У нас длинные руки

Два года назад «Б.О» утверждал, что форензик* не является научной дисциплиной, поскольку нет количественных закономерностей, объясняющих развитие системы в пространстве и времени. А вот сейчас ситуация изменилась



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Мнение «Б.О» базировалось тогда на беседе **Сергея Петренко,** директора по информационной безопасности (CISO) Университета «Иннополис», и **Михаила Смирнова,** главного редактора Ассоциации по вопросам защиты информации BISA.

В то время в ИБ невозможно было создать «модель конфликта», позволяющую теоретически вывести закономерности. Единственная возможность — кропотливый и долгий сбор статистики. Поэтому нормативная документация покрывает лишь базовый уровень ИБ, а повышенный уровень приходится «закрывать» методами управления рисками.

Прошло каких-то два года, помноженных на коэффициент условий кибервойны. Многократно возросший поток ИБ-статистики вкупе с развитием ИИ, который позволил обработать огромные массивы данных, помогли преодолеть дистанцию, отделявшую долгое время форензик (науку об исследовании ИБ-доказательств) от классической криминалистики. Главное здесь то, что форензик приобрел новое применение в качестве real-time аналитического инструмента в области AML, комплаенса и финансовой разведки.

Прозрачная «крипта»

Судить о реальных возможностях отечественного форензика, по понятным причинам, можно лишь по косвенной информации — спецслужбы не любят раскрывать свои тайны. Тем не менее кейсов (пускай и иностранных), по которым можно оценить развитие этой дисциплины, уже достаточно.

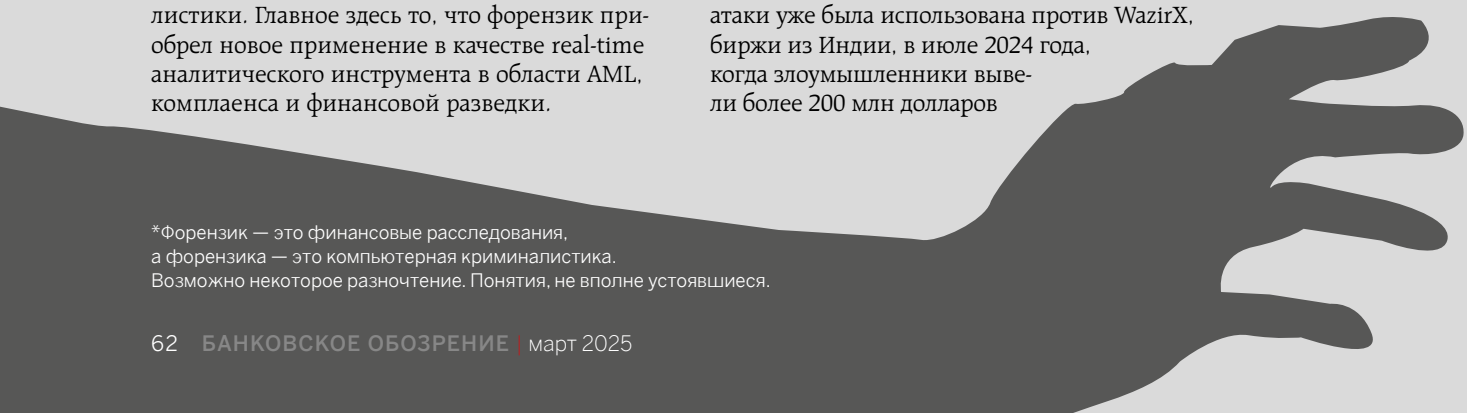
Мир становится все более и более открытым для расследований. Как ни парадоксально, но обеление происходит из-за особенностей криптовалют, которые часто используют в противоправных целях. А зря! Блокчейны, на которых они базируются, открыты для всех.

Например, это подтверждает красноречивый кейс февраля 2025 года, когда криптобиржа Bybit сообщила о взломе одного из своих холодных кошельков Ethereum, с которого было выведено более 1 млрд долларов в ETH и других активах. Первым на подозрительные транзакции обратил внимание криптодетектив ZachXBT — он зафиксировал перевод крупных сумм с кошельков Bybit. CEO биржи **Бен Чжоу** подтвердил атаку и объяснил, что злоумышленники использовали сложный метод подмены транзакции (по сути — взлом с фишингом), который позволил им получить полный контроль над активами.

На основании этих заявлений можно сделать вывод о том, что мир «крипты» успешно обзавелся всей той ИБ-инфраструктурой, которая характерна для мира «фиата». В частности, успешно заработали форензик-сервисы, что было бы невозможно без налаживания полноценных KYC- и AML-процедур.

Как проявилась эта работа на практике? Сервисы мониторинга блокчейна довольно быстро обработали телеметрию и успешно начали маркировать эти кошельки как потенциально скомпрометированные, что позволило иным криптобиржам отслеживать пути движения похищенного и в соответствии со своими политиками безопасности реагировать.

Это дало и время, и пищу для анализа данного инцидента экспертами и детективами, которые установили, что методика такой атаки уже была использована против WazirX, биржи из Индии, в июле 2024 года, когда злоумышленники вывели более 200 млн долларов



*Форензик — это финансовые расследования, а форензика — это компьютерная криминалистика. Возможно некоторое разночтение. Понятия, не вполне устоявшиеся.

в криптовалюте. Тогда расследование связало атаку с северокорейской хакерской группировкой Lazarus, которая специализируется на кибератаках на криптовалютные платформы. Дальше — дело техники и Интерпола.

Что касается последних новостей из нашей страны, то Росфинмониторинг планирует до конца 2025 года подключить российские банки к сервису «Прозрачный блокчейн», который позволит выявлять связи проводимых банковскими клиентами операций с фиатными деньгами и с криптовалютой. Об этом 21 февраля 2025 года заявил **Антон Лисицын,** заместитель директора этой службы, на Уральском форуме «Кибербезопасность в финансах 2025».

Зачем это нужно? По данным финансовой разведки, с 2022 года количество связанных с криптовалютой подозрительных транзакций значительно выросло. Это привело к увеличению числа уголовных дел и активизации финансовых расследований. Сейчас сервисом пользуются более 12 тыс. специалистов, в том числе сотрудники правоохранительных органов и подразделений антиотмывочной разведки стран СНГ.

«Классика» вечна

Расширяется и практика проведения классических форензик-расследований ИБ-инцидентов. Богатую пищу для размышлений аналитиков принесла восьмая ежегодная конференция Moscow Forensics Day по цифровой криминалистике и информационной безопасности, прошедшая в сентябре 2024 года.

Понятно, что деанонимизация мессенджера Telegram превратила его в клондайк для форезников. Выступление **Игоря Бедерова,** руководителя департамента киберрасследований компании T.Hunter, раскрыло некоторые секреты Полишинеля. По его словам, «ключи шифрования Telegram — это во многом аллегория. Они могут представлять собой банальнейшее соглашение, даже понятийное, между **Павлом Дуровым** и иностранными спецслужбами, предполагающее допуск последних к инфраструктуре мессенджера. Скажу откровенно, французское Сюртэ — это не ФСБ, и их явно не удовлетворит связка металлических ключей, отправленная по почте».

В итоге Telegram стал, по сути, игрушкой в руках французских спецслужб и даже начал показательно сотрудничать с Международным фондом наблюдения за интернетом (Internet Watch Foundation, IWF) для борьбы с распространением материалов о сексуальном насилии над детьми. Павел Дуров заявил о намерении превратить подход к модерации Telegram из предмета критики в пример для подражания. Так и хочется процитировать классика применительно к будущим разоблачениям: «О сколько нам открытий чудных»… Они могут даже затмить откровения **Эдварда Сноудена** и **Джулиана Ассанджа.**

А о том, как на практике форензики и специалисты в области OSINT могут это сделать, намекнула **Ольга Тушканова,** представитель Научно-исследовательского института криминалистики Главного управления криминалистики Следственного комитета. Другой важный вопрос, поднятый ей, касается доморощенных диванных исследователей, которым вдруг станут доступны огромные массивы чувствительной информации. Поэтому силовые ведомства страны крайне беспокоят ошибки неквалифицированных экспертов, проводящих экспертизы,

О возможной судьбе Telegram можно судить на основе показательной новости начала февраля 2025 года: Интерпол в сотрудничестве с силовыми структурами шести европейских государств провел спецоперацию, в рамках которой была ликвидирована служба обмена зашифрованными сообщениями MATRIX. Отмечается, что на протяжении трех месяцев спецслужбы в режиме реального времени отслеживали переписку членов организованных преступных группировок.

Психология на службе киберкриминалистики

Что касается будущего форензика, то о нем сейчас можно услышать в самых неожиданных местах. Например, в дискуссиях психологов или на мероприятиях для ИБ-директоров банков. Одно из перспективных направлений развития связано с изучением психологии хакеров и инсайдеров во взаимосвязи с общей теорией психотипов коррупционеров и т.д., что приближает форензик уже к службам банковского и антикоррупционного комплаенса во исполнение 273-ФЗ от 2008 года. Об этом было ярко заявлено в ходе круглого стола по комплаенсу на XXI Международном банковском форуме, прошедшем осенью 2024 года.

Очевидно, что киберкриминалистика может помочь, например, в идентификации фальшивых доверенностей на совершение операций с использование электронных средств платежа (ЭСП). В своей массе это доверенности сроком до одного года на открытие счетов и совершение операций в крупных кредитных организациях. Найдет свое место она и в разработке и оттачивании Росфинмониторингом типологий мошеннических схем.

А вот психологи говорят в контексте форензика о взаимосвязи личностных качеств «темной триады» с кибербуллингом, эмпатией и эмоциональным интеллектом на базе моделирования структурных уравнений. Б.О

