Платформа SICP для отслеживания подозрительных транзакций и обеспечения безопасности блокчейнов

Александр Подобных, *независимый эксперт по ИБ в SICP.ueba.su*

22 июля 2020 г. Государственная Дума приняла в третьем чтении закон “О цифровых финансовых активах”, новые правила вступят в силу с 1 января 2021 г. К концу 2020 г. ожидается рассмотрение закона “О цифровой валюте”, в 2019 г. были приняты закон “О цифровых правах” и закон “О привлечении инвестиций с использованием инвестиционных платформ”. Таким образом, с начала 2021 г. в России будет осуществляться идентификация владельцев цифровых активов, внедряться скоринг транзакций и реализовываться мониторинг криптовалютных транзакций.

Уже и классические финансы тяготеют к сфере электронных и цифровых валют, о чем свидетельствуют совсем недавно принятые закон "О национальной платежной системе" и положение Банка России 719-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств".

Сфера криптовалют технически более сложна, чем традиционные финансы, заметно более децентрализована и менее контролируема. Поэтому требуются инструменты, помогающие использованию криптовалют в законном ключе и для законных целей.

Традиционная задача UEBA заключается в своевременном обнаружении целевых атак и инсайдерских угроз. Классические решения UEBA обрабатывают большой объем данных из различных источников, определяют нормальные модели поведения для каждого пользователя и объекта и уведомляют ИБ-специалистов, если замечают отклонения от этих моделей.

Но сфера криптовалют технически более сложна, чем традиционные финансы, заметно более децентрализована и менее контролируема. Поэтому требуются инструменты, помогающие использованию криптовалют в законном ключе и для законных целей.

Основой платформы можно считать возможность оценки криптовалютных кошельков и транзакций с помощью динамического скоринга.

SICP

Платформа SICP[1] уже более двух лет разрабатывается и совершенствуется группой экспертов из различных отраслей – экономической безопасности, информационной безопасности, форензики, финтеха, рисков и аудита. В настоящее время эта работа происходит на базе отдела специальных разработок Технопарка Санкт-Петербурга, созданного для взаимодействия по модели государственно-частного партнерства.

Изначально платформа SICP создавалась как реализация технологии UEBA (User and Entity Behavior Analitics) и основывалась на выявлении киберугроз криптокошелькам с учетом поведения пользователей, устройств, приложений и объектов в информационной системе.

Однако очень быстро проект перерос в разработку собственных методов и методик анализа транзакций и оценки криптовалютных кошельков.

Основой платформы можно считать возможность оценки криптовалютных кошельков и транзакций с помощью динамического скоринга. Всего в системе определены пять уровней риска, от низкого до критического, они соотнесены с CIS Controls 7.1. и визуализируются в SICP подсветкой от зеленого до красного цветов.

Политика безопасности платформы SICP учитывает положительный опыт CIS в сфере управления активами, передовых методов защиты от кибератак и повышения эффективности программы кибербезопасности.

Сервисы в составе SICP

На платформе SICP доступны четыре сервиса: СмартЭхо, КриптоСонар, МетаСфера и КриптоЦЕРТ.

1. Сервис СмартЭхо предназначен для оценки рисков криптокошелька или транзакции в блокчейне и позволяет получить сведения об объемах средств в различные временные периоды. Пользовательские отметки являются важной частью сервиса, они учитываются при скоринге наряду с основными факторами риска.

2. Сервис КриптоСонар предназначен для визуального исследования транзакций, а также для отображения анализируемых кошельков и других известных субъектов.

3. Сервис МетаСфера предназначен для анализа пула криптовалютных кошельков по внутренним тегам, включая количество транзакций, объем отправленных и полученных средств в различных валютах. Могут использоваться как общие внутренние теги, так и скрытые, специальные, доступ к которым имеют только исследователи, эксперты или ограниченные рабочие группы.

В сервисе МетаСфера ведутся черные и белые списки, статистика по использованию средств, учитываются вопросы различных юрисдикций, визуализируются профили подозрительных адресов.

4. О сервисе КриптоЦЕРТ (CryptoCERT) расскажем более подробно.

[1] *Security Intelligence Cryptocurrencies Platform (SICP), или в русскоязычном варианте когнитивная система аналитики Транзакция Криптовалюта Актив (КосаТКА), sicp.ueba.su.*

КриптоЦЕРТ

В конце июля 2020 г. командой SICP был анонсирован запуск КриптоЦЕРТ, первого российского коммерческого центра мониторинга криптовалютных транзакций, решающего задачи выявления рисков криптокошельков и реагирования на инциденты в сфере оборота криптовалют. Это первый подобный сервис, работающий в России и странах СНГ. Любой гражданин или организация могут направить в КриптоЦЕРТ сведения о мошенничестве, связанном с криптовалютами, а также о другой угрозе или риске. На общедоступной интерактивной карте отображаются отпрофилированные криптокошельки в разрезе по странам.

Платформа КриптоЦЕРТ не только позволяет вести мониторинг финансовых операций в блокчейн-системах и проводить исследование сущностей, но и предоставляет обширный функционал мониторинга нод блокчейнов, автоматизированного аудита субъектов, анализа защищенности веб-сервисов и аудита смарт-контрактов.

Непрерывно ведутся работы по совершенствованию авторских алгоритмов динамического скоринга (настраиваемая поверхность скоринга), выявлению мошенников, усиливается интеграция с модулями машинного обучения, а также искусственного интеллекта, ведутся тестирования и исследования в данной области. Более того, платформа SICP поддерживает различные модели скоринга с возможностью их быстрой загрузки для использования в различных юрисдикциях с учетом требований локальных регуляторов.

КриптоЦЕРТ осуществляет неформальное взаимодействие с ФинЦЕРТ Центробанка России. Это сотрудничество планируется продолжить, несмотря на структурные изменения в Центробанке, и даже расширить за счет документального, а затем и законодательного закрепления процедур взаимодействия.

В настоящее время ведутся переговоры с регуляторами по обучению и применению платформы КриптоЦЕРТ в рамках работы в сфере оборота виртуальных активов и цифровых финансовых активов, проводятся консультации по вопросам налогообложения.

Взаимодействие с федеральными органами исполнительной власти осуществляется посредством заключения соглашений о взаимодействии и соглашений о неразглашении. По запросу федеральных органов исполнительной власти и ассоциации судебных экспертов командой SICP прорабатывается вопрос хранения во внутреннем блокчейне доказательств с контрольными суммами для возможности верификации юридически значимых доказательств из любой точки мира.

На настоящий момент налажено неформальное взаимодействие КриптоЦЕРТ с другими аналогичными платформами и антифрод-системами в Европе, Южной Корее, США.

Мы отмечаем заинтересованность в КриптоЦЕРТ со стороны банков, страховых компаний, инвестиционных фондов, криптовалютных бирж, платежных шлюзов, силовых ведомств, нотариусов и оценщиков.

Правовой фон работы SICP

Не секрет, что основная системная проблема, связанная с использованием криптовалют, заключается в возможности их применения для проведения незаконных операций, в частности для легализации криминальных доходов, а также для финансирования запрещенных видов деятельности.

Наиболее значимым в России законом в части противодействия отмыванию преступных доходов является 115-ФЗ "О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма".

В 2018 г. Советом ЕС была принята директива, регулирующая европейские правила по предотвращению отмывания денег и финансирования терроризма. Эти правила являются пятым по счету и последним обновлением Европейской "антиотмывочной" директивы, за что и получили условное название The Fifth Anti-Money Laundering Directive, или 5AMLD. В свете этой директивы уже с начала 2020 г. у субъектов должны быть внедрены процедуры KYC (Know Your Customer) и AML/CFT (Anti-Money Laundering, Counter-Terrorist Financing), и многие компании в Европе уже используют эти инструменты с 2019 г.

Практически все ведущие криптобиржи и процессинговые сервисы внедрили стандарты ISO/IEC 27001, равно как и GDPR, KYC-политики или сторонние решения, AML/CFT-сервисы и процедуры. Тяготеющие к американским финансовым рынкам компании также прошли аудит SOC2 (Service and Organization Controls 2).

Угрозы и защита

Защита должна быть направлена на все компоненты цифрового актива – информационный, экономический, стоимостный, правовой. Стоит выделить следующие основные риски цифровых финансовых и виртуальных активов: доступность блокчейнов, целостность смарт-контрактов, конфиденциальность ключевой информации.

Существуют и дополнительные угрозы и риски, касающиеся цифровых активов:

- увеличение поверхности угроз, влияющих на все отрасли экономики;
- лавинообразный рост мошенничества из-за неосведомленности граждан;
- доступность для противоправных действий и высокотехнологичных преступлений;
- бесконтрольный транзит средств между юрисдикциями;
- отсутствие унифицированного подхода к регулированию и налогообложению;
- проблемы идентификации и аудируемости сайдчейнов, анонимных криптовалют, приватных смарт-контрактов;
- излишняя централизация или избыточная децентрализация, санкции.

SICP обеспечивает операционную, транзакционную безопасность и реализацию следующих процедур:

- идентификация/верификация (KYC);
- дью-дилиджанс пользователей и компаний (DD);
- ответственное должностное лицо (CCO);
- мониторинг транзакций (KYT);
- оценка рисков AML/CFT;
- учет страновых рисков.

И несомненно, стоит отметить тот факт, что сегодня к квалификационным требованиям к ИБ-специалистам финансовой сферы добавляется обязательное наличие навыков анализа больших данных и оптимизации алгоритмов машинного обучения. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru

Основная системная проблема, связанная с использованием криптовалют, заключается в возможности их применения для проведения незаконных операций, в частности для легализации криминальных доходов, а также для финансирования запрещенных видов деятельности.

Практически все ведущие криптобиржи и процессинговые сервисы внедрили стандарты ISO/IEC 27001, равно как и GDPR, KYC-политики или сторонние решения, AML/CFT-сервисы и процедуры.

Сегодня к квалификационным требованиям к ИБ-специалистам финансовой сферы добавляется обязательное наличие навыков анализа больших данных и оптимизации алгоритмов машинного обучения.