

Генеральный директор компании «Фаззи Лоджик Лабс» Лилия Шароватова рассказала «Б.О» на полях форума «Кибербезопасность в финансах 2026» о наиболее острых проблемах и трендах антифрод-индустрии

**Лилия Шароватова («Фаззи Лоджик Лабс»):**

# Необходимо совместное принятие ответственности



Текст

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

— Лилия, что представляет собой Cybercrime-as-a-Service (CaaS)? Когда эксперты рынка начали говорить об этом феномене?

— CaaS — это модель «киберпреступность как сервис», когда преступные группы продают или сдают в аренду «под ключ» инструменты, инфраструктуру и даже исполнителей для проведения мошеннических операций как за подписку, так и за разовую плату или процент.

В «пакет услуг» обычно включают готовые решения для фишинга, панели управления, базы данных и различные виды доступов, специализированные прокси- и антидетект-решения, механизмы массового создания аккаунтов («фарм»), помощь посредников («дропов/мулов») в операциях по выводу средств, разработку и реализацию финансовых схем, а также образовательные курсы и техническую поддержку.

Как об устойчивом рыночном тренде о CaaS стали говорить примерно с конца 2000-х, хотя отдельные элементы «мошенничества как сервиса» существовали раньше.

— Банк России в Обзоре основных типов компьютерных атак в финансовой сфере в 2025 году от 13 февраля 2026 года пишет о 50%-ном росте ransomware-as-a-service атак за год. Много спорят и о DDoS as a Service. Можно ли говорить о тотальном переходе злоумышленников на сервисную модель?

— По моему убеждению, о тотальном переходе злоумышленников на сервисную модель говорить некорректно. Скорее, мы наблюдаем устойчивую автоматизацию киберпреступности: многие инструменты и этапы атаки все чаще покупают как услугу, что снижает порог входа и позволяет быстро масштабировать кампании.

Для массовых и тиражируемых сценариев сервисная модель действительно стала одной из ключевых, поскольку есть разделение ролей, «партнерки», готовая инфраструктура и поддержка. Это увеличивает число инцидентов даже без пропорционального роста ядра опытных атакующих.

Но часть поставщиков первичного доступа — особенно в целевых, высокоценных или политически чувствительных операциях — сохраняют закрытые цепочки и критические компетенции внутри, чтобы контролировать риски и не зависеть от внешних подрядчиков. Поэтому правильнее говорить о гибридной экосистеме, где сервисы усиливают и ускоряют атаки, но не заменяют всех злоумышленников.

— Вследствие развития каких технологий CaaS стал возможен технически и экономически выгодным? Какова при этом типичная «продуктовая линейка» мошенников?

— CaaS стал возможен из-за ряда факторов: доступности недорогих облачных сервисов и виртуальных серверов (VPS), технологий анонимизации трафика (VPN, Tor, защищенного хостинга), развития мессенджеров и распространения криптовалют.

Это привело к возникновению специализированных теневых площадок с системой рейтингов продавцов и арбитражем споров. Появились конструкторы и панели для автоматизации, инструменты обхода антифрода (антидетект-браузеры, прокси, эмуляторы), VoIP для дешевых обзвонков на фоне массы утекших персональных данных. Все это значительно снизило стоимость входа, повысило скорость развертывания схем и облегчило ведение преступной деятельности в формате «мошенничество как услуга».

Типичная продуктовая «линейка» включает в себя привлечение жертв (Phishing-as-a-Service, рассылка спама, звонки из колл-центров), взлом учетных записей (перепродажа логинов, кража одноразовых кодов), маскировку следов преступления (создание фальшивых профилей, использование спецбраузеров и прокси) и вывод денежных средств (кардеры, специалисты по обналачиванию). Дополнительно предлагаются инфраструктура, включая серверы и домены, поддельные документы, обход КУС-проверок, а также детальные инструкции по проведению махинаций.

— Почему традиционные контуры защиты проигрывают, как говорят в шахматах, темп?

— Потому что защита тоже должна стать платформенной! Нам нужны сборная экосистема из модулей (идентификация, мониторинг, аналитика, отклик), общие данные и быстрые интеграции — чтобы включать нужные блоки под задачу и масштабировать их как сервис. На данный момент мы видим несколько проблем: бюрократия на местах, законодательные требования и, в большинстве своем, межотраслевая разрозненность. Время от сигнала до блокировки остается слишком большим.

Антифрод в рамках предложенной модели функционирует как непрерывный поток обработки данных в режиме реального времени. Процесс начинается со сбора телеметрии, включая информацию об устройстве, сети и поведении пользователя. Затем осуществляется оценка уровня риска посредством сочетания заранее установленных правил и машинного обучения (ML). Завершающим этапом становится оркестровка необходимых мер реагирования: дополнительные проверки, ограничение транзакций или полная блокировка подозрительных операций.

Основные проблемы, возникающие в ходе реализации подобной схемы, связаны с социальной инженерией, низким качеством процедур идентификации (КУС) и подделками документов, недостаточным уровнем качества исходных данных, а также необходимостью поддержания оптимального баланса между обеспечением безопасности и сохранением удобства пользователей.

— Встает вопрос, а не должна ли защита тоже стать платформенной индустрией? И где сейчас в ней слабое звено? Как выглядит антифрод как часть потенциальной индустрии ИБ?

— ИБ как индустрия должна начинаться с унификации как базового слоя, примером чего является ГИС АНТФРОД — первый шаг государства к созданию общих правил и единого стандарта антифрода. Вместо подхода «каждый сам за себя» предлагается внедрение индустриального контура с платформой, процессами и метриками, обеспечивающими одинаковое масштабирование защиты для всех участников рынка, независимо от размера бизнеса. Автоматизация рутинных операций, таких как скоринг, снижает нагрузку на сотрудников, оставляя специалистам наиболее сложные случаи и контроль качества.

Однако важно помнить, что качество данных имеет первостепенное значение: модели, обученные на неполных или искаженных данных, приводят к систематическим ошибкам, которые невозможно устранить исключительно «прогоном через ИИ». Для эффективного функционирования системы необходим цикл контроля качества, включающий в себя проверку точности данных, постоянный мониторинг изменений, оценку ошибок, в том числе ложноположительных и ложноотрицательных срабатываний, обеспечение прозрачности и своевременную перенастройку алгоритмов. Иначе индустриализация превращается в масштабирование ошибок.

— Очевидно, что защита должна работать в режиме реального времени. Можно ли этого добиться без ML в антифроде? А с помощью чего еще?

— Реал-тайм в антифроде обязателен, и он существовал всегда. Например, авторизации и стоп-листы работали еще в XX веке: платежные карточки международной платежной системы VISA впервые были выпущены в нашей стране в 1988 году. Но сегодня резко увеличились и скорость атак, и их поверхность, поскольку приходится мониторить мобильные и онлайн-каналы, а также облачные сервисы. Кроме того, появился разнообразный инструментарий по деанонимизации атакующих, который также обязан работать в режиме реального времени.

В итоге старых правил и «ручных» проверок уже недостаточно. Поэтому реал-тайм как класс требований давно стал нормой, особенно в карточных сценариях — ответы от системы требуются в пределах сотни миллисекунд. Новизна сейчас — не в самом реал-тайме, а в количестве каналов и событий, которые необходимо обрабатывать и «склеивать» между собой в рамках типичного договора SLA, а также в том, что мошенничество уходит в более сложные цепочки сценариев, включающих в себя несколько шагов, сущностей и систем.

В свете сказанного ML в антифроде — уже не «фишка», а базовый технологический слой. Но, к сожалению, многие крупные игроки отрасли упираются в потолок качества на внутренних данных и начинают искать внешние сигналы. При этом скорость и объем данных сами по себе не гарантируют результата — важны качество сигналов, объяснимость, управление ошибками и правильная сборка цепочек событий.



Фото: «Б.О.» Ирина Анисина

— Но при этом человек все равно останется слабым звеном? Что с этим можно поделать? Может, предложить пользователям некие экономические стимулы для повышения бдительности?

— Человек действительно остается самым уязвимым звеном: социальная инженерия масштабируется, а когнитивные ограничения и поведенческие паттерны — нет. Поэтому атаки все чаще нацелены не на «взлом системы», а на «взлом решения человека».

Чем антифрод-система может с организационно-технологической точки зрения помочь в сложившейся ситуации? Можно предложить, например, четыре группы мер.

Во-первых, важно по умолчанию устанавливать, где только возможно, безопасные настройки и внедрять интеллектуальные механизмы сопротивления атакам: адаптивную многофакторную аутентификацию (риск-адаптивная MFA), лимиты и временные задержки на нетипичные переводы, «охлаждение» перед переводом на новый счет.

Во-вторых, необходима своевременная помощь пользователям прямо в момент совершения действия: сценарии предупреждения об угрозах фишин-

га, четкие экраны подтверждения переводов, обязательный обратный звонок банку при крупных или необычных операциях. Мы можем твердо заявить, что такое подтверждение, как, например, «Вы говорите с оператором?» или «Вас просили установить удаленный доступ?», дает немедленный отрезвляющий эффект на подверженных влиянию людей.

В-третьих, защита должна охватывать каналы связи и используемые устройства: жесткая фиксация устройств, использование безопасного чата и звонков непосредственно внутри приложений, автоматический мониторинг попыток подключения сторонних утилит, эмуляторов и запуска виртуальных сред.

В-четвертых, важную роль играет принцип совместной ответственности: простые правила возмещения или компенсации убытков клиентам, соблюдавшим базовые правила безопасности: например, не устанавливавшим удаленные сервисы управления устройствами и не передававшим одноразовые пароли. Такой подход снимает психологические барьеры, уменьшает чувство вины пострадавших и стимулирует их своевременно сообщать о случившихся инцидентах.

Что касается экономических стимулов для повышения бдительности людей, то тут тоже есть обширный набор инструментов.

Например, чтобы защитить себя и своих клиентов от мошенников, банки предлагают разные приятные бонусы. Если клиент пользуется надежной защитой своего аккаунта, проходит обучение по безопасности и не допускает нарушений, ему могут предложить скидки на банковские услуги или страхование, повышенный кешбэк и увеличенные лимиты на операции. За выполнение простых, но важных шагов, таких как подтверждение крупного платежа звонком в банк, начисляются приятные бонусы. Чем выше ваша безопасность и ниже риск, тем выгоднее становится обслуживание за счет гибкой тарификации риска: транзакции обрабатываются быстрее и дешевле. Но если аккаунт кажется ненадежным, сервис может стать дороже и замедлится обработка операций.

Чтобы не быть голословной, расскажу о том, как компания «Фаззи Лоджик Лабс» создала увлекательную игру «Финополья», основанную на технологиях ИИ и направленную на повышение финансовой грамотности игроков. Главную роль исполняет персонаж-аватар Василиса, символизирующая опыт и способность решать самые трудные задачи. Игроки отправляются в захватывающее путешествие по интерактивной вселенной, исследуют неизведанные места, отдыхают рядом с зеленым дубом вместе с ученым котом и участвуют в приключениях известных исторических героев. Им предстоит подсмотреть секретный диалог богов Олимпа Зевса и Геры, поддержать поэта Владимира Маяковского в совершении безопасной онлайн-транзакции и уберечь отважного д'Артаньяна от попадания на опасный сайт-мошенника.

— **А самой индустрии антифрода требуются ли новые стандарты и протоколы, чтобы «шить» защиту?**

— По моему глубокому убеждению, прежде всего необходимо развивать уже доказавшую свою эффективность

практику обмена индикаторами компрометации и примерами успешных кейсов между компаниями, поскольку победить мошенничество в одиночку невозможно.

Антифрод не работает, если ответственность распределена неравномерно или вообще разорвана: продуктовые показатели нацелены на увеличение оборота, тогда как риски и последствия ложатся на службу информационной безопасности. Необходимо совместное принятие ответственности бизнесом, подразделениями информационной безопасности и комплаенс-контроля с едиными KPI и согласованными процедурами оценки и принятия риска.

Следующим важным этапом является обеспечение равной доступности отраслевых решений для всех участников рынка: крупные компании способны приобретать дорогостоящие продукты, малые предприятия — нет. Следовательно, важнейшими факторами становятся разработка стандартов и снижение порога входа.

— **На каком уровне сейчас находятся регулирование и правоприменение? Возможна ли кооперация с правоохранительными органами?**

— Государство активно участвует в процессе борьбы с мошенничеством, внедряя такие инструменты, как система ГИС АНТИФРОД, и определяя критерии для выявления и предотвращения мошеннических действий. Например, с июля 2026 года НСПК сделает обязательным применение расширенного индикатора риска при совершении переводов с использованием СБП, были выпущены приказы Банка России № ОД-1765 «Об установлении признаков выдачи наличных денежных средств без добровольного согласия клиента с использованием банкоматов» и № ОД-2506 «Об установлении признаков осуществления перевода денежных средств без добровольного согласия клиента».

Регулирование в области антифрода представляет собой сложную задачу по достижению баланса между обеспечением безопасности и соблюдением прав клиентов. Различия в целях и точках зрения приводят к появлению ограничений, снижающих эффективность принимаемых мер. Для решения этой проблемы необходимы профессиональная экспертиза, внедрение и пилотирование профильных сервисов как подход «регуляция через практику»: проведение тестов, сбор и оценка показателей эффективности, последующая коррекция мероприятий.

— **Какие можно строить прогнозы развития отрасли антифрода на 12–24 месяцев?**

— Самый очевидный прогноз, который я могу уверенно сделать сегодня, заключается в следующем: киберпреступность продолжит расширяться, активно инвестируя в технологическое развитие и приобретение доступов и данных для усиления методов социальной инженерии. Это приведет к тому, что антифрод-системы будут больше ориентироваться на внешние сигналы, межотраслевое взаимодействие и создание более жесткой связки «продукт — риск — ответственность».