности, и работающих на цифровой основе (Цифровая трансформация. Термины и определения: СТБ 2583-2020. – Введ. 2021–03–01. – Минск: Госстандарт, 2020. – 16 с.). Поэтому выделенные Валютным управлением Сингапура ключевые компоненты цифровой инфраструктуры и определяют уровень безопасности производственных процессов финансовых институтов. Рассмотрим их подробнее.

Ключевым элементом цифровой инфраструктуры является надежная **цифровая идентичность**, позволяющая отдельным лицам, предприятиям и государственным учреждениям представлять себя и действовать от имени других в цифровом пространстве. Цифровую идентичность личности понимают как «совокупность уникальных персональных данных личности, представленных в цифровой форме, позволяющих идентифицировать данную личность от иных субъектов цифрового взаимодействия» [5, с. 9].

Цифровая идентичность позволяет автоматизировать доступ к службам, предоставляемым компьютерами, и позволяют самим компьютерам опосредовать отношения. Она выступает в качестве общего, надежного и повторно используемого способа передачи данных. Цифровая идентичность позволяет пользователям использовать одно средство аутентификации через несколько цифровых сервисов (включая веб-сайты, приложения, устройства). Эти данные в совокупности определяют личность и могут использоваться для идентификации отдельного лица, предприятия или государственного учреждения. Цель цифровой идентичности шире, чем общая идентификация конечного пользователя: она может подтвердить его способность получить доступ к услугам или выполнить конкретную задачу.

С цифровой идентичностью связаны механизмы, обеспечивающие надлежащее использование персональных данных (Personal Data Protection Act 2012, URL: https://sso.agc.gov.sg/Act/PDPA2012). Они необходимы для обеспечения надлежащей безопасности, предотвращения мошенничества и других мер контроля, а также для других целей, подразумеваемых в силу характера использования данных. Такое использование персональных данных законно и все виды использования должны сообщаться/доводиться до сведения пользователей надлежащим образом. В результате пользователи должны понимать, как используются их данные и для каких целей, а объем данных должен быть достаточен для достижения конкретной цели. Операторы информационных систем должны использовать уведомления и формы согласия, чтобы пользователи цифровых инфраструктур понимали порядок использования их персональных данных.

Устраняя необходимость использования нескольких паролей и процедур проверки личности, цифровая идентичность позволяет клиентам использовать одно средство идентификации себя в нескольких цифровых сервисах, включая веб-сайты, приложения, устройства и проч. Это позволяет пользователю определить себя как конечного адресата

услуги или товара. Цифровая идентичность принадлежит, управляется и контролируется индивидом, что означает, что он имеет право на доступ к своим персональным данным, их изменению и удалению, а также имеет право на защиту в случае нарушения его прав. Ввиду сложности валютно-финансовых и торгово-экономических отношений, вовлекающих в правовую плоскость нескольких субъектов одновременно, возникает объективная необходимость создания так называемой «экосистемы», сложной цифровой инфраструктуры, обеспечивающей безопасный обмен данными между конечными пользователями, информационными посредниками, поставщиками услуги и провайдерами услуг по верификации данных, равно как и операторами персональных данных вместе с техническими устройствами хранения таких данных [2, p. 10].

Авторизация определяется как процесс предоставления пользователю или группе пользователей определенных разрешений, прав доступа и привилегий в компьютерной системе [6, с. 402].

Для того чтобы информационные системы работали эффективно, большинство стран и регионов ввели в действие комплекс правовых норм и других требований, гарантирующих понимание пользователей о процессах использования информация в каждом цифровом контексте. Цель этих требований заключается в обеспечении транспарентности информации для отдельных лиц, а также большей подотчетности всех операторов (как государственных, так и частных лиц), которые могут использовать персональные и конфиденциальные данные для осуществления сделки или оказания услуг (Cybersecurity Act 2018, URL: https://www.csa.gov.sg/legislation/cybersecurity-act).

Один из наиболее распространенных методов обеспечения прозрачности и получения **согласия** от физического лица заключается в том, чтобы направить физическому лицу какое-либо уведомление, а затем запросить согласие на использование, указанное в уведомлении. Существуют различные модели уведомления и согласия, которые были развернуты рядом систем. Наиболее распространенным является **механизм явного уведомления и согласия,** который позволяет конечным пользователям выбирать, как их данные используются, когда они в цифровом виде взаимодействуют и осуществляют транзакции с выбранными ими поставщиками услуг (Technology Risk Management Guidelines for Financial Institutions 2021, URL: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines).
Это дает пользователям возможность контролировать свои данные, давать согласие на обмен данными или инициирование платежей. Этот метод является моделью высокого доверия, позволяющей пользователям осуществлять определенный контроль над своими действиями и транзакциями в цифровой экономике.

Все механизмы авторизации и согласия требуют четкого и прозрачного раскрытия информации о том, как и какая информация будет собираться, использоваться и передаваться. Чтобы цифровая среда функционировала и вызывала доверие у пользователей, транспарентность (прозрачность) является ключом к обеспечению понимания сторонами своих обязанностей друг перед другом. В зависимости от конфиденциального характера идентификационных и персональных данных, а также от того, как эта информация будет использоваться и насколько широко она будет распространяться или публиковаться, важно, чтобы все стороны понимали необходимость обеспечения безопасности информации и принципа минимизации данных (сбор, использование и хранение только тех данных, которые необходимы для создания и предоставления данной услуги). Все стороны должны раскрывать, либо первоначально, либо по запросу, все виды использования данных. Для дальнейшего

достижения доверия и контроля пользователей следует по возможности внедрять технологии повышения конфиденциальности и безопасности, чтобы свести к минимуму обмен персональными и конфиденциальными данными в открытом виде, чтобы обеспечить необходимую всем сторонам защиту [2, p. 11].

Службы согласия обычно представлены в виде информационной панели или хранилища данных, которые предоставляют пользователям информацию о том, какие данные будут использоваться, для каких целей и с какими поставщиками услуг. После авторизации пользователь работает со службой согласия, выбирая ряд сервисов, для которых он разрешает использовать свои данные, и дает разрешение или согласие на использование своих данных для ряда транзакций или сервисов. Этот тип разрешения может быть выдан на неограниченный период времени или иметь определенную дату действия. Он по-прежнему позволяет пользователю устанавливать уровень и тип обмена информацией и типы использования. Пользователь может в любое время снова войти в хранилище данных или на панель инструментов, чтобы изменить свои настройки или разрешения и/или выбрать новые сервисы, с которыми можно поделиться своими данными. Преимущество этого метода заключается в том, что он устраняет трения, связанные с повторным прерыванием потоков данных для получения согласия от человека. У него также есть недостаток, заключающийся в том, что пользователи не обязательно регулярно просматривают свои личные кабинеты, чтобы убедиться, что они помнят или полностью понимают последствия своего согласия и связанного с этим обмена данными.

Для обеспечения беспрепятственных платежей как между цифровыми, так и между цифровыми и физическими средами необходима **функциональная совместимость платежных систем** (интероперабельность платежных систем). Интероперабельность - сложное и многогранное понятие, включающее в себя компоненты управления, технические аспекты и брендинг. Управление включает в себя набор правил и контрактов, которые позволяют сторонам участвовать в процессе клиринга и расчетов (обычно известный как «схема»). Управление может быть установлено локальным актом финансового института или законом (Payment Services Act 2019, https://www.mas.gov.sg/regulation/acts/payment-services-act). Технические компоненты представляют собой инфраструктуру, с помощью которой осуществляется обмен платежными (или связанными с ними) сообщениями, а также форматы, сети, протоколы безопасности и механизмы, обеспечивающие безрисковое и своевременное выполнение функций клиринга и расчетов.

Функциональная совместимость платежных систем зависит от следующих факторов: 1) субъекты доступа - доступ к схеме оплаты часто не ограничивается банками. Компании и сторонние поставщики решений (поставщики платежных шлюзов, gateway providers) также могут иметь доступ в соответствии с правилами и структурой схемы; 2) недискриминационный и простой характер доступа означает простые и обоснованные параметры присоединения к платежной схеме. Они включают в себя адаптацию и постоянное участие. Небольшие банки или новые участники отрасли не должны сталкиваться с неоправданно высокими или неадекватными входными барьерами; 3) инновативность - дизайн схемы и ее инфраструктура должны поощрять инновации. Простота доступа и общие стандарты сообщений являются ключевыми. Практическим путем необходимо выявлять и реализовывать новые варианты использования платежных систем (независимо от лежащих в их основе платежных схем; 4) защита пользователей - должны быть предусмотрены меры по защите прав пользователей, в частности, защита данных и обнаружение мошенничества; 5) время проведения операций – обработка

платежей может осуществляться по расписанию, т.наз. пакетная обработка (batch, scheduled processing) или в режиме реального времени. Последнее время во всем мире наблюдается сдвиг в пользу последнего. Тем не менее, пакетная обработка по-прежнему имеет значительные преимущества там, где не требуется режим реального времени, например ежемесячные выплаты заработной платы; 6) управление рисками является ключевой проблемой для платежных схем. Требуются механизмы для устранения расчетного риска, управления репутационным риском и предоставления банкам возможности управлять кредитным риском; 7) возможность замены является важным фактором снижения риска и обеспечения возможности выбора для пользователя. Возможность замены одной платежной схемы на другую (например, осуществление платежей в режиме реального времени и пакетных платежей) помогает снизить риск технического сбоя банка или платежной схемы. Замена также позволяет покупателям и продавцам выбрать наиболее подходящий вариант осуществления платежей; 8) стандарты связи, основанные на ISO 20022, являются общими открытыми стандартами. Они помогают банкам и другим учреждениям оптимизировать свои системы и позволяют поставщикам разрабатывать услуги и продукты. Допускается замена общих стандартов сообщений; 9) безопасность - стандарты безопасности напрямую поддерживают целостность и договорной характер платежной схемы. Стандарты должны быть достаточно сильными, чтобы противостоять новейшим угрозам, и должны обеспечивать аутентификацию, конфиденциальность, целостность данных и неотказуемость (non-repudiation) работы. Неотказуемость является ключом к поддержке договорного характера платежной схемы и системы ответственности для неё [2, p. 12].

Эта факторы определяют необходимость разработки сервисов, опирающихся на местную клиринговую и расчетную инфраструктуру. В качестве примера можно привести прокси (proxy) - альтернативу номерам банковских счетов и такой сервис как Request-to-Pay (RtP). Proxy дословно переводится как «посредник». Это минимальный набор данных (QR-код, номер телефона или адрес электронной почты, например), к которым привязаны банковские реквизиты бенефициаров. Платежи совершаются простым указанием прокси бенефициара, сохраняя его персональные или конфиденциальные данные в тайне от плательщика. Прокси – это альтернативный известный и удобный идентификатор, обеспечивающий безопасность данных банковского счета. Он также работает независимо от текущего счета и связанного с ним банка (другими словами, владелец счета может переместить свой счет в другой банк, и платежи будут следовать до тех пор, пока обновляется информация о едином прокси/счете).

Request-to-Pay дословно переводится как «запрос на оплату» и означает, что получатель платежа инициирует запрос на конкретную операцию от плательщика. Система предоставляет цифровой запрос, который плательщик может получить на своем мобильном устройстве. Он может появиться в мобильном банковском приложении или через стороннее приложение. После этого плательщик может принять или отклонить платежный запрос. В зависимости от региона запрос может также включать подробную информацию о сделке, дату платежа или другие реквизиты счета-фактуры. Если плательщик утверждает платежи, получателю платежа инициируется перевод в режиме реального времени. Этот сервис обеспечивает быстрый способ осуществления операций между двумя сторонами без необходимости запоминания или поиска полной информации о счете.

Обмен данными позволяет конечным пользователям сделать свои данные доступными и доступными для своих поставщиков услуг в течение установленного периода времени и с определенной целью. Можно обмениваться данными, чтобы обеспечить финансовое

планирование через приложения и финансовые консультанты, что упрощает сбор информации для подачи налогов или подачи заявок на кредиты на основе проверенной информации. Обмен данными также может поддерживать платежи, аутентифицируя учетные записи их владельцев и обеспечивая цифровую идентификацию, предоставляя информацию для аутентификации человека. Данные, подлежащие обмену, могут включать детали кредита, данные о транзакциях, демографические данные и активы. Как и другие элементы, поддерживающие цифровую инфраструктуру, для обмена данными потребуются технические компоненты и компоненты управления.

Чтобы обмены данными осуществлялись должным образом в контексте конкретной цифровой инфраструктуры, необходимо учитывать цели, для которых будет использоваться обмен данными, и следующие критерии проектирования. Во-первых, это требования безопасности, гарантирующие, что обмен данными является безопасным, но при этом достаточно гибким для реализации новейших технологий. Во-вторых, это требования конфиденциальности, обеспечивающих прозрачность и понятность процессов, в которых используются данные, для пользователей, а также согласие на передачу и использование своих данных и возможность отозвать это согласие. В-третьих, это технические стандарты, обеспечивающие совместимость механизмов передачи данных. Программные интерфейсы приложения (application programming interface, API) должны предоставлять данные необходимого качества в одном и том же формате для определенных вариантов использования. В-четвертых, это стандарты аутентификации физических или юридических лиц в их учетных записях и данных для ограничения мошеннического доступа и ограничения обмена или хранения банковских учетных данных. В-пятых, это стимулы для поставщиков данных (например, финансовых учреждений) для обеспечения своевременного доступа к данным, поскольку отсутствие стимулов может создавать препятствия для обмена данными. И наконец, это паритет доступа к данным для частных лиц и малого бизнеса для получения полной экономической выгоды для всех участников экосистемы, а также равные режимы деятельности для всех участников экосистемы. Это позволит обеспечить конкуренцию между поставщиками данных (например, финансовыми учреждениями), агрегаторами данных (т. е. техническими посредниками и поставщиками услуг) и пользователями данных (такими как поставщик платежных функций) [2, p. 13].

Безопасность обмена данными зависит от нескольких факторов. Это, прежде всего, функциональная безопасность API и аналогичные механизмов передачи данных для обеспечения текущего обмена данными между поставщиками данных, любыми посредниками и конечным пользователем данных. Аутентификация пользователей в их учетных записях должна осуществляться безопасным и надежным способом, что снижает риски мошенничества. Должны быть предусмотрены возможности управления и менеджмента данными (data governance and data management) для преобразования предоставленных данных в необходимую информацию для конкретных вариантов использования, например, для осуществления анализа с целью предотвращения мошенничества. Менеджмент данными включает в себя процессы от создания данных до их удаления. Управление данными заключается в создании правил и решений для операционных процессов, которые выполняются в рамках этих процессов (поэтому управление данными не является отдельным процессом). И наконец, важным фактором является разработка, корректировка и обновляемость и корректировка управленческих и технических стандартов уполномоченными государственными органами и саморегулируемыми организациями.

В отличие от интернет-инфраструктуры, создание цифровой инфраструктуры требует не

только соблюдения технических стандартов. Например, при осуществлении цифровых транзакций внутренние и внешние обмены финансовой информацией строятся на доверительных сетях, которые регулируются правовыми, деловыми и техническими соглашениями и стандартами. По мере того, как данные становятся все более ценными в цифровой экономике, есть веское основание для применения механизмов «управления цифровыми платежами» для обеспечения доверия в цифровых инфраструктурах. Это, в конечном счете, приводит к созданию цифровой инфраструктуры, которая позволяет конечным пользователям контролировать как свои деньги, так и данные надежным образом, помещая человека в центр цифровой экосистемы.

Валютное управление Сингапура выступило с инициативой об объединении усилий всех регуляторов по выработке общего стратегического понимания, определении надлежащих инструментов регулирования и взаимодействия соответствующих заинтересованных сторон. Финансовый регулятор подверг критике склонность государственного аппарата к чрезмерному регулированию внедрения инноваций. По его мнению, наилучшей мотивацией инновационной деятельности исторически является коммерческий фактор. [2, p. 3]. Технологические новшества регулярно внедряются компаниями, ищущими рыночные ниши, которыми являются неудовлетворенные потребности конечных пользователи (потребители, компании или правительства). Инновации должны приносить желаемые и необходимые результаты. Правительство должно взять на себя роль создателя благоприятного климата для инвестиций в инновации. Сингапур уже давно является глобальным лидером, установив правильный баланс между поощрением инвестиций в новые технологии в финансово-банковской сфере и защитой своего населения от недобросовестных субъектов. Это является результатом активного взаимодействия государственного аппарата и руководства финансовых институтов.

Выводы. В результате проведенного исследования мы пришли к следующим выводам. Валютное управление Сингапура выдвигает одинаковые требования к безопасности цифровых инфраструктур как в государственном, так и в частном секторе. В любой цифровой инфраструктуре должна быть обеспечена безопасность четырех ключевых компонентов: 1) цифровой идентичности (digital identity), 2) авторизации и согласия (authorization and consent), 3) функциональной совместимости платежных систем (payments interoperability) и 4) обмена данными (data exchange). Цифровая идентичность определяет уверенность с двух сторон цифрового взаимодействия. Каждый участник должен быть уверен, что сторона на другом конце - это тот субъект, за кого он себя выдает. Поэтому должны быть разработаны механизмы для обеспечения аутентификации и подтверждения личности пользователя при одновременном обеспечении конфиденциальности и безопасности информации. Цифровое взаимодействие должно быть прозрачными, безопасными и эффективными. Данные должны использоваться в соответствии с целями, которые для которых они предоставлены, и таким образом, который ожидается и понимается пользователями. В цифровую инфраструктуру должны быть встроены инструменты и механизмы, объясняющие пользователям, каким образом осуществляется сбор, использование и обмен их информацией, а также дающие возможность владеть, управлять и контролировать свои персональные и конфиденциальные данные. Обеспечение функциональной совместимости платежных систем включает управленческие и технические факторы, учет которых влияет на безопасность транзакций. Аналогичными должны быть подходы и к обмену данными: поставщики данных (финансовые институты) должны обеспечивать использование данных в интересах конкретного лица. Обмен данными позволяет производить платежи, осуществлять финансовое планирование, создавать цифровую идентичность, создавать кредитные файлы и совершать иные действия, обусловленные природой цифровой

инфраструктуры.

Основными факторами безопасности цифровой инфраструктуры финансово-банковского сектора являются следующие. Это целостный подход к разработке политики регулирования, равно как и определяющая роль финансового регулятора в создании цифровой инфраструктуры. Кроме того, важно помнить, что техническая сторона является лишь одним из элементов цифровой инфраструктуры: необходимо сбалансировать нормативные, технические и деловые стандарты. Внимание должно быть сфокусировано на укреплении доверия конечного пользователя. Защищенность цифровой инфраструктуры финансовых институтов от угроз повышает степень доверия к этим институтам со стороны инвесторов. Поэтому финансовые институты Сингапура имеют высокую инвестиционную привлекательность.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект»

Библиография

1. Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117.
2. Foundational digital infrastructures for inclusive digital economies. – Singapore: Monetary Authority of Singapore, 2021. – 58 p.
3. Махалина О.М., Махалин В.Н. Цифровизация бизнеса увеличивает затраты на информационную безопасность // Управление. 2020. Т. 8. № 1. С. 134-140.
4. Козачок В.И., Власова С.А. Факторы, определяющие информационную безопасность корпорации // Среднерусский вестник общественных наук. 2014. № 5 (35). С. 30-34.
5. Дудко М.О. Цифровая идентичность личности: теоретико-правовой аспект // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2019. Т. 9. № 3. С. 6-12.
6. Филяк П.Ю., Захаренков И.А., Перевезенцев И.С. Обеспечение информационной безопасности информационной системы с помощью искусственного интеллекта - подходы, технология (часть 1) // Информация и безопасность. 2021. Т. 24. № 3. С. 401-412.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ на статью на тему «Определение факторов безопасности цифровой инфраструктуры в финансово-банковском секторе: подход Сингапура».
Предмет исследования. Предложенная на рецензирование статья посвящена вопросам определения «…факторов безопасности цифровой инфраструктуры в финансово-банковском секторе: подход Сингапура». Автором выбран особый предмет исследования: предложенные вопросы должны были бы исследоваться с точки зрения информационного права Сингапура, но имеются лишь ссылки на НПА Сингапура и

перевод отдельных разделов Стратегии национальной кибербезопасности (National Cybersecurity Strategy 2016), при этом автором отмечено, что «Финансовые институты развитых экономик мира становятся мишенями серьезных кибератак». Изучается законодательство, имеющее отношение к цели исследования. Также изучается и обобщается определенный объем научной литературы по заявленной проблематике, анализ и дискуссия с авторами-оппонентами отчасти присутствует. При этом автор отмечает, что «Противодействовать информационным угрозам можно при условии их определенности, то есть известности тех показателей (факторов), которые определяют саму сущность существования объекта. В связи с этим необходимость определения таких факторов является насущным вопросом, стоящим перед регулятором».

Методология исследования. Цель исследования определена названием и содержанием работы: «Безопасность финансово-банковского сектора имеет информационную природу, поскольку по своей сути он представляет собой совокупность данных, отражающих движение капиталов и работу инструментов», «…охарактеризовать подход Сингапура по определению факторов безопасности цифровой инфраструктуры в финансово-банковском секторе». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с вышеназванными вопросами и использованием определенного опыта. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется совокупность общенаучных, специально-юридических методов познания. В частности, методы анализа и синтеза позволили обобщить некоторые ограниченные подходы к предложенной тематике и отчасти повлияли на выводы автора. Наибольшую роль сыграли специально-юридические методы. В частности, автором применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства Сингапура. При этом в контексте цели исследования формально-юридический метод мог бы быть применен в совокупности со сравнительно-правовым методом, тем более, что автор заявляет: «Для получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный и формально-логический методы) и специальных юридических методов познания (сравнительно-правовой и формально-юридический методы)». В частности, делаются такие выводы: «Основными факторами безопасности цифровой инфраструктуры финансово-банковского сектора являются следующие. … целостный подход к разработке политики регулирования, равно как и определяющая роль финансового регулятора в создании цифровой инфраструктуры. … техническая сторона …: необходимо сбалансировать нормативные, технические и деловые стандарты» и др. Таким образом, выбранная автором методология адекватна цели статьи, позволяет привести отдельные аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является одной из важных в мире и России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает, что «Сингапур …является также ключевым международным финансовым и торговым центром. Это делает его идеальной мишенью для кибератак, последствия которых гораздо серьезнее, чем обычное нарушение общественного и экономического благополучия Сингапура – под удар попадает вся цепочка международных поставок и банковская сфера, а в перспективе – и международная экономика». И на самом деле здесь должен следовать анализ работ оппонентов и НПА, и он следует в основном в отношении Стратегии национальной кибербезопасности (National Cybersecurity Strategy 2016) и автор показывает умение владеть материалом, в некоторых случаях приводя перевод из нее. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи вызывает сомнения. Она не

выражается в конкретных научных выводах автора. Среди них, например, такой: «Защищенность цифровой инфраструктуры финансовых институтов от угроз повышает степень доверия к этим институтам со стороны инвесторов». Как видно, указанный и иные «теоретические» выводы не могут быть использованы в дальнейших научных исследованиях. Таким образом, материалы статьи в представленном виде могут иметь ограниченный интерес для научного сообщества.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как посвящена вопросам определения «…факторов безопасности цифровой инфраструктуры в финансово-банковском секторе: подход Сингапура». В статье присутствует очень краткая аналитика по научным работам оппонентов (их всего 4), поэтому автор отмечает, что уже ставился вопрос, относительно близкий к данной теме: «Выбранная нами для исследования тема еще не достаточно изучена в российской научной литературе и является логическим продолжением нашего исследования в рамках гранта…», но автор практически не использует материалы оппонентов и не приводит результаты предыдущих исследований, дискутирует с отдельными оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг некоторых целей своего исследования. Качество представления исследования и его результатов следует признать не до конца доработанным. Из текста статьи прямо следуют предмет, задачи, методология, но отсутствуют результаты юридического исследования, научная новизна. Оформление работы соответствует отдельным формальным требованиям, предъявляемым к подобного рода работам. Складывается впечатление, что работа представляет из себя пособие, в котором расписываются вопросы безопасности «цифровой инфраструктуры в финансово-банковском секторе» и приводит ссылки на НПА Сингапура. Существенные нарушения данных требований: отсутствие научной новизны; небольшое количество литературы по данной теме, соответственно оппонентов практически нет и др.

Библиография. Следует низко оценить качество использованной научной литературы. Присутствие современной научной литературы могло бы показать обоснованность выводов автора. Труды приведенных авторов соответствуют теме исследования, но не обладают признаком достаточности, способствуют раскрытию некоторых общих аспектов темы.

Апелляция к оппонентам. Автор провел анализ текущего состояния исследуемой проблемы. Автор описывает некоторые точки зрения оппонентов на проблему, аргументирует правильную по его мнению позицию, опираясь на работы оппонентов, предлагает варианты решения отдельных проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, не всегда конкретными. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам только после доработки. На основании изложенного, суммируя все положительные и отрицательные стороны статьи рекомендую «отправить на доработку».