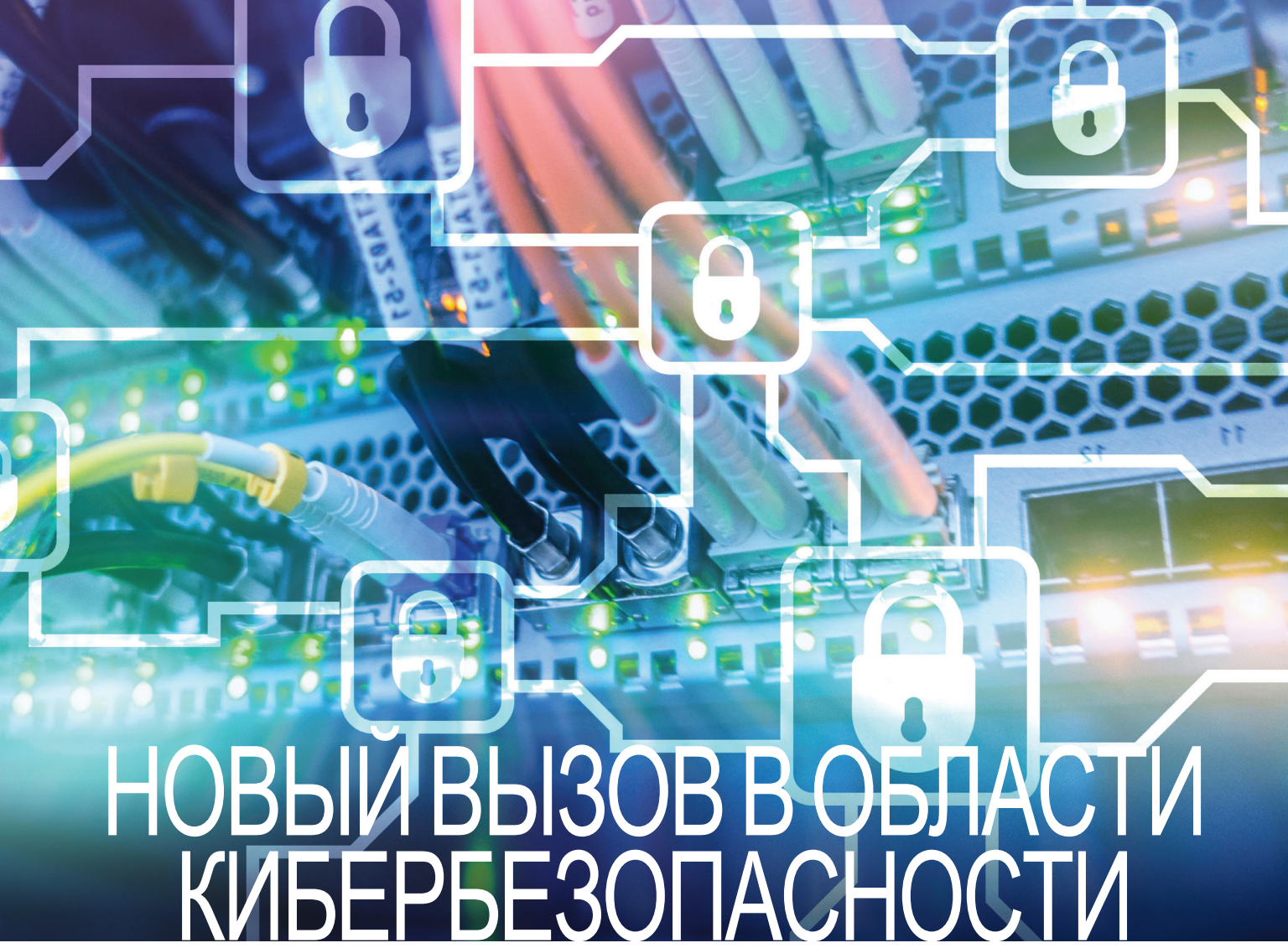

НОВЫЙ ВЫЗОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

ДЛЯ ЦЕНТРАЛЬНЫХ БАНКОВ

Цифровые валюты центральных банков могут создавать риски в отношении безопасности, но при ответственном подходе их можно превратить в потенциальные возможности

Джош Липски, Оле Моер и Джулия Фанти

В обычно осторожном мире центральных банков идея цифровой валюты центрального банка (ЦВЦБ) развивается с молниеносной скоростью. Исследование Центра геоэкономики Атлантического совета показывает, что 105 стран и валютных союзов в настоящее время изучают возможность запуска ЦВЦБ в виде либо розничной валюты, эмитируемой для широкой общественности, либо оптовой, которая в основном используется для межбанковских операций. Их число увеличилось с примерно 35-ти в 2020 году. К тому же интерес проявляют не только небольшие экономики; 19 стран Группы 20-ти рассматривают возможность выпуска ЦВЦБ, и большинство из них уже продвинулись дальше стадии исследования.

Однако по мере того, как все больше стран запускают пилотные проекты ЦВЦБ, опасения по поводу кибербезопасности и конфиденциальности становятся все более серьезными. Председатель Федеральной резервной системы Джером Пауэлл недавно назвал «киберугрозу» своим главным опасением в отношении финансовой стабильности, а в недавнем докладе Палаты лордов Соединенного Королевства риски в отношении кибербезопасности и конфиденциальности особо отмечены как потенциальные причины для отказа от разработки ЦВЦБ.

Эти опасения небезосновательны. Уязвимые места ЦВЦБ могут быть использованы для дискредитации финансовой системы страны. ЦВЦБ смогут накапливать конфиденциальные данные о платежах и пользователях в беспрецедентных масштабах. Оказавшись в чужих руках, эти данные могут быть использованы для шпионажа за частными операциями граждан, получения конфиденциальной информации о физических

Технология позволяет центральным банкам обеспечить гарантии как кибербезопасности, так и защиты конфиденциальности в любом проекте ЦВЦБ.

лицах и организациях, и даже для кражи денег. Если ЦВЦБ будет внедрена без надлежащих протоколов безопасности, она может существенно расширить масштабы и объемы многих угроз безопасности и конфиденциальности, которые уже существуют в современной финансовой системе.

До недавнего времени в мире кибербезопасности и центральных банков было проделано мало работы, чтобы реально понять конкретные риски для кибербезопасности и конфиденциальности, связанные с ЦВЦБ. Мало кто задумывался о том, способны ли конструктивные особенности ЦВЦБ смягчить риски или, возможно, даже повысить кибербезопасность финансовой системы.

В нашем новом исследовании, опубликованном в недавнем докладе Атлантического совета под названием «Недостающий ключ. Проблема кибербезопасности и ЦВЦБ», проводится анализ новых угроз кибербезопасности, которые ЦВЦБ могут представлять для финансовых систем, и приводится обоснование того, что директивные органы располагают достаточным количеством вариантов безопасного внедрения ЦВЦБ. Существует множество вариантов конструктивных решений для ЦВЦБ, начиная от централизованных баз данных до распределенных реестров и систем на основе токенов. Каждый проект должен быть рассмотрен, прежде чем делать выводы об угрозах кибербезопасности и конфиденциальности. Эти проекты также необходимо сравнить с нынешней финансовой системой — той, которая не дает Пауэллу спать по ночам, — чтобы определить, могут ли новые технологии обеспечить более безопасные варианты.

Какие же основные новые киберугрозы могут возникнуть в ЦВЦБ? И что более важно, что можно сделать для смягчения этих рисков?

Централизованный сбор данных

Многие из предлагаемых вариантов конструктивных решений для ЦВЦБ (особенно розничных ЦВЦБ) включают централизованный сбор данных об операциях, что создает серьезные риски для конфиденциальности и безопасности. С точки зрения конфиденциальности такие данные могут быть использованы для слежки за платежами граждан. Накопление такого количества конфиденциальных данных в одном месте также увеличивает угрозу безопасности, намного повышая отдачу для потенциальных злоумышленников.

Однако риски, связанные с централизованным сбором данных, можно смягчить, либо вообще отказавшись от их сбора, либо выбрав структуру проверки, в которой каждый компонент видит только тот объем информации, который необходим для его функционирования. В последнем подходе могут помочь криптографические инструменты, такие как доказательства с нулевым разглашением, которые удостоверяют личные данные, не раскрывая их и не подвергая их опасности, или методы криптографического хеширования. Например, в рамках совместного проекта Федерального резервного банка Бостона и Массачусетского технологического института по изучению ЦВЦБ США (Project Hamilton) разработана система, которая разделяет проверку операции на этапы, и на каждом этапе требуется доступ к различным частям данных об операции.

Эти криптографические методы могут быть расширены еще больше для создания систем, которые проверяют правомерность операций только с помощью зашифрованного доступа к таким сведениям о транзакции, как отправитель, получатель или сумма. Хотя эти инструменты кажутся неправдоподобными, они прошли широкую проверку на криптовалютах, сохраняющих конфиденциальность, таких как Zcash, и в их основе лежат значительные достижения в криптографическом сообществе. Суть в том, что технология позволяет центральным банкам обеспечить гарантии как кибербезопасности, так и защиты конфиденциальности в любом проекте ЦВЦБ.

Прозрачность и конфиденциальность

Общей проблемой с проектами, обеспечивающими сохранение конфиденциальности (включая те, которые используют специализированные криптографические методы), является снижение прозрачности для регулирующих органов. Регулирующим органам, как правило, требуется достаточно большой объем информации для определения подозрительных операций, что позволяет им выявлять случаи отмывания денег, финансирования терроризма и другой незаконной деятельности.

Но даже это не является вопросом выбора. Криптографические методы могут быть использованы для разработки ЦВЦБ,

ФОТО: FUNTAP VIA GETTY IMAGES

Потребность в установлении международных стандартов и расширении обмена знаниями между банками имеет решающее значение в этот период быстрого развития и внедрения.

которые обеспечивают конфиденциальность, подобную наличным деньгам, до определенного порога (например, 10 000 долларов США), позволяя государственным органам осуществлять достаточный надзор со стороны регулирующих органов. Такой порог не сильно отличается от нынешней системы в США, которая позволяет сократить отчетность по операциям до 10 000 долларов США. На самом деле во многих отношениях в новой системе ЦВЦБ не нужно заново изобретать протоколы безопасности, а вместо этого можно их усовершенствовать.

Несколько стран обязались создать или даже уже запустили розничные ЦВЦБ, базовая инфраструктура которых основана на технологии распределенного реестра. Нигерийская eNaira, запущенная в октябре 2021 года, является хорошим примером. Такие проекты требуют привлечения третьих сторон в качестве агентов проверки операций. Это вводит новую роль для третьих сторон (например, финансовых и нефинансовых учреждений) в денежных операциях центрального банка. Критически важно, что гарантии безопасности реестра будут зависеть от беспристрастности и доступности сторонних агентов проверки, над которыми центральный банк может не иметь прямого контроля. (Хотя технологию распределенного реестра возможно реализовать со всеми агентами проверки, контролируемыми центральным банком, это в значительной степени противоречит цели использования технологии.) Связанные с этим риски потенциально могут быть снижены посредством регулирующих механизмов, таких как требования о проведении аудита и строгие требования к раскрытию информации о нарушениях. Тем не менее нет четкого плана для разработки этих правил в системе, столь же ограниченной по времени и тесно взаимосвязанной, как ЦВЦБ на основе распределенного реестра. Вот почему потребность в установлении международных стандартов и расширении обмена знаниями между банками имеет решающее значение в этот период быстрого развития и внедрения.

Угроза или возможность?

За последние 18 месяцев некоторые центральные банки преждевременно решили, что ЦВЦБ создает слишком много рисков для кибербезопасности и конфиденциальности. Мы хотели определить, что на самом деле является угрозой, а что по факту является возможностью. Мы пришли к выводу, что у органов государственного управления есть широкий выбор вариантов проектов ЦВЦБ, включая новые варианты, которые еще не были полностью протестированы в текущих пилотных проектах центральных банков. Эти варианты представляют различные компромиссные решения с точки зрения производительности, безопасности и конфиденциальности. Органам государственного управления следует выбирать вариант проекта, исходя из потребностей страны и приоритетов в области экономической политики. Согласно нашей оценке этих компромиссных вариантов, ЦВЦБ по своей сути не являются более или менее безопасными, чем существующие системы. Хотя ответственные подходы должны принимать во внимание кибербезопасность, это не должно препятствовать рассмотрению вопроса о том, следует ли вообще разрабатывать и тестировать ЦВЦБ.

Одно совершенно ясно в наших исследованиях. Разрозненные международные усилия по созданию ЦВЦБ, вероятно, приведут к проблемам совместимости и трансграничным киберугрозам. По понятным причинам страны сосредоточены на внутреннем использовании, при этом слишком мало внимания уделяется трансграничному регулированию, функциональной совместимости и установлению стандартов. Независимо от того, решат ли США, как эмитенты основной мировой резервной валюты, запустить ЦВЦБ, Федеральная резервная система должна помочь в руководстве процессом разработки глобальных основ регулирования ЦВЦБ в организациях, устанавливающих стандарты. Международные финансовые форумы, включая Банк международных расчетов, МВФ и Группу 20-ти, призваны сыграть столь же важную роль.

Риски для кибербезопасности и конфиденциальности, связанные с ЦВЦБ, реальны. Однако решения этих проблем находятся в пределах досягаемости специалистов по технологиям и директивных органов. Было бы прискорбно заранее решить, что риски слишком высоки, прежде чем разработать решения, которые могли бы реально помочь создать более современную и стабильную глобальную финансовую систему. ФР

ДЖОШ ЛИПСКИ — старший директор Центра геоэкономики Атлантического совета и бывший сотрудник МВФ. **ОЛЕ МОЕР** — научный сотрудник Центра геоэкономики Атлантического совета. **ДЖУЛИЯ ФАНТИ** — старший научный сотрудник Центра геоэкономики Атлантического совета и доцент кафедры электротехники и вычислительной техники в Университете Карнеги-Меллона.