# Максим Степченков (RuSIEM): Раньше атаковали хакеры, теперь атакуют кибервойска

## О том, как комплексный подход к анализу угроз помогает компаниям адаптировать свою информационную безопасность к актуальным рискам, рассказал Максим Степченков, совладелец компании RuSIEM

*Текст*
**ЕЛЕНА ПОКАТАЕВА,**
ОБОЗРЕВАТЕЛЬ **«Б.О»**

**— Максим, как сегодня выглядит комплекс угроз, которые необходимо учитывать компаниям? Что изменилось после февральских событий?**
— По большому счету основные угрозы не изменились — нарушения конфиденциальности данных, доступа к данным. Но принципиально поменялось следующее: раньше компании из государственного или коммерческого сектора атаковали зарубежные хакеры, сегодня атакуют кибервойска. Если раньше мы могли рассчитывать на поддержку со стороны правоохранительных органов других стран, то сегодня это фактически невозможно, ведь зачастую эти нападения спонсируются самими государствами, в результате чего утрачено доверие к западным средствам ИБ. Еще одно существенное событие — отключилось большое количество западных средств защиты информации.

**— Как выглядит российский рынок SIEM после того, как его покинули западные вендоры?**
— В целом, рынок российских решений ИБ всегда был впереди остальных отраслей с точки зрения импортонезависимости. Так что радикальных сдвигов на этом рынке не случилось. Произошло замещение определенных продуктов западных производителей российскими, сам набор решений при этом практически не изменился. То, что рекомендовали компании год-два назад, они рекомендуют и сейчас, только акцент сместился в сторону более быстрого принятия решений, более оперативного запуска средств защиты информации и более комплексного подхода.

По сути, клиент выбирает между российским или псевдороссийским — тем, что можно купить, обойдя западные ограничения. Но, отмечу, в основном компании стремятся приобретать российские продукты.

**— На какие параметры стоит обращать внимание клиентам?**
— Во-первых, не следует забывать принцип Парето («20% усилий дают 80% результата, а остальные 80% усилий — лишь 20% результата»). Зачастую мы сталкиваемся с тем, что заказчики хотят получить огромное количество функций, которые никогда не будут использовать. Поэтому вначале стоит понять, какие сервисы вы будете реально эксплуатировать, чтобы не переплачивать. Во-вторых, важна возможность быстрого внедрения и удобной эксплуатации системы, чтобы не оказаться в ситуации, когда приобретенные решения некому сопровождать, настраивать под собственные особенности.

**— В чем различия продуктов разных поставщиков с точки зрения функционала SIEM?**
— Стандартный функционал SIEM есть у всех, а различаются они «фишечками» с аналитическим функционалом. Мы как производитель решений аналитики с использованием механизмов машинного обучения знаем, что невозможно заранее написать все правила корреляции, предугадать все возможные векторы атаки. Поэтому в функционале SIEM я особо выделяю подсистему, которая выявляет аномалии. Она играет роль, если хотите, «головного мозга» системы ИБ.

**— Чем могут различаться способности «головного мозга» разных систем?**
— В качестве примера рассмотрим одну «фишечку». Есть два подхода к агрегации данных об угрозах: агрегация инцидентов и агрегация событий. Мы придерживаемся стратегии агрегации инцидентов: если одновременно произошло 100 одинаковых инцидентов, то они «схлопываются» в один и расследуются как один инцидент. Сторонники второго подхода считают, что если произошло 100 одинаковых событий, то они «схлопываются» в один инцидент, который расследуется соответствующим образом. Мы против данного подхода, поскольку в этом случае логи становятся видоизмененными, и это затрудняет их использование в качестве доказательства в суде. Оппоненты, в свою очередь, указывают: за счет агрегации событий мы уменьшаем объемы хранения информации. Как видите, аргументы есть у обеих сторон. В результате мы сейчас выпускаем версию RuSIEM, в которой реализованы оба подхода.

**— В современном мире и транзакции, и атаки происходят в режиме реального времени. Насколько оперативно способна система SIEM реагировать на происходящее?**
— Система SIEM обязана обрабатывать события с той скоростью, с которой идет атака, своевременно выявлять угрозы и предпринимать необходимые действия.

**— Инструментарий расследования имеет значение для выбора SIEM-системы?**
— Имеет, но непринципиальное. Многое зависит от того, как в компании организованы процессы ИБ. Можно ведь использовать, например, системы SOAR (Security Orchestration Automation and Response), которые объединят различные решения защиты в единую систему, в качестве инструментария реагирования, но при этом не организовать процессы. А можно использовать утилиты, встроенные в операционные системы, сетевое оборудование, и, грамотно организовав процессы, вовремя устранять все угрозы. Так что и при расследовании, и при реагировании первичны процессы, под них потом выбирают инструменты.

**— Комплексный подход к анализу угроз также реализуется в концепции центра мониторинга информационной безопасности SOC. Как выглядит SOC в общем контексте комплексных решений для обработки угроз?**
— SOC — инструмент полезный, но не обязательный. Речь ведь идет о том, что в компании должны быть организованы процессы, заточенные под это решение, чтобы в случае угроз своевременно и качественно реагировать на них. Поэтому SOC полезна как концепция защиты. А на каких продуктах она будет реализована — это вопрос индивидуальный.

Кто-то реализует свой SOC на SIEM. Действительно, если в компании есть электронная почта, выход в интернет и антивирус, то у нее должна работать SIEM. С ее помощью можно создать огромное количество правил и закрыть огромное количество угроз. И я знаю такие компании, в которых один IT-специалист успешно обслуживает защиту сотен компьютеров пользователей. У него два основных инструмента. Во-первых, создание резервной

копии системы, что происходит неукоснительно по завершении рабочего дня в компании. Во-вторых, SIEM-система, которая показывает ему в начале рабочего дня ситуацию с атаками. Если что-то произойдет, то есть резервная копия системы, которая позволит восстановить рабочий режим. Если критичных бизнес-процессов в компании нет, то можно использовать и такой простой вариант.

Есть и другие мнения. Некоторые специалисты уверены, что внутренний SOC обязательно должен включать SOAR, специализированные средства расширенной детекции (XDR, Extended Detection and Response), защиту конечных точек (EDR, Endpoint Protection Platform), защиту веб-приложений (WAF, Web Application Firewalls), защиту от DDoS-атак и прочее. Здесь я вновь намню правило Парето: от всех на свете угроз не защититься, нужно выбирать те, которые адекватны для конкретной компании.

Дело вообще не в количестве используемых ИБ-решений. Я не раз сталкивался с ситуацией, когда заказчики хотят использовать 20, а то и 30 разных ИБ-продуктов, но теряются с ответом на вопрос: как защищенность IT-систем компании увеличится от добавления того или иного решения? И масштаб компании тоже не очень важен. Маленькая компания, где отсутствует существенная конфиденциальная информация, может легко перенести два-три дня простоя IT-систем. И такая же маленькая компания, но владеющая огромными активами, может потерять колоссальные денежные средства за пару часов простоя.

**— Вы предложили хороший образ: SIEM — головной мозг системы ИБ. Но головной мозг надо пополнять новыми знаниями. Как происходит постоянное «повышение квалификации» этих систем?**

— В первую очередь это анализ обратной связи со стороны заказчиков, текущих потребителей, подключение к расследованию инцидентов, своя экспертная база знаний. Естественно, мы прислушиваемся к общественному мнению, к тому, что происходит как на российском, так и на международном рынках, какие советы дают профессионалы из различных сфер ИБ. Так что, если какие-то функции SIEM у нас не реализованы в настоящий момент, но такие пожелания начали витать в воздухе, значит, они точно появятся в первом или втором квартале следующего года. Наша система RuSIEM постоянно развивается, модифицируется.

**— SIEM относится к числу интеллектуальных систем, а они обычно дорогие…**

— Это миф и попытка некоторых игроков рынка аргументировать высокую стоимость своих решений. Конечно, за бесценок SIEM не приобрести, но такая система доступна самым разным компаниям. Приходите, мы вам это докажем. У нас в числе клиентов есть и совсем маленькие компании, которые считают каждую копейку. Не бойтесь внедрять SIEM, не бойтесь делать это собственными руками — все получится! Это действительно крайне важный и необходимый инструмент для любой современной компании. Б.О