Альтернативная финансовая система. Начало

Тренды и вызовы в деятельности операторов информационных систем, необходимость создания отраслевых стандартов безопасности

Текст
АНАТОЛИЙ ПОЛТАВСКИЙ,
ОСНОВАТЕЛЬ ГРУППЫ КОМПАНИЙ «МАДРИГАЛ», К.Э.Н.



«Война — это мир», — написал Джордж Оруэлл. «Мир — это война», можно перефразировать его. Глобальные события, которые мы наблюдаем в последние несколько лет, кардинально меняют наше представление о мире, в частности о мире финансов.

Мы находимся на этапе зарождения новой социально-экономической формации. Цифровизация всех отраслей экономики, роботизация, повсеместное внедрение алгоритмов машинного обучения с замещением базового интеллектуального труда человека, формирование альтернативных финансов — все это приводит к оптимизации/сокращению ресурсной составляющей экономики. Развитие носит революционный характер, и стремительность требует быстрой и эффективной адаптации экономики и общества.

Цифровые финансовые активы (ЦФА) и деятельность операторов информационных систем (ОИС) — это формирование альтернативной, но в перспективе просто новой финансовой системы. Так или иначе, ЦФА и цифровой рубль в среднесрочной перспективе (три — пять лет) в значительной степени заменят «классическую» финансовую систему. Актуальность брокеров, депозитариев, банков (в классическом представлении) сведется к минимуму. С развитием и внедрением

цифрового рубля, появлением различных форм «цифрового» кредита и депозита по типу персонализированных долговых ЦФА изменится и банковский рынок.

Деятельность ОИС построена на технологии блокчейн; по сути, это СУБД, разделенная на несколько частей и объединенная алгоритмами шифрования. Данная технология на порядок эффективнее, быстрее, безопаснее и надежнее «классических» решений учета, хранения информации и управления ею. Однако большое внимание к этой технологии позволило выявить (и выявлять далее) ряд уязвимостей непосредственно в архитектуре некоторых решений. Например, перехват и подмена информации в момент синхронизации узлов блокчейна, SQL-инъекции с подменой данных и некоторые другие. Необходимо принять во внимание развитие перспективной технологии квантового дешифрования на горизонте трех-четырех лет, защиты от которой на практике сейчас нет. Сама система неавтономна и требует разворачивания сложной и дорогой базовой инфраструктуры, которая подвержена стандартным угрозам безопасности.

Информационная безопасность (ИБ) в данном направлении обрела совершенно иные границы, это «краеугольный камень» всей отрасли. Уровень технологичности и ожидаемый масштаб деятельности ОИС превосходит «эталон» современного финансового рынка — банк. Обращаемся к требованиям регулятора, который на данный момент делит рынок на кредитные и некредитные организации, а уровень защищенности в зависимости от размера бизнеса — на минимальный и стандартный. ОИС является некредитной финансовой организацией (НКО) и должен соблюдать соответствующие требования ГОСТ Р 57580.1, положений Банка России 757-П и 779-П с минимальным уровнем защиты (п. 1.4.4 757-П), при этом стандартный уровень защиты не отражает специфику бизнеса. Требования к защите информации занижены. Необходима большая совместная работа участников рынка и регулятора для создания соответствующих надежных и эффективных отраслевых стандартов безопасности. Ниже приведены некоторые примеры.

Сложность и дороговизна инфраструктуры популяризовали на рынке решение по разворачиванию системы в облаке. Подобное решение несет экзистенциальные риски существованию ОИС и сохранности данных. Во-первых, взлом/угон учетной записи облачного ресурса и полная потеря контроля над системой без возможности оперативного восстановления как учетной записи, так и данных. Во-вторых, целевая DDOS-атака на ОИС в облаке, если угроза существенна для самого провайдера, ОИС просто заблокируют. В-третьих, работа с облаком — это дополнительные каналы связи и как следствие дополнительные уязвимости, возможны перехват и подмена данных. В-четвертых, ограничение в масштабируемости бизнеса, так как облачные провайдеры из-за особенностей архитектуры ограничивают предельный размер арендуемых ресурсов. Поэтому необходимо использование ОИС собственной инфраструктуры, частично дополненной облачной (узел верификации, Backup). Это должно стать базовым отраслевым стандартом.

Что касается вопроса импортозамещения в финансовом секторе, при всем скепсисе участников рынка относительно отечественных продуктов (мнение, что это всего лишь перелицованные opensource-решения), данные продукты, как правило, имеют глубокую аналитику исходного кода и исключают большинство критических уязвимостей, что существенно повышает уровень безопасности. Использование коммерческого системного ПО из недружественных государств существенно снижает уровень защиты и операционной надежности ОИС, возможен несанкционированный доступ к инфраструктуре, обновление безопасности в санкционных условиях не осуществляется. Текущие требования законодателя и регулятора ко всем финансовым организациям дают возможность до 01.01.2030 (переходный период, Постановление Правительства РФ № 1912 от 14.11.2023) использовать импортное ПО и оборудование, за исключением средств защиты (до 01.01.2025 — Указ Президента РФ № 250 от 01.02.2022). Рынок только формируется, и рационально для данной отрасли ввести требование о максимальном импортозамещении на старте, определить порядок и объем в соответствующем отраслевом стандарте.

Многие участники рынка уже сейчас используют партнерские взаимоотношения для верификации узлов блокчейна, что в случае киберинцидента позволит восстановить целостность системы. Данная практика должна лечь в основу отраслевого стандарта.

Полностью обеспечить ИБ инфраструктуры ОИС (как и любой другой критической инфраструктуры) нельзя, но можно снизить риски и величину потенциального ущерба.

В условиях беспрецедентного санкционного давления, в которых сейчас находится Россия, встал вопрос об ускорении цифровой трансформации, в частности, финансового сектора, о создании новой независимой финансовой системы. Проблемы, которые возникают при осуществлении международных расчетов, побудили законодателя в ускоренном режиме легализовать новые формы платежей, используя ЦФА. Одновременно это поставило под прицел недружественных стран всех ОИС, как с точки зрения перманентного санкционного давления, так и с позиций возможного усиления кибератак и их направления для исключения в корне появления альтернативной системы. Здесь также актуальна совместная работа участников рынка и регулятора для выработки общих принципов существования этой альтернативной системы расчетов и ее безопасности. В качестве решения возможно создание на базе ОИС расчетного консорциума для осуществления внешнеэкономической деятельности с набором различных ЦФА от разных операторов и единой системы платежных агентов для распараллеливания денежных потоков.

Новый формирующийся рынок и глобальная цифровая трансформация требуют совершенно иных подходов к коллективной безопасности, выработки единых отраслевых стандартов, появления информационного и расчетного консорциумов (не путаем с СРО). Б.О

реклама