Обзор и тренды
российских Bug Bounty площадок

Алексей ГРИШИН,
директор по развитию сервисов кибербезопасности системного интегратора по ИБ «Бастион»

Сегодня вопросы кибербезопасности привлекают особое внимание. Рост угроз со стороны хакерских группировок и трудности с внутренней безопасностью в компаниях были и раньше, но текущая ситуация обязывает бизнес внимательнее следить за своей инфраструктурой. Нехватка профессиональных ИБ-кадров на рынке труда сказывается на качестве обслуживания и защиты информационных систем. Кроме того, все больше ограничений связано с изменениями в законодательстве.

Как и прежде, компании выбирают между штатными специалистами, услугами внешних ИБ-компаний и вольными багхантерами-аутсорсерами – «белыми хакерами», которые готовы отыскать уязвимость в любой инфраструктуре за вознаграждение.

Крупный и средний бизнес, раньше полагавшийся на внутренние ресурсы в вопросах кибербезопасности, стал чаще обращаться к программам Bug Bounty на специализированных площадках. Такая «корректировка» процессов поиска и обработки уязвимостей, в условиях кадрового голода ИБ-рынка, позволяет провести комплексный анализ защиты инфраструктуры и преодолеть ограничения собственного штата. Выгода в этом подходе понятна: компании могут временно привлекать внешних специалистов с уникальными навыками, а исследователи получают возможность дополнительной монетизации, реализуют накопленную экспертизу и сталкиваются с новыми вызовами для профессионального развития.

Спрос на услуги багхантеров стабильно растет не только среди российских коммерческих организаций. На Bug Bounty платформы выходят государственные информационные системы, как из отдельных областей, так и министерств. Такая динамика спроса и сильная внутренняя конкуренция Bug Bounty площадок в России позволили им менее чем за два года пройти 3–5-летний путь, который проделали их иностранные коллеги.

С 2022 года корпорации в сфере информационной безопасности начали вкладывать значительные ресурсы в разработку собственных баг-баунти решений. В течение 2022 года в России появились две Bug Bounty платформы: BI.ZONE Bug Bounty и Standoff365 Bug Bounty. Программы крупных игроков ИТ-рынка, размещенные вне платформ, также претерпели качественные изменения, став процессно сильнее. В результате российский рынок Bug Bounty площадок оказался не только финансово доступнее, но и лучше адаптирован к потребностям локального бизнеса.

Финансовый аспект сыграл одну из ключевых ролей в переходе на российские Bug Bounty платформы. Обслуживание на таких площадках обходится дешевле: платежи и комиссии не зависят от колебаний валютных курсов, что делает участие в программах выгодным для бизнеса. Однако размер выплат для багхантеров-аутсорсеров сильно снизился, значительно сократив их число на и так изолированном рынке. Российские платформы оказались в особом положении с выраженной потребностью в услугах со стороны вендоров и в условиях кадрового голода ИБ-рынка.

Отличия российских и зарубежных Bug Bounty платформ

Российский рынок Bug Bounty активно развивается — на нем представлены три платформы: BI.ZONE Bug Bounty, Standoff365 Bug Bounty и Bugbounty.ru.

Отечественные и зарубежные платформы Bug Bounty существенно отличаются подходом к работе с багхантерами и бизнесом. Западные платформы, например, HackerOne, ориентированы преимущественно на коммерческие задачи и привлекают опытных багхантеров со всего мира высоким вознаграждением и большим количеством заказчиков. Они выполняют роль посредника между бизнесом и «белыми хакерами», поскольку не только берут агентский процент за выплаты, но и зарабатывают на подписке за размещение.

Российские платформы Bug Bounty больше фокусируются на развитии, консолидации своих сообществ и прогрессе навыков начинающих багхантеров. Эти площадки предлагают тренировочные полигоны, инфраструктурные задачи и соревнования для развития

компетенций исследователей в области кибербезопасности, чтобы привлечь и удержать их на своей платформе. Российские площадки, по аналогии с иностранными, берут агентские комиссии за выплаты, но стоимость размещения на них ниже. Платформы зарабатывают на дополнительных услугах: разборе поступающих Bug Bounty отчетов или организации закрытых мероприятий для лучших исследователей.

На российских платформах, несмотря на значительное количество зарегистрированных пользователей, число специалистов, активно занимающихся поиском уязвимостей, существенно меньше. Например, на платформе Standoff зарегистрировано около семи тысяч пользователей, однако, только двести-триста из них регулярно занимаются поиском багов. Остальные занимаются обучением или участвуют в соревновательных мероприятиях — CTF. Эта ситуация во многом отражает дефицит квалифицированных кадров в сфере информационной безопасности в стране. В российском ИБ-сообществе закрытые мероприятия сосредотачивают внимание багхантеров на определенных программах, что значительно увеличивает количество уязвимостей и скорость их обнаружения.

Конкуренция среди российских платформ Bug Bounty стимулирует их развитие. Они регулярно проводят обновления платформы, помогают багхантерам в продвижении их личного бренда, организуют обучающие курсы и курируют профильные чаты для общения «белых хакеров». Все это делается с целью удержания интереса багхантеров и привлечения новых. Активность Bug Bounty платформ создает благоприятные условия для роста российского сообщества ИБ, несмотря на все сложности.

А что по деньгам?

Денежная политика отечественных и зарубежных платформ Bug Bounty существенно различается. Международные платформы обычно предлагают более высокие вознаграждения за выявленные уязвимости.

- Обилие программ на международных платформах Bug Bounty создает конкурентную среду. Компании вынуждены предлагать высокие вознаграждения, чтобы находиться в рынке стоимости уязвимостей и в условиях жесткой конкуренции привлекать внимание исследователя к себе.
- Раскрытие отчетов, содержащих крупные вознаграждения зарубежных компаний, рассматриваются как часть их стратегии продвижения. Такие публикации формируют позитивный имидж ответственного бизнеса, заботящегося о безопасности своих пользователей. Это положительно влияет на репутацию компании на зарубежном рынке.

Анонимные выплаты в криптовалюте на международных платформах Bug Bounty дают багхантерам дополнительное преимущество. Во многих юрисдикциях они все еще не подлежат налогообложению.

В России вознаграждения на платформах Bug Bounty ниже, чем на международных. Причины: меньшие финансовые возможности компаний и ограниченное число программ, конкурирующих за внимание исследователей. Однако российские платформы внедряют новые стимулы — сезонные увеличения вознаграждений и бонусные системы. Можно сказать, что стоимость выплат на Bug Bounty платформах в России точно будет расти.

Текущее положение российских багхантеров

Багхантеров интересует наличие уникальных и интересных программ, недоступных на других площадках. Закрытые проекты крупных отечественных компаний привлекают багхантеров возможностью работы с новыми продуктами и задачами. Российские специалисты достаточно быстро адаптировались к рыночным условиям. Теперь многие работают на нескольких платформах одновременно, расширяя доступ к интересным им программам, поэтому крупные вендоры публикуются сразу на нескольких площадках для максимизации внимания.

Кроме того, важно удобство подачи отчетов и коммуникации с вендором. Багхантерам нужен простой и понятный процесс оформления найденных уязвимостей. Платформы с удобными инструментами для создания и раскрытия отчетов экономят время исследователей. Это позволяет им сосредоточиться на поиске уязвимостей, а не на технических аспектах отчетности.

Перспективы Bug Bounty площадок

Рынок Bug Bounty в России проходит стадию формирования и развития, причем сразу несколько факторов способствуют росту отечественных платформ.

- Ужесточение законодательства создает сложности для международных сервисов, что побуждает российские компании искать альтернативы.
- Активное развитие образовательных инициатив также повышает интерес к Bug Bounty программам. Платформы создают учебные курсы, проводят соревнования и другие мероприятия. Это привлекает новых участников и повышает уровень компетентности багхантеров.
- Рост популярности платформ открывает новые возможности для российских специалистов ИБ. Они получают доступ к проектам, учитывающим специфику отечественного рынка. Это способствует развитию экспертизы в области информационной безопасности внутри страны.
- Усиление внимания к кибербезопасности на государственном уровне также играет важную роль. Оно создает благоприятную среду для развития Bug Bounty программ и платформ. Компании, ответственные за ГИС, все чаще рассматривают такие программы как эффективный инструмент повышения защищенности своих продуктов.

Российские Bug Bounty платформы обладают значительным потенциалом для развития, но их будущее зависит от способности эффективно адаптироваться к изменениям как на локальном, так и глобальном уровнях. В сегменте присутствует сильная конкуренция, что значительно ускоряет технологическое развитие направления. ■