

Поиск уязвимостей за вознаграждение: реальная обстановка на мировом и российском рынках bug bounty

Часть 1

Платформы bug bounty: исследование мирового рынка

Резюме

- **Программа bug bounty** — процесс, в рамках которого привлекается множество внештатных исследователей кибербезопасности для поиска уязвимостей в программном обеспечении, веб-приложениях и IT-инфраструктуре.
- Программы bug bounty **нацелены на результат**, поэтому вознаграждение выплачивается только за обнаруженную уязвимость, а не за время, которое было затрачено на ее поиск.
- **Условия успеха** программы **bug bounty**: необходимые инфраструктура и кадры, опыт, известность компании, умение точно определить целевые информационные активы, подлежащие тестированию, и границы исследования.
- Для помощи в проведении программ bug bounty созданы **платформы bug bounty**, предназначенные для организации поиска уязвимостей, предоставления необходимой инфраструктуры, поддержки и экспертных рекомендаций, но в первую очередь для анализа защищенности сообществом исследователей безопасности.
- **Открытые программы** платформ **bug bounty** предназначены для всех участников сообщества вне зависимости от уровня подготовки; **закрытые программы** — только для определенного круга исследователей по приглашению компании-клиента. Большинство платформ (88%) публикуют и открытые, и закрытые программы, 8% — только закрытые, 4% — только открытые.
- **Наиболее востребованными услуги** платформ **bug bounty** оказались в следующих отраслях¹: IT-компании (16%), онлайн-сервисы (14%), сфера услуг (13%), торговля (11%), финансовые организации (9%) и блокчейн-проекты (9%).
- **7200 долларов — средняя сумма вознаграждения** за найденную уязвимость критического уровня опасности, 3000 — высокого, 1100 — среднего, 254 доллара — за уязвимость низкого уровня опасности.
- **Наибольшие средние суммы вознаграждений** за уязвимости критического и высокого уровня опасности выплачиваются в программах bug bounty блокчейн-проектов (13 000 и 5300 долларов соответственно) и IT-компаний (6600 и 2200 долларов соответственно). Тройку лидеров замыкают медицинские учреждения: 5500 долларов за уязвимость критического уровня опасности и 1600 долларов — высокого.
- **Итоговая стоимость услуг платформ** складывается из нескольких составляющих. Во-первых, это стоимость **первичного размещения**, которая рассчитывается для каждого клиента индивидуально. Во-вторых, стоимость подписки на услуги платформы, в число которых входят использование инфраструктуры, взаимодействие с исследователями, верификация уязвимостей. Средняя цена годовой подписки на услуги платформ bug bounty составляет 16 000 долларов. В-третьих, в зависимости от плана подписки или опасности уязвимости **платформа** удерживает **комиссию**, которая составляет в среднем 20% от каждой выплаты исследователям и не вычитается из награды исследователя.

Введение

Уязвимости представляют собой недостатки и ошибки проектирования, разработки или администрирования, которые позволяют злоумышленникам реализовать недопустимые для организаций события. Для повышения уровня защиты приложений команда специалистов по ИБ, работающая в организации, должна в кратчайший срок найти и исправить все уязвимости — и сделать это быстрее злоумышленников. Однако их усилий может оказаться недостаточно, а нарушители могут нанести серьезный ущерб, воспользовавшись всего одной критически опасной уязвимостью.

Уязвимости могут появиться в самых неожиданных, а порой и в самых очевидных местах: людям свойственно ошибаться. Разработчики могут ошибаться при проектировании и реализации приложений. По данным нашего исследования, в 2020–2021 годах в 62% веб-приложений были выявлены уязвимости критического уровня опасности, и это с учетом того, что за 2019–2021 годы среднее количество уязвимостей на одно веб-приложение сократилось более чем на треть вследствие развития и внедрения инструментов для выявления уязвимостей, например анализаторов кода, а также подходов безопасной разработки. Автоматизированные решения для выявления уязвимостей по-прежнему актуальны, но не всегда действенны, особенно если дело касается поиска критически опасных уязвимостей, связанных с контролем доступа, или, например, уязвимостей бизнес-логики. Рост числа кибератак и выявление неизвестных ранее уязвимостей затрудняет защиту информационных активов: в I полугодии 2022 года было совершено на 16% больше кибератак, чем за аналогичный период прошлого года. С учетом постоянного обновления версий приложений анализ защищенности вручную становится слишком трудозатратным и дорогим. Выявление наиболее опасных для бизнеса уязвимостей в максимально сжатые сроки с небольшими затратами звучит как несбыточная мечта.

Но что будет, если объединить поиск уязвимостей с помощью автоматических средств и ручной анализ защищенности и если эти мероприятия будут проводиться не несколькими экспертами по ИБ в течение рабочего дня, а целым сообществом исследователей безопасности со всего мира — круглосуточно и без выходных? Мы проанализировали 24 платформы, на которых собрано множество программ bug bounty, чтобы рассказать для чего нужны такие платформы, какие задачи они помогают решать, какова стоимость их использования для организации и на какое вознаграждение могут претендовать исследователи безопасности. Методика исследования подробно описана в конце отчета.

Краудсорсинговый подход к обеспечению кибербезопасности является одним из лучших решений вышеописанных проблем для бизнеса: он позволяет непрерывно тестировать и выявлять уязвимости ПО, сайтов и инфраструктуры, привлекая неограниченное число исследователей безопасности. Лучший способ реализовать данный подход — объявить о программе bug bounty.



Ключом к успеху краудсорсинговой программы безопасности является привлечение как можно большего числа квалифицированных исследователей.

Bug bounty: программы и платформы

Программа bug bounty — это процесс привлечения бизнесом внештатных исследователей кибербезопасности и специалистов по анализу защищенности и тестированию на проникновение к проверке своего программного обеспечения, веб-приложений и инфраструктуры с условием выплаты вознаграждения за выявленные уязвимости.

Программы bug bounty дают компаниям возможность протестировать свои информационные активы под разными углами: любой исследователь может принять участие в тестировании, используя разные подходы и инструменты для поиска уязвимостей. Компании сами определяют границы работ и полностью контролируют бюджет, проверку отчетов о найденных уязвимостях и стоимость вознаграждения за каждую уязвимость.

Bug bounty — это подход, ориентированный на результат. При классическом подходе к анализу защищенности организациям приходится платить за время, затраченное на поиск уязвимостей, вне зависимости от того, будут ли они обнаружены. При использовании bug bounty организации выплачивают награду исследователям за обнаруженные и подтвержденные уязвимости в зависимости от уровня их опасности. Кроме того, конкуренция в сообществе и вознаграждение за результат мотивируют исследователей мыслить нестандартно и выявлять уязвимости, наиболее опасные для бизнеса.



В программах bug bounty **исследователи получают вознаграждение за найденную уязвимость**, а не за время, затраченное на ее поиск.

Привлечение внешних специалистов позволяет более эффективно выявлять слабые места и разгрузить собственных IT-специалистов, чтобы они могли сосредоточиться на укреплении слабых мест и дальнейшем развитии продуктов и сервисов. Оплата только за обнаруженные уязвимости позволяет рационально использовать бюджет компании.

Сложности реализации программ bug bounty

Несмотря на преимущества bug bounty, не все организации могут позволить себе проведение подобных программ, и на то есть несколько причин:

1. Все отчеты, присылаемые исследователями, подлежат первичной сортировке для выявления дубликатов, некорректных отчетов, для определения уровня опасности обнаруженной уязвимости и для отсева отчетов об уязвимостях с крайне низким уровнем опасности. Кроме того, необходимо организовать эффективное взаимодействие с исследователями, постоянную обратную связь и верификацию обнаруженных уязвимостей. Все эти **действия требуют от организации дополнительных ресурсов**.
2. Самостоятельное создание подробных отчетов о показателях программы bug bounty для оценки эффективности, обеспечения прозрачности, формирования и мониторинга ключевых показателей может оказаться затруднительным для организаций, которые **не имеют достаточного опыта** в проведении подобных программ.
3. Чтобы получить наибольший эффект от программы bug bounty нужно **заранее максимально четко определить границы проведения работ** и те информационные активы, которые будут тестироваться исследователями, что может оказаться **нетривиальной задачей** для некоторых организаций.

- 4. Известность организации играет важную роль.** Объявление программы bug bounty может не найти отклика в сообществе исследователей, так как, работая с малоизвестной организацией, они должны учитывать возможные риски. Стоит ли тратить время на поиск уязвимостей в системах этой организации, будут ли вовремя и справедливо выплачиваться вознаграждения, насколько профессионально выстроена программа bug bounty — вот первые вопросы, которые возникают у исследователей.

Платформы bug bounty

Для того чтобы помочь бизнесу справиться с этими и другими сложностями, стали появляться платформы **bug bounty** — своего рода агрегаторы, которые собирают программы различных организаций и позволяют исследователям безопасности выбрать интересующий их проект. Такие платформы предоставляют организациям всю необходимую инфраструктуру для эффективного проведения программ bug bounty, а также помощь во взаимодействии с исследователями и экспертную поддержку в верификации уязвимостей.

В платформах bug bounty удачно объединены два элемента:

Сообщество исследователей безопасности. Сообщество — это основная ценность платформы: чем больше в нем участников и чем выше их уровень подготовки, тем эффективнее поиск уязвимостей. Платформы прикладывают большие усилия для развития и поддержки своего сообщества, и на его формирование могут потребоваться годы. В среднем компании, оказывающие услуги анализа защищенности, задействуют для проверки приложения от пяти до пятнадцати сотрудников. За это же время ваше приложение могут протестировать сотни или даже тысячи специалистов и исследователей со всего мира, зарегистрированных на платформе. Исследователи могут активно тестировать приложения месяцами или годами, в отличие от классического анализа защищенности, который длится около месяца. Это позволяет снизить шанс появления необнаруженных уязвимостей и обеспечить непрерывный анализ защищенности приложений.

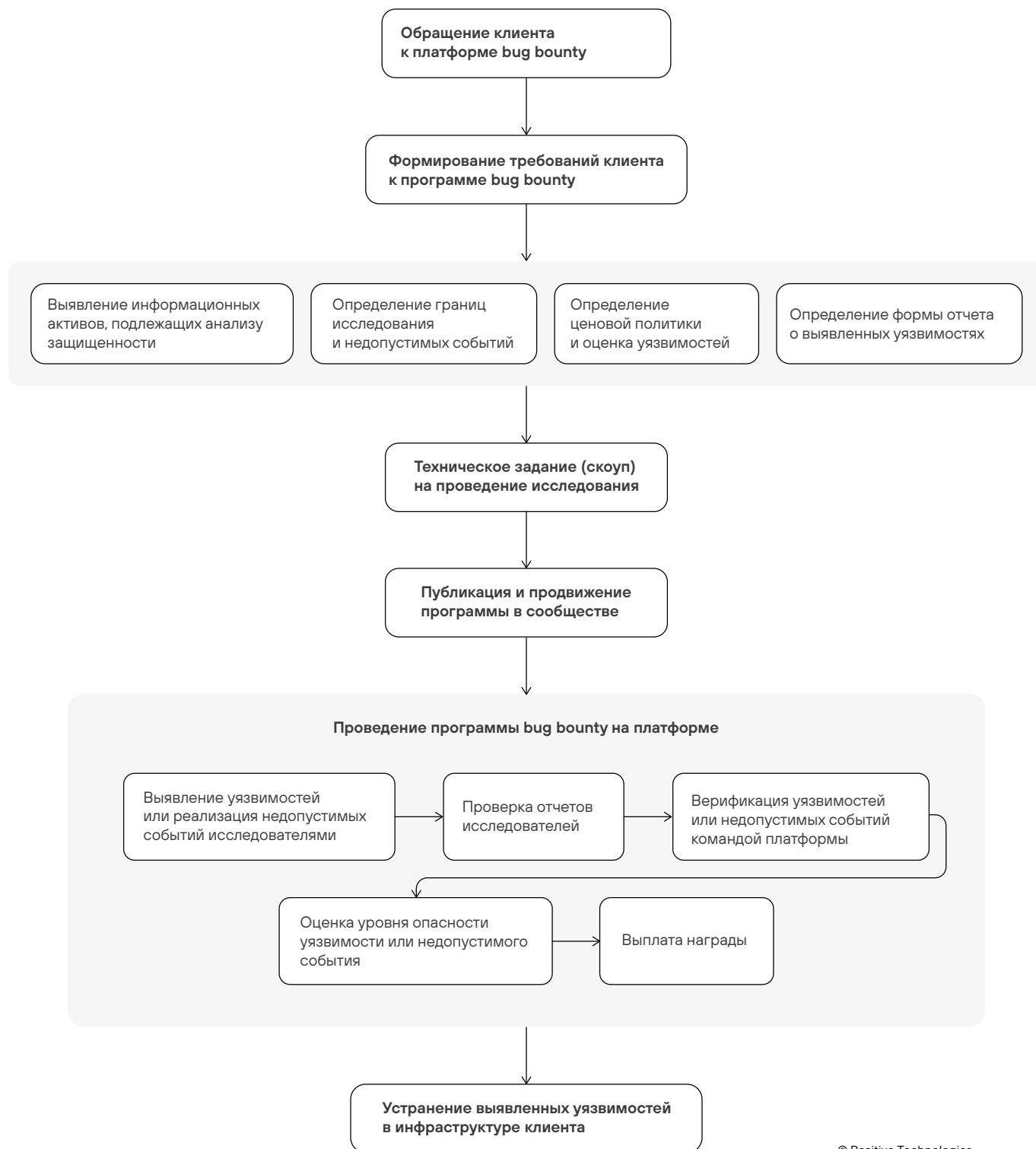
Высококвалифицированная команда специалистов по кибербезопасности, занимающаяся проверкой отчетов исследователей и верификацией обнаруженных ими уязвимостей. Также в задачи команды платформы входят поддержка клиентов и взаимодействие с исследователями.

Все исследователи, приступившие к поиску уязвимостей, обязуются придерживаться принципа ответственного разглашения, который гарантирует организациям, что об обнаруженной уязвимости не узнает никто, кроме платформы и исследователя, а организация получит достаточно сведений об уязвимости и времени для ее устранения.

Наиболее крупные мировые платформы bug bounty: HackerOne, BugCrowd, Intigrity, Synack, YesWeHack.

За что нужно платить и сколько это стоит

После того как организация вместе с представителями платформы определяет границы исследований, недопустимые события (в случае со Standoff 365), ценовую политику и форму отчета о выявленных уязвимостях, платформа публикует программу на своих ресурсах и продвигает ее в сообществе (в зависимости от типа программы), тем самым привлекая исследователей к участию в ней. Исследователи находят уязвимости и отправляют отчеты команде платформы, которая проверяет наличие уязвимости в исследуемом приложении, ее уникальность и соответствие границам исследования.



© Positive Technologies

Рисунок 1. Реализация программы bug bounty с помощью платформы

В случае соблюдения трех перечисленных выше условий отчет засчитывается, исследователю выплачивается вознаграждение и начисляются рейтинговые баллы, а организация получает подробный отчет об обнаруженной уязвимости.

Стоимость услуг платформ bug bounty складывается из нескольких составляющих:

Стоимость первичного размещения программы на платформе. За эту сумму компания получает помощь в определении границ исследования, недопустимых событий, ценовой политики и формы отчета об уязвимостях. Стоимость первичного размещения зависит от множества факторов, например от рода деятельности компании-клиента, ее размера и капитализации, и рассчитывается индивидуально.

Подписка на услуги платформы. В стоимость подписки входит привлечение сообщества к размещенной программе, использование инфраструктуры платформы для получения отчетов от исследователей и формирования аналитики по идущей программе, проверка отчетов исследователей, верификация уязвимостей (триаж) и взаимодействие с исследователями.

Комиссия платформы от сумм выплат. Размер комиссии зависит от плана подписки (чем дороже подписка, тем ниже комиссия) или от уровня опасности уязвимости, за которую производится выплата (чем опаснее уязвимость, тем выше комиссия).



16 000 \$ — средняя стоимость подписки на услуги платформ bug bounty в год.
20% от каждой выплаты — средняя комиссия платформ.

Существует две модели оплаты труда исследователей платформы компаниями:

Прямые выплаты. Компании-клиенты могут выплачивать единовременное вознаграждение исследователям через платформу за каждую обнаруженную уязвимость. Такая модель больше подходит для краткосрочных программ, при этом финансовое взаимодействие с исследователями осуществляет клиент, что может быть сопряжено с определенными трудностями.

Выплаты из фонда программы, который заранее резервируется компанией-клиентом. Такая модель больше подходит для долгосрочных программ. Она позволяет организациям уйти от прямого взаимодействия с исследователями по финансовым вопросам и дает возможность платформам действовать более автономно.

Как оценить опасность уязвимости и от чего зависит вознаграждение

Ценовая политика может быть установлена в зависимости от опасности той или иной уязвимости для бизнеса, например исходя из оценки уязвимости по методике [CVSS 3.1](#).

Таблица 1. Оценка степени опасности уязвимости по CVSS 3.1

Опасность уязвимости по CVSS 3.1	Значение вектора CVSS 3.1	Примеры уязвимостей
Критическая	от 9 до 10	Внедрение XXE- и SQL-кода со значительным воздействием на приложение; удаленное выполнение произвольного кода и повышение привилегий
Высокая	от 7 до 8,9	IDOR, Stored XSS и CSRF со значительным воздействием на приложение; SSRF и обход аутентификации
Средняя	от 4 до 6,9	IDOR, Reflective XSS и CSRF со средним воздействием на приложение
Низкая	от 0,1 до 3,9	Неверные параметры SSL; XSS и CSRF с незначительным воздействием на приложение

В среднем за критически опасные уязвимости компании готовы платить исследователям более 7000 долларов. Например, за выявление уязвимости для внедрения SQL-кода и несанкционированное получение данных в Twitter исследователь может получить 12 000 долларов. За выявление уязвимостей, связанных с некорректной авторизацией и аутентификацией, исследователь может в среднем рассчитывать на 3000 долларов на различных платформах. А выплата за самую распространенную уязвимость межсайтового выполнения сценариев (cross-site scripting, XSS), которая была выявлена в 13% приложений, по данным [Zerocopter](#), может составить от 250 до 700 долларов в зависимости от степени воздействия.

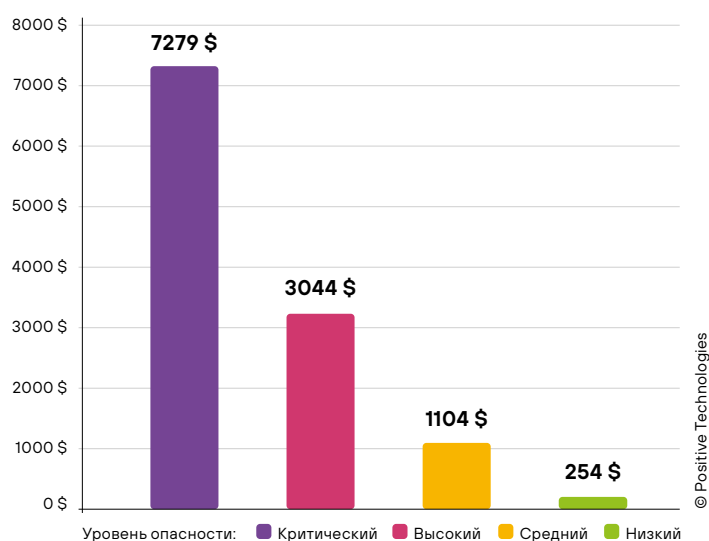


Рисунок 2. Средняя сумма вознаграждения в зависимости от опасности уязвимости

Исследователи могут получить дополнительное вознаграждение за оперативную помощь организации в устранении выявленных уязвимостей. Подобный подход применяется на платформе Huntr.

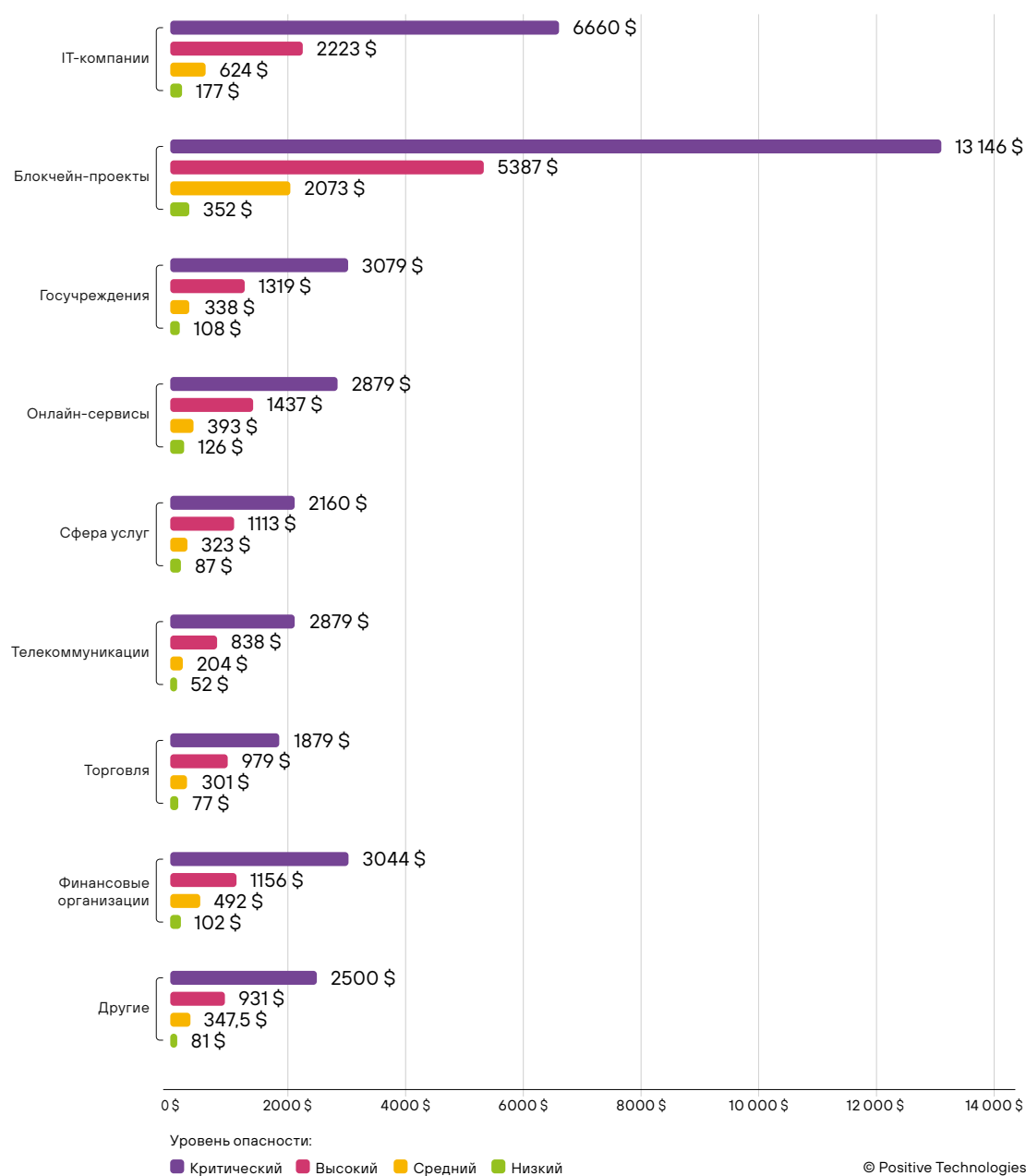


Рисунок 3. Средние суммы вознаграждений за одну уязвимость

Вознаграждения за уязвимости среднего и низкого уровня риска достаточно невысоки, в отличие от уязвимостей критического и высокого уровня, которые могут стать источником наиболее опасных для бизнеса угроз — утечек конфиденциальной информации, несанкционированного доступа к приложению или атак на локальные ресурсы. Бизнес понимает последствия реализации опасных уязвимостей и готов платить значительно больше за выявление уязвимостей высокого и критического уровня опасности. Например, участвовавшие в последние месяцы случаи атак на блокчейн-проекты вынуждают разработчиков тщательнее выявлять уязвимости в своих продуктах, а за уязвимости критического и высокого уровня опасности предлагается максимальное вознаграждение — 13 100 и 5300 долларов соответственно. Особо опасные уязвимости могут оцениваться в 100 000 долларов и более. Решения IT-компаний также должны быть защищены от атак. Такие компании, как Sony и Intel, предлагают не менее достойные награды: 50 000 и 100 000 долларов соответственно за уязвимости критического уровня риска.

Но для того чтобы точнее определить степень опасности, каждой организации необходимо знать, как возможная эксплуатация уязвимостей может повлиять на ее деятельность и может ли эксплуатация уязвимости привести к недопустимым для бизнеса последствиям. Платформа Standoff 365 предлагает исследователям попробовать новый подход: помимо обычного поиска уязвимостей и предоставления отчетов, исследователям предлагается не просто найти уязвимость, но и продемонстрировать реализацию недопустимого события на основе найденных брешей. Если отчет с четким исчерпывающим описанием полного вектора атаки и использованием уязвимостей будет верифицирован командой платформы, то исследователь может рассчитывать на вознаграждение, которое в разы превышает выплаты за обычные уязвимости.



Недопустимое событие — это событие, возникающее в результате действий злоумышленников, которое делает невозможным достижение операционных и стратегических целей или приводит к длительному нарушению основной деятельности организации.

Такой подход выгоден для всех взаимодействующих сторон. Компания-клиент получает подробный отчет об эксплуатации целого ряда уязвимостей, которые привели к реальной атаке и недопустимому событию, возможность оперативно исправить уязвимости и реальное представление о последствиях и сценариях атаки. Исследователь получает значительно большее вознаграждение и продвигается в рейтинге, а платформа может одновременно проверить цепочку уязвимостей вместо разрозненных отчетов.

Сводная статистика платформ bug bounty

На мировом рынке платформы bug bounty представлены неравномерно, и не в каждой стране можно найти крупные и заслуживающие доверия платформы. Лидером по количеству крупных платформ bug bounty является Азиатский регион, в котором размещены 38% исследованных платформ. На втором месте Европейский регион, в котором находится треть исследованных платформ, в том числе одни из наиболее крупных, например Intigriti, YesWeHack, Zerocopter и Standoff 365. Доля платформ Североамериканского и Ближневосточного регионов составила 21% и 8% соответственно.

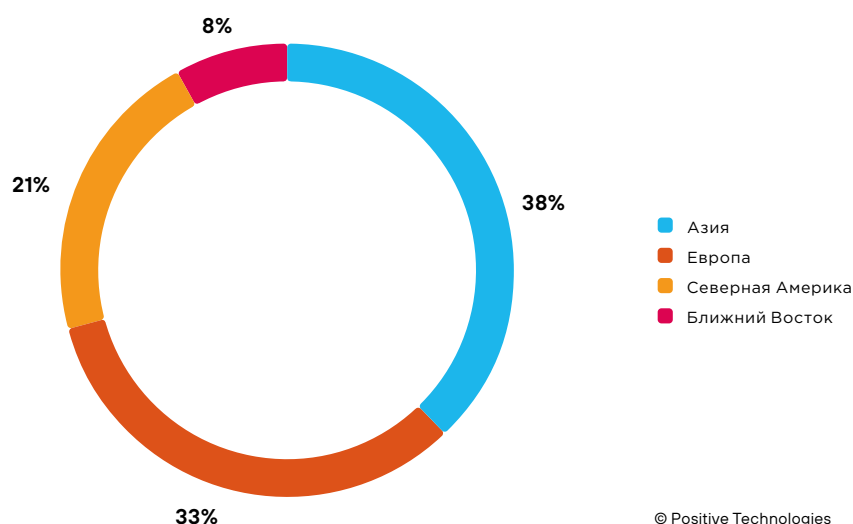


Рисунок 4. Распределение платформ bug bounty по регионам

Одно из главных преимуществ краудсорсингового подхода к обеспечению безопасности — это число участников. Однако не все исследователи обладают требуемой квалификацией или являются специалистами в определенной сфере (в сфере веб-приложений, блокчейна и т. п.), а организации не всегда готовы сразу обрабатывать большое количество обнаруженных уязвимостей. Поэтому на платформах реализуются два типа программ — открытые и закрытые.

- 1 —→ **Открытые программы** позволяют любому исследователю получить к ним доступ и приступить к поиску уязвимостей.
- 2 —→ **Закрытые программы** ориентированы на определенную группу исследователей, которые получают к ним доступ по приглашению.

Открытые программы позволяют получить больший охват, расширить категории и увеличить количество обнаруживаемых уязвимостей благодаря разнообразным навыкам и опыту исследователей. Но стоит учесть, что квалификация участников открытых программ может

существенно различаться, что не способствует выявлению уязвимостей критического и высокого уровня опасности. Закрытые программы позволяют отбирать специалистов, которые соответствуют заданным требованиям, или приглашать наиболее продвинутых исследователей, чтобы повысить шансы обнаружения серьезных уязвимостей. Такие платформы, как Synack и Cobalt, проводят только закрытые программы, в которых принимают участие члены сообщества, прошедшие строгий квалификационный отбор.

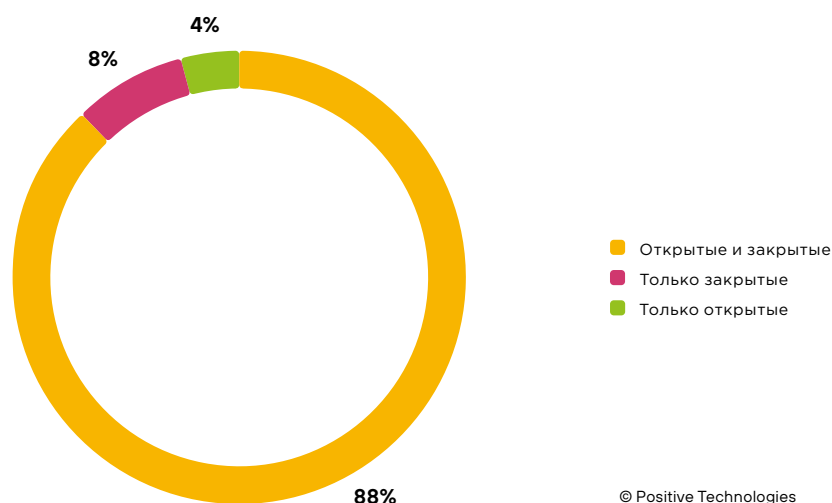


Рисунок 5. Распределение платформ bug bounty в зависимости от проводимых программ

Бизнес не упускает возможности прибегнуть к таким перспективным способам обеспечения кибербезопасности, как программы bug bounty, и пробует внедрять их в свои процессы. IT-компании, постоянно работающие над улучшением своих приложений, являются наиболее частыми клиентами таких платформ (16%). Каждое десятое приложение на платформах bug bounty предоставлено финансовым или торговым секторами: согласно отчету платформы HackerOne, прирост числа клиентов из этих секторов в 2021 году составил 62% и 51% соответственно. Недавние взломы ([1], [2]) криптовалютных площадок (9%) выявили потребность в создании программ bug bounty для поиска уязвимостей в протоколах и смарт-контрактах.

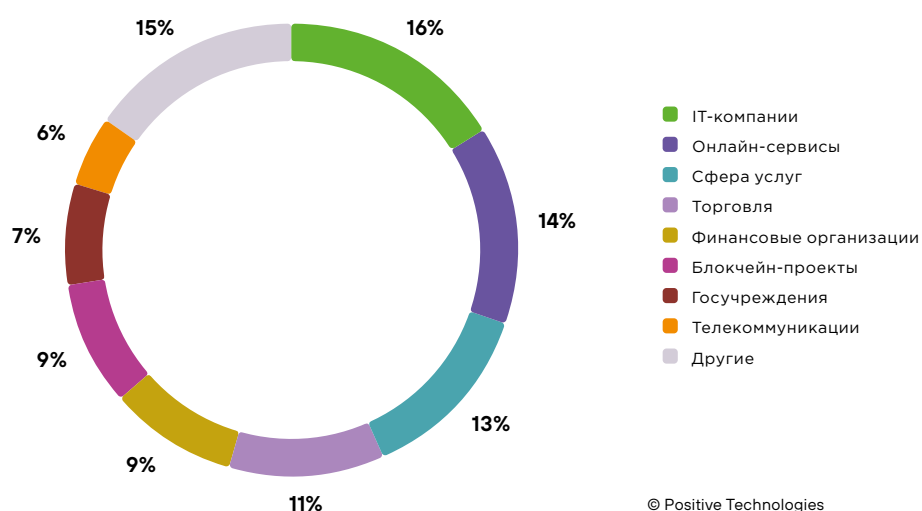


Рисунок 6. Отраслевое распределение участников платформ bug bounty

Перспективы развития и проблемы рынка bug bounty

Программы и платформы bug bounty находят все большее распространение среди организаций, заинтересованных в обеспечении кибербезопасности своих ресурсов. Аналитики платформы HackerOne отмечают, что в 2021 году количество программ bug bounty увеличилось на 34% по сравнению с 2020 годом, а исследователи безопасности выявили на 21% больше уязвимостей за аналогичный период. Данные исследования AllTheResearch предсказывают рост рынка bug bounty до 5,4 млрд долларов к 2027 году.

Драйверами роста рынка bug bounty выступают:

- распространение интернета во всем мире;
- растущая осведомленность о необходимости обеспечения информационной безопасности;
- привлекательные суммы вознаграждения за найденные ошибки;
- широкое применение онлайн-сервисов в организациях в связи с тем, что сотрудники все чаще используют портативные и другие устройства, подключенные к интернету;
- высокий спрос на средства обеспечения кибербезопасности среди организаций;
- технологические достижения и тенденции, такие как IoT, IIoT, облачные вычисления, искусственный интеллект, машинное обучение и «Индустрия 4.0».

Однако достижению прогнозируемых показателей могут помешать следующие факторы:

- отсутствие расширения рынка в менее развитых странах;
- сложность поиска уязвимостей без приобретения дополнительного специализированного программного обеспечения;
- жесткая конкуренция в отрасли;
- сложность поиска уязвимостей из-за мер безопасности при разработке веб-приложений.

Выводы

Краудсорсинговый подход к обеспечению безопасности является одним из наиболее перспективных, а его реализация в виде программ bug bounty обеспечивает множество преимуществ над классическими решениями: ориентацию на результат, непрерывность тестирования, гибкость и масштабирование программы, а также прозрачную систему вознаграждений.

Однако реализация программ bug bounty доступна далеко не всем: одни организации не могут точно определить границы исследования, другим не хватает опыта или ресурсов для проведения собственных программ, а третьи сталкиваются с дефицитом доверия со стороны исследователей безопасности.

Для решения вышеописанных проблем были созданы платформы bug bounty — агрегаторы, которые собирают программы различных организаций. Платформы позволяют исследователям безопасности самостоятельно выбрать интересующий их проект, помогают компаниям-клиентам выбрать целевые приложения, системы тестирования и границы исследования. Также они берут на себя всю основную работу по взаимодействию с исследователями и проверке их отчетов. Это разгружает IT-отделы компаний, которые могут сосредоточиться на доработке приложений и систем в соответствии с отчетами о выявленных уязвимостях.

За умеренную плату организации получают всю необходимую инфраструктуру, поддержку, возможность платить только за результат, а самое главное — исследователей, которые готовы различными способами выявлять уязвимые места в режиме 24/7. На платформе Standoff 365 у компаний-клиентов есть уникальный шанс проверить свои продукты на возможность реализации недопустимых событий. Такой подход позволяет получить представление о последствиях атаки на приложение, максимально соответствующей реальной угрозе, и подробный отчет для оперативного устранения выявленных недостатков.

Не останутся в обиде и исследователи: оперативная обратная связь с представителями платформы, справедливые вознаграждения за обнаруженные уязвимости, значительно увеличивающиеся в случае реализации недопустимых событий, рейтинговая система, позволяющая принимать участие в более прибыльных закрытых программах, — все это повышает конкуренцию в сообществе и стимулирует его развитие.

Методика исследования

В этом отчете содержатся результаты исследования 24 наиболее крупных¹ и активных² на момент исследования платформ bug bounty из разных регионов мира, из которых были собраны данные о следующих показателях: географическом расположении, типах программ, реализуемых платформами, отраслевом распределении участников, средних суммах вознаграждения в зависимости от степени опасности уязвимости и отрасли, средней стоимости вхождения на платформу, средней комиссии, взимаемой с каждой выплаты исследователю. В табл. 2 приведен список исследованных платформ bug bounty с указанием их географического расположения.

Информация получена с официальных сайтов платформ и не содержит данных, находящихся в ограниченном доступе. Средние значения вознаграждений по отраслям рассчитаны на основе среднего максимального и среднего минимального значений по каждой отрасли и платформе. Средние значения вознаграждений в зависимости от степени риска рассчитаны на основе среднего максимального и среднего минимального значений выплат в зависимости от уровня опасности и платформы. Все суммы приведены в долларах США.

Степень опасности уязвимостей оценивалась по системе Common Vulnerability Scoring System (CVSS) версии 3.1. На основе полученных значений определялись качественные оценки критической, высокой, средней и низкой опасности.

2 Сообщество платформы насчитывает более 700 пользователей.

3 На платформе размещено не менее 20 активных программ bug bounty

Таблица 2. Исследованные платформы bug bounty

Платформа	Страна
Intigrity	Бельгия
Huntr	Великобритания
Hackrate	Венгрия
WhiteHub	Вьетнам
BugRank	Вьетнам
Safevuln	Вьетнам
Zerocopter	Голландия
Bugbase	Индия
BugsBounty	Индия
Redstorm	Индонезия
Ravro	Иран
Vulbox	Китай
thebugbounty	Малайзия
Bugbounty.sa	Саудовская Аравия
Bugcrowd	США
Synack	США
Cobalt	США
HackerOne	США
Federacy	США
YesWeHack	Франция
Yogosha	Франция
Cyscope	Швейцария
HackenProof	Эстония
Bugbounty.jp	Япония

Часть 2

Bug bounty в России: состояние рынка и перспективы

В мире растет популярность программ bug bounty, в ходе которых компания привлекает сторонних специалистов по безопасности — так называемых «белых хакеров» — для тестирования своего ПО на уязвимости за вознаграждение или иные «плюшки». В отличие от пентестов с привлечением подрядчиков, в случае с bug bounty оплата происходит за обнаруженные уязвимости, а не за время, специалистом по ИБ. В России интерес к этой практике тоже увеличивается, причем не только со стороны бизнеса, который раньше начал прибегать к bug bounty, но появляется и со стороны госсектора. TAdviser изучил текущее состояние и перспективы этого рынка и подготовил соответствующий обзор. Партнером материала выступила Positive Technologies.

Об обзоре

Целью обзора являлась проверка ряда гипотез:

- Рынок bug bounty в России — формирующийся, только зарождается, и его в ближайшее время ждет бурный рост.
- Рынок bug bounty в России сегодня формируют B2C-продукты и сервисы, где есть зрелые процессы кибербезопасности: (IT-компании, финансы, e-commerce).
- Рынок bug bounty в России будет расти за счет появления программ в объектах критической инфраструктуры (КИИ) как расширение процессов управления уязвимостями (в дополнение к сканерам безопасности и периодическим пентестам).
- Интерес к bug bounty в КИИ в первую очередь лежит в плоскости проверки возможности реализации их недопустимых событий, а не в поиске отдельных уязвимостей.

Positive Technologies выступила в качестве стороны, предложившей гипотезы выше, а также в качестве компании, которая поделилась экспертизой в обозначенной области, не влияя на редакционную работу при подготовке материала, на оценки и выводы, приведенные редакцией в обзоре.

Обзор не ставил целью сравнительный анализ Positive Technologies с конкурентами в обозначенной области, и редакция при использовании информации, связанной с конкурентами, придерживалась политики нейтральности, избегая, чтобы кто-то выглядел более или менее выгодно на фоне остальных.

Для подготовки данного материала TAdviser использовал информацию из общедоступных ресурсов, а также полученную аналитиками TAdviser примерно от 20 источников из сферы ИБ. Сюда входят представители всех ключевых компаний-провайдеров услуг bug bounty в России на данный момент, ряд компаний — пользователей программ bug bounty, открыто поделившихся данными и комментариями, а также несколько экспертов, пожелавших сохранить анонимность, один из которых — источник в Минцифры.

Работа над обзором проводилась в сентябре — октябре 2022 года.

Текущее состояние рынка

С точки зрения профиля деятельности в настоящий момент основная масса заказчиков программ bug bounty в России представлена крупным бизнесом, преимущественно таким, который обслуживает очень большое количество пользователей (клиентов) и для которого брешы в безопасности несут крайне высокие финансовые и репутационные риски. Среди них:

- банки,
- интернет-сервисы,
- электронная коммерция,
- разработчики IT-продуктов,
- ритейл.

Для крупных IT-компаний в России, в частности, использование процессов bug bounty уже стало распространенной практикой, считают в «Авито».

Интернет-компании можно назвать первопроходцами в области bug bounty. Так, «Яндекс» заявляет, что он первым запустил подобную программу в 2012 году. Это всего на год позже, чем, например, соцсеть Facebook. В июне 2021 года «Яндекс» сообщал, что с момента запуска «Охоты за ошибками» он перечислил участникам программы больше 30 млн рублей.

VK — еще одна из первых компаний в России, которая начала платить внешним исследователям за найденные уязвимости. С 2013 года VK получила более 15 тыс. отчетов, что позволило ей усилить защиту пользовательских данных и исправить уязвимые места. Всего за время действия программы bug bounty компания выплатила более 185 млн рублей (данные на август 2022 года).

Текущих пользователей программ bug bounty, даже тех, для кого создание и предоставление IT-продуктов и сервисов не является основным бизнесом, характеризует наличие развитой собственной разработки ПО. Как известно, за последние годы упор на инсорсинг разработки ПО делали в том числе многие банки, ритейл. Об усиливающейся роли инсорсинга разработки в российских компаниях TAdviser пишет уже несколько лет подряд.

Онлайн-банк «Точка» запустил публичную программу bug bounty в 2020 году. С февраля 2022 года компания перестала использовать программу из-за санкций, но за время ее использования успела оценить экономическую выгоду, рассказал TAdviser Алексей Киреев, менеджер направления «Информационная безопасность» в «Точке». За время пользования bug bounty «Точка» получила отчеты от почти 300 исследователей со всего мира и выплатила им вознаграждение, соответствующее опасности найденных уязвимостей, — всего около 6 000 долларов.

Организации, которые не делают ставку на инсорсинг разработки ПО, менее склонны прибегать к программам bug bounty. При этом они могут уделять не меньшее внимание кибербезопасности, чем те, кто разрабатывает собственное ПО, используя другие способы и инструменты обеспечения надежности своей IT-инфраструктуры, включая пентесты, которые проводит специально нанятые компании. Так, например, в небольшом по размеру активов московском банке «Держава» рассказали TAdviser, что не планируют прибегать к bug bounty, пока не начнут разработку собственных решений.

«Bug bounty, как правило, объявляют разработчики приложений и сетевых платформ, чтобы обнаружить проблемы в безопасности своих продуктов. Банк «Держава» не занимается разработкой собственных информационных систем и сервисов, а использует решения сторонних разработчиков, поэтому и опыта использования таких программ у банка нет, — поясняет TAdviser Вадим Жилин, начальник департамента информационных технологий АКБ «Держава». — Задачи по поиску уязвимостей в этих решениях — зона ответственности самих разработчиков. Для проверки IT-инфраструктуры банка на постоянной основе привлекаются внешние компании, имеющие опыт работ и лицензии на выполнение соответствующих работ. В целях минимизации рисков и получения максимального результата мы стараемся использовать разные компании».

На HackerOne, самой популярной в мире специализированной платформе, где заказчики размещают свои программы bug bounty, отмечают, что это практика не для всех: организация должна обладать развитой корпоративной программой безопасности, позволяющей исправлять найденные новые уязвимости. Без наличия базового процесса исправлений bug bounty не лучшее решение, констатируют в HackerOne.

Некоторые компании проводят открытые программы bug bounty, в которых может участвовать широкий пул хакеров, а другие предпочитают закрытый формат, когда к участию допускается ограниченный круг тщательно отобранных исследователей. Эксперты рынка ИБ, с которыми пообщался TAdviser, дают разные оценки соотношения открытых и закрытых программ. Исходя из них, можно склоняться к тому, что не менее 50% программ bug bounty в России сейчас являются закрытыми. Один из собеседников TAdviser оценил долю закрытых программ в 80%. В чем причина этого?

Многие пока только пробуют эту услугу, боятся публичных упоминаний, говорит Лука Сафонов, технический директор компании «Синклит», которая развивает платформу Bug Bounty Ru. Он цитирует руководство одного из предприятий, где говорят: «Наша компания не может иметь уязвимостей, поэтому никаких публичных программ».

Для многих компаний bug bounty это новый процесс, его еще нужно тестировать и налаживать. Бизнес подходит к этому осторожно и сильно перестраховывается. Чтобы лучше контролировать бюджет на вознаграждения и не получить чрезмерно много отчетов, не имея ресурса для должной обработки, клиенты сначала пробуют приватные программы, объясняет Евгений Волошин, директор блока экспертных сервисов BI.ZONE.

Обкатав этот процесс в закрытом режиме, некоторые компании затем переходят к формату открытой программы. Примером может служить Rambler&Co. У компании уже был опыт использования подобной программы в закрытом режиме, когда приглашают участвовать ограниченное число исследователей, а в сентябре 2022 года она объявила о запуске открытой программы bug bounty.

TAdviser насчитал порядка 40 компаний, в разное время объявивших о запуске открытых программ bug bounty. В их числе:

- Rambler&Co,
- VK (включая «Алгоритмику», «ВКонтакте», «Дзен», «Одноклассники», TAPM, «Тетрику», «Учи.ру», GeekBrains, Mail.ru, Skillbox, VK Cloud, VK Play и другие проекты),
- «СберМарке»,
- Delivery Club,
- Ozon,
- «Яндекс»,
- QIWI,
- «ПИК»,
- «Азбука вкуса»,
- «Авито»,
- «ЮMoney»,
- «Тинькофф»,
- «Лаборатория Касперского»,
- «СКБ Контур»,
- «Мамба»,
- Wildberries,
- банк «Точка»,
- Webinar.ru,
- Cloud4Y,
- Jivo,
- ISPSYSTEM,
- «Конфидент»,
- LiveAgent,
- Beget,
- «Центральная касса»,
- GetYourGuide,
- проект «Бессмертный полк» и др.

Кроме того, по информации TAdviser, приватными программами bug bounty отметились Skyeng, drive.ru (бесплатная), «Циан» (бесплатная), Альфа-Банк и Райффайзен Банк.

По данным, полученным от игроков рынка, пользоваться программами bug bounty только-только начинает и госсектор, но пока очень ограниченно и исключительно в приватном режиме. О причинах этого и перспективах подробная информация приведена в одном из блоков обзора ниже.

Компании проводят программы bug bounty как полностью своими силами, так и с помощью специализированных платформ. Об особенностях обоих подходов подробнее тоже будет рассказано в блоках ниже.

Что касается специализированных платформ для размещения программ bug bounty, до недавнего времени в России, как и в мире, наиболее популярной была HackerOne, запущенная в 2012 году и базирующаяся в Сан-Франциско (США). Ее пользователями являются многие крупные глобальные компании. Прибегают к ее услугам и госорганы, в том числе Минобороны США. И в поиске уязвимостей по программам, размещенным на HackerOne, участвуют исследователи со всего мира.

Среди российских пользователей HackerOne числились компании Mail.ru, Ozon, «Лаборатория Касперского», «Авито» и другие. Россия также была в тройке стран, чьи хакеры получали наибольшие объемы выплат на этой платформе.

Однако в марте 2022 года на фоне российско-украинского конфликта HackerOne отключила российских пользователей. В связи с этим возникла острая необходимость в развитии собственных аналогичных платформ. При этом из-за санкций российские платформы имеют ограничения по сравнению с такими глобальными платформами: в связи со сложностями по части международных платежей их исследовательская аудитория ограничена преимущественно белыми хакерами из России.

До 2022 года попытки создать российские аналоги HackerOne предпринимались, но, как правило, они оканчивались неудачей. Одним из первопроходцев был проект BugHunt, запущенный группой разработчиков еще в 2014 году. Первым его клиентом стал сервис DocShell — система комплексного управления ИБ. За три недели существования сервиса BugHunt и программы вознаграждения DocShell было получено почти 40 отчетов с информацией о различных «дырах». Несмотря на бодрое начало, BugHunt не «взлетел» и довольно скоро был вынужден закрыться.

TAdviser пообщался с источником, хорошо знакомым с историей запуска этого проекта. Он считает, что BugHunt опередил время: «Сейчас реакция рынка на кибербезопасность стала совсем другой, и законодательство в области ИБ стало значительно более комплексным, а в 2014-м даже услуги по выполнению требований закона № 152-ФЗ «О персональных данных» было сложно продвигать на рынке». Кроме того, команде BugHunt не хватило опыта в запуске стартапов и денег на маркетинг, добавил собеседник TAdviser.

По состоянию на октябрь 2022 года действуют три основные российские платформы для проверки защищенности внешней инфраструктуры с привлечением независимых исследователей. В частности, с февраля 2021 года работает платформа Bug Bounty Ru. В мае 2022-го в рамках международной конференции по практической кибербезопасности Positive Hack Days была представлена платформа Standoff 365 Bug Bounty, созданная российским разработчиком Positive Technologies. А недавно, в августе, на другой международной конференции по практической кибербезопасности — OFFZONE 2022 — была представлена платформа по поиску уязвимостей от BI.ZONE, «дочки» «Сбера».

Специализированные платформы для проверки защищенности внешней инфраструктуры с привлечением независимых исследователей

Ниже в таблице представлены некоторые характеристики основных существующих на текущий момент в России платформ bug bounty, актуальные на середину октября 2022 года.

Название площадки	Bug Bounty Ru	Standoff 365 Bug Bounty	BI.ZONE Bug Bounty
Компания	«Киберполигон», «Синклит»	Positive Technologies	BI.ZONE
Сайт	bugbounty.ru	bugbounty.standoff365.com	bugbounty.bi.zone
Примеры пользователей	Движение «Бессмертный полк», «СберМаркет», Тинькофф Банк	«Азбука вкуса», Rambler&-Co, VK	«Авито»
Запущена	Февраль 2021 года	Май 2022 года	Август 2022 года
Сообщество	OWASP, Telegram-канал	Positive Hack Days, Standoff, Standoff Talks, Telegram-канал	OFFZONE, Telegram-канал
Зарегистрировано хантеров, активных хантеров	Около 2500, 800	Более 2500, не делятся на активных и неактивных	Более 400, не делятся на активных и неактивных
Количество действующих программ bug bounty	Порядка 10	21 (запущенные отдельными брендами и чаще всего юристами, которые могут принадлежать одной материнской компании)	2
Рейтинг хантеров	+	+	+
Модели монетизации	Взимает процент от выплат хакерам, за хостинг (приватных программ и подбор хантеров) и триаж (разбор отчетов)	Годовая подписка, процент от выплат хакерам, дополнительные услуги (триаж отчетов, реализация недопустимых событий и др.)	Годовая подписка, которая дает возможность размещать программы на платформе. Выплата компаний комиссии BI.ZONE с каждого вознаграждения за подтвержденную уязвимость. Дополнительные услуги от BI.ZONE (например, триаж уязвимостей)

Источник: TAdviser

Примечание. В таблице выше использовались общедоступные данные, а также данные, предоставленные самими платформами, актуальные на середину октября.

Bugbounty.ru, запущенная раньше остальных, и Standoff 365 Bug Bounty к середине октября 2022 года привлекли сопоставимое количество участников. В Bugbounty.ru рассказали, что за время работы платформы через неё «белые хакеры» получили выплаты более 2 млн рублей.

Bl.ZONE Bug Bounty, самая молодая платформа, продолжает активно набирать аудиторию. По состоянию на середину октября на Bl.ZONE Bug Bounty более 400 зарегистрированных исследователей и ее используют две компании — Bl.ZONE и «Авито». На платформе пока что запущена публичная программа Bl.ZONE, а «Авито» готовит свою программу, рассказали TAdviser в компании. В сентябре компания докладывала, что спустя три недели после запуска программы зарегистрировавшиеся на платформе bug bounty багхантеры получили в общей сложности более 160 тыс. рублей за найденные уязвимости в рамках программы Bl.ZONE.

Ничто не мешает белым хакерам регистрироваться на всех трех площадках и участвовать в наиболее выгодных и интересных программах bug bounty. Лука Сафонов, технический директор «Синклит», считает, что спустя какое-то время все крупнейшие площадки bug bounty придут примерно к одинаковому количеству исследователей: по его оценке, это может быть порядка 4 тыс. специалистов.

Вместе с тем, само по себе количество хакеров на платформе не говорит о ее результативности, гораздо более важным показателем является количество получаемых валидных отчетов о найденных уязвимостях. Таковыми, как правило, считаются отчеты исследователей, по которым впоследствии выплачиваются вознаграждения.

Помимо трех вышеуказанных платформ стоит сказать еще об одной. В качестве площадки для запуска программы bug bounty специально для госсектора, крупнейших коммерческих компаний и повышения уровня защищенности объектов критической информационной инфраструктуры (КИИ) планировалось использовать национальный киберполигон. Об этом «Ростелеком» объявлял на ПМЭФ в 2021 году. Национальный киберполигон, в свою очередь, функционирует на базе ресурсов «Ростелеком-Солар», «дочки» «Ростелекома».

В «Ростелеком-Солар» в сентябре 2022-го рассказали TAdviser, что программа bug bounty действует на базе национального киберполигона с 2021 года, но каких-либо конкретных результатов работы этой программы сообщить не смогли.

«В рамках программы уже проведен ряд успешных исследований, расширяется круг вендоров, предоставляющих свои решения для тестирований. Однако в силу закрытого режима исследований мы не можем раскрывать их детали», — заявил Дмитрий Малинкин, замдиректора национального киберполигона компании «Ростелеком-Солар».

Цена вопроса для белого хакера и заказчика

Вилка размера вознаграждений, которые компании готовы выплачивать исследователям за найденные уязвимости, довольно широкая — от нескольких тысяч рублей до нескольких сотен тысяч. В отдельных случаях выплаты составляют более 1 млн рублей.

Размеры выплат зависят от ряда факторов: от бюджета, которым располагает компания, пользующаяся программой bug bounty, от того, насколько опасной является найденная уязвимость, от простоты ее эксплуатации и воздействия на данные пользователей.

В компании Cloud4Y рассказали, что, в частности, при оценке уязвимостей руководствуются своим экспертным мнением и шкалой рейтинга уязвимостей VRT (Vulnerability Rating Taxonomy). Вознаграждение в зависимости от критичности уязвимости составляет от 30 до 1000 долларов.

По данным, полученным TAdviser от специализированных платформ bug bounty, по состоянию на середину октября максимальный размер выплат по действующим у них программам — порядка 250–300 тыс. рублей.

Схожий максимум вырисовывается, если взглянуть на программы bug bounty, организованные компаниями на собственных ресурсах. Так, например, в программе bug bounty умных устройств с «Алисой» «Яндекса» вознаграждения варьируются от 15 тыс. до 300 тыс. рублей. Подробнее — в таблице ниже.

Таблица 3. Размеры выплат хакерам за найденные уязвимости по программе bug bounty умных устройств с «Алисой» «Яндекса»

Уровень опасности проблемы	Критический	Высокий	Средний	Низкий
Вознаграждение	300 000 ₽	150 000 ₽	75 000 ₽	15 000 ₽

Источник: «Яндекс»

А в честь десятилетия своей программы bug bounty «Яндекс» расщедрился и объявил, что победители конкурса, которые сообщат о найденной уязвимости в период с 20 сентября по 19 октября включительно, получат денежное вознаграждение, увеличенное в десять раз.

Очень крупное вознаграждение — до 1 800 000 рублей — за найденную уязвимость можно получить, например, и в VK.

Важно отметить что, несмотря на привлекательные денежные вознаграждения, зачастую это не является решающим фактором участия исследователя в bug bounty. Такие программы позволяют специалистам по ИБ легально пощупать безопасность интересных систем и приобрести ценный опыт. И, как можно заметить на рекрутинговом портале hh.ru, нередко опыт участия в bug bounty и положительный рейтинг на различных площадках bug bounty указывается в вакансиях в качестве требования к специалистам по ИБ. В Positive Technologies считают, что интересные задачи — это не менее важная мотивация к участию в bug bounty, чем деньги.

Что касается бюджета, который компании стоит закладывать на программу bug bounty, если она проводит ее на специализированной платформе, он должен включать:

- оплату подписки,
- выплату комиссии с оплаты хакерам за найденные уязвимости (если платформа взимает такую комиссию),
- непосредственно выплаты вознаграждения хакерам,
- накладные расходы на денежные переводы физлицу (хакеру).

Дмитрий Ким, бизнес-лидер Standoff в Positive Technologies, объясняет, что три последние указанные статьи расходов будут сильно зависеть от скоупа (scope), который определит для себя компания. Скоуп — это разрешенная область действий, устанавливаемые программой bug bounty границы, в рамках которых разрешено производить багхантинг. Чем шире скоуп, тем более крупный бюджет надо закладывать.

Основываясь на опыте работы платформы, своим клиентам с большим скоупом (более десяти полноценных многофункциональных веб-приложений) в Positive Technologies рекомендуют закладывать 5 млн рублей на год, и в эту сумму не входит стоимость подписки. При небольшом скоупе эта сумма может быть значительно ниже. За это время будет можно будет оценить объемы реально необходимых расходов, потому что нельзя заранее предсказать, сколько уязвимостей и насколько опасных найдут в системах исследователи: их может быть 10, а может и 100. Но при рекомендуемом объеме предусматриваемых средств в 5 млн рублей, как показывает практика Positive Technologies, заказчик не рискует ошибиться с бюджетом, и это позволяет ему комфортно пользоваться программой.

Вместе с тем, добавляя в компании, при формировании бюджетов разные заказчики отталкиваются от разных вещей: кто-то за точку отсчета берет стоимость определенного количества критически опасных уязвимостей, кто-то — определенный процент от своего бюджета на управление уязвимостями. Некоторые сначала запускают закрытую программу, смотрят, сколько отчетов о найденных уязвимостях приходит, и, оценив потенциальный поток, рассчитывают бюджет.

Причины обращения организаций к bug bounty

Опрошенные TAdviser компании, использующие программы bug bounty, объясняют преимущества этого подхода следующим образом:

- В первую очередь в bug bounty нас привлекает возможность постоянного контроля за уязвимостями и процессами в ИБ. Этот метод позволяет выявить ошибки и устранить их до того, как ими мог бы воспользоваться злоумышленник.
- Использование bug bounty в дополнение к существующим у нас внутренним системам ИБ позволяет усилить непрерывный анализ защищенности периметра и продуктов компании с привлечением множества независимых специалистов, таким образом масштабируя команду ИБ.
- Bug bounty позволяет передавать узкоспециализированную работу подрядчикам. Так мы можем экономить время фулстек-специалистов и распоряжаться им более эффективно.
- Загруженность штатных специалистов, которые не могут все свободное время посвятить поиску уязвимостей, — это тоже повод задуматься о привлечении добровольцев.
- Свежий и разнообразный взгляд на действующие системы защиты, проверка на прочность, желание развивать инфраструктуру дальше, перед этим убедившись в ее стабильности и надежности.
- С программой bug bounty служба ИБ более точно знает все свои слабые места и неработающие процессы и, следовательно, действует эффективнее.
- Позволяет обеспечить непрерывный анализ защищенности сервисов силами независимых исследователей безопасности, при этом сохраняется высокая экономическая эффективность.
- Желание стать сильнее, крепче в плане защищенности и в долгосрочной перспективе снизить затраты на киберзащиту.

«Стоимость найденной уязвимости в bug bounty в 7-9 раз ниже, чем в пентесте, так как вознаграждение выплачивается по факту найденной ошибки. При проведении исследования оплачивается время специалистов, потраченное на поиск уязвимости. В некоторых частных случаях экономия получается существенной», — говорит Алексей Гришин, руководитель направления bug bounty, VK.

«Bug bounty для ИБ — как специи для блюда»

При всех преимуществах bug bounty компании, использующие эту практику, и поставщики услуг, опрошенные TAdviser, единодушны, что она не заменит собой традиционные технологические решения и методы, такие как, например, сканеры безопасности и периодические пентесты. Bug bounty скорее является дополнением к существующим средствам защиты, позволяет дополнительно повысить уровень зрелости компании в области ИБ и дополнить безопасную разработку.

Руководитель направления bug bounty VK Алексей Гришин красиво описывает этот метод: «Bug bounty для ИБ — как специи для блюда».

«Bug bounty не заменяет традиционные решения, а дополняет их. Первые позволяют найти относительно простые уязвимости, а хакерам остается вручную искать небанальные, сложные», — говорит Евгений Руденко, директор по кибербезопасности Rambler&Co.

При этом при полном отказе от автоматизированных средств в программах bug bounty увеличивается число простых уязвимостей, и исследователи фокусируются на них, вместо того чтобы рассматривать действительно интересные кейсы, за которые можно получить большее вознаграждение.

Классические инструменты ИБ — для сетевой фильтрации, надежной аутентификации, авторизации и криптографии — будут актуальны в любом случае, считают в «ЮMoney». Bug bounty лишь дополняет этот набор и помогает находить недочеты в системах.

Bug bounty могут стать более выгодным и эффективным методом проверки защищенности в сравнении с классическим тестированием на проникновение. Как правило, пентесты проводятся в течение ограниченного времени, а их результаты заведомо непрогнозируемы. Программы bug bounty обычно рассчитаны на более длительный срок и углубленную работу, заказчики таких исследований платят исключительно за результат.

«С нашей точки зрения, максимальный эффект достигается при комбинированном использовании этих методов. Однако не стоит забывать, что внешние аудиты и программы bug bounty являются пусть и важной, но только частью мер, реализуемых при комплексной защите информационных систем», — отмечает директор Национального киберполигона компании «Ростелеком-Солар» Дмитрий Малинкин.

Бизнес-лидер Standoff в Positive Technologies Дмитрий Ким подчеркивает, что bug bounty очень комплементарна остальным процессам ИБ, которые есть у заказчика: компании делают и пентесты, выполняют анализ защищенности приложений, имеют цикл управления уязвимостями и другое. Bug bounty хорошо дополняет эти вещи, потому что сканеры, например, помогают находить уязвимости, но они несопоставимы с живым человеком по креативности подходов. Сканеры могут обеспечить порядка 80% результата, но остальные 20% нельзя получить автоматизированными средствами, говорит он.

«Это очень творческий процесс. От исследователя требуется проверка разных гипотез: что можно сломать, как можно это сделать», — говорит Дмитрий Ким.

Оценка эффективности программы

Общение с пользователями программ bug bounty показывает, что компании используют схожие подходы к оценке их эффективности. В «Авито», например, говорят, что, как правило, сопоставляют затраты на программу и результативность работ привлеченных исследователей. Исходя из этого можно делать выводы об эффективности работы программы.

В Cloud4Y результативность оценивается по количеству и опасности найденных уязвимостей. Но при этом компания не имеет права расслабляться: «Если багхантеры не шлют сообщения о серьезных проблемах, это не значит, что их нет. Их могли не найти или найти, но желать проэксплуатировать», — поясняет специалист по информационной безопасности Cloud4Y Виталий Павлов.

При проведении программы bug bounty на специализированной платформе наиболее сильно на эффективность влияют прозрачность программы, адекватные суммы вознаграждений, высокий уровень профессионализма триажеров и быстрые ответы, считает технический директор компании «Синклит» Лука Сафонов.

После получения данных об уязвимости для компании важно оперативно закрыть ее, чтобы не успела состояться эксплуатация. Дмитрий Ким из Positive Technologies говорит, что платформы bug bounty, как правило, не отслеживают, закрыла компания уязвимость или нет.

«Однако бывает, что заказчик снова обращается к исследователю, обнаружившему уязвимость, чтобы перепроверить ее и убедиться в том, что она закрыта», — поясняет он.

Сделай сам vs. багхантинг на платформе: что лучше

Как упоминалось ранее, компании, привлекающие белых хакеров, организуют поиск уязвимостей в своей IT-инфраструктуре с их помощью либо за счет собственных ресурсов, либо на специализированных платформах. Выбор подхода зависит от ограничений и условий, в которых существует компания.

«Оба этих подхода имеют право на существование, выбор компании зависит от ее приоритетов и готовности решать возникающие сложности самостоятельного управления программой. Например, надо решить, готова ли компания самостоятельно работать над организацией платежей и привлечением исследователей. Плюсы организации программы инхаус — полный контроль над процессом и экономия на сервисных сборах площадки», — считает Валентин Лякутин, руководитель продуктовой безопасности «Авито».

В VK поясняют, что для удачного запуска программы необходима платформа для обмена сообщениями с исследователями, внутренний трекер для отслеживания разбора багов, техническая команда для создания правил, исправления и валидации уязвимостей. Также необходимо использовать инструменты для привлечения исследователей, продумать каналы для выплаты вознаграждений.

Если компания решает организовать bug bounty самостоятельно, ей придется как минимум самой организовать взаимодействие с багхантерами — от привлечения их внимания до юридического оформления, говорит Евгений Волошин, директор блока экспертных сервисов BI.ZONE. Используя платформу bug bounty, компания снимает с себя рутинные действия и концентрируется только на закрытии найденных уязвимостей, верификация может быть осуществлена также силами платформы. Плюс бизнесу не нужно разбираться с юридической стороной выплаты вознаграждений багхантерам: все это уже налажено на стороне платформы.

Сами компании — пользователи специализированных платформ bug bounty, опрошенные TAdviser, приводят следующие аргументы в пользу их применения:

- Отдельная площадка для программы bug bounty — это удобно как для хакеров, так и для заказчиков. Первые могут в одном месте найти компании, которые готовы платить за найденные уязвимости, и, кроме того, не нужно дополнительно разбираться в особенностях оплаты конкретного заказчика. Вторые могут сэкономить на запуске собственной внутренней программы.
- Платформа выступает гарантом и экспертом в решении спорных ситуаций.
- Платформа агрегирует в себе множество вариантов оплаты работы исследователей, и самих исследователей тоже больше. Правда, количество в данном случае не обязательно переходит в качество.

Есть и мнение, что возможна, гибридная схема, то есть организация багхантинга собственными силами с применением внешней платформы; это оптимальный вариант.

«Внешние платформы могут стать посредниками в ситуации, когда обе стороны опасаются или не доверяют друг другу. Например, багхантер не уверен, заплатят ли ему за уязвимость, а компания — что человек получит деньги за найденную проблему не только от самой компании, но и от всех желающих. Внешняя платформа создает некоторое доверие. Наш опыт показывает, что удобно использовать внешнюю платформу. Она дает больший охват, статистику, гарантии. С другой стороны, не про все уязвимости хотелось бы говорить на сторонней площадке. Чем меньше людей знают о ней, тем спокойнее компании. Гибридная схема позволяет дать на откуп платформе небольшие уязвимости, а серьезные — обсуждать напрямую с багхантером», — объясняет Виталий Павлов, специалист по информационной безопасности Cloud4Y.

Перспективы и точки роста

Развитие ИТ и ИБ в России хотя и имеет региональную специфику, но в целом происходит в русле глобальных тенденций. А последние данные указывают на рост популярности программ bug bounty. Об этом говорит, в частности, [платформа HackerOne](#). Глобально расширяется спектр организаций, прибегающих к bug bounty: теперь этот метод используют в том числе небольшие компании и госорганизации. Растет и количество белых хакеров.

Аудитория белых хакеров, доступных для российских организаций, сузилась на фоне санкций и отказа иностранных платформ работать с россиянами. Кроме того, часть специалистов по ИБ, которые и ранее были в дефиците, уезжают за рубеж. Рынок ИБ довольно узкий, в нем есть косяк наиболее активных участников, какого-то значительного притока ждать пока неоткуда.

Придать импульс российскому рынку bug bounty могло бы развитие сотрудничества с азиатским рынком, включая сотрудничество в области платежных систем. Тогда исследовательская аудитория могла бы расшириться за счет специалистов, например, из Индии и других стран.

Как бы то ни было, некоторые опрошенные TAdviser заказчики, имеющие опыт в bug bounty, и представители российских платформ считают, что в ближайшем будущем популярность этого метода в России будет расти и что он может стать массовым. Так, Лука Сафонов прогнозирует, что «массовым он обязательно станет на горизонте двух-трех лет».

Евгений Волошин из BI.ZONE также считает, что в ближайшие годы bug bounty в России станет одним из популярных путей увеличения защищенности систем для бизнеса. При этом, полагает он, перспективы использования bug bounty в госсекторе не отличаются от перспектив для частного бизнеса: «Клиентам от государства придется подготовиться к bug bounty и четко понять, что они хотят получить».

Как уже говорилось, в России подавляющее большинство заказчиков программ bug bounty — это частный бизнес, но уже можно говорить, что интерес к этой практике как способу повышения уровня защищенности есть не только у него. В той или иной степени он также присутствует у госкомпаний, госорганов и в целом у владельцев объектов критической информационной инфраструктуры. Потенциально они могли бы составить существенную долю пользователей программ bug bounty.

За последнее время, особенно в 2022 году, значительно выросло количество кибератак на IT-инфраструктуру российских организаций, что связано среди прочего с текущей геополитической обстановкой. Это один из факторов, заставляющих обращать внимание на bug bounty, наряду с ростом спроса на средства защиты: организации сейчас вынуждены все больше фокусироваться на ИБ и готовы смотреть на самые различные опции для повышения уровня защищенности своей инфраструктуры.

Кроме того, ужесточение требований со стороны государства и усиление контроля за исполнением этих требований стимулируют организации повышать уровень зрелости процессов ИБ и обращать внимание на различные способы усиления защиты.

Вместе с тем даже при наличии интереса к bug bounty со стороны госсектора, госкомпаний и владельцев объектов КИИ есть ряд факторов, сдерживающих применение этой практики в данных сегментах в России. При этом регулярные пентесты с привлечением внешних исследователей в этих сегментах уже широко распространены и, более того, закреплены в нормативно-методических документах Банка России и ФСТЭК.

Ограничения для использования bug bounty

Один из ключевых барьеров, препятствующих сейчас более широкому распространению bug bounty в России, лежит в юридической плоскости. В «Ростелекоме», например, рассказали TAdviser, что их компания имеет опыт проведения программ и мероприятий типа bug bounty, однако в силу ряда организационных и юридических ограничений невозможно сделать это постоянной практикой.

«Программы и мероприятия типа bug bounty — достаточно перспективное решение для повышения уровня защищенности. Однако для применения этого решения в качестве стандартного механизма обеспечения ИБ, в частности для повышения уровня защищенности объектов КИИ, необходимо привлечение государства, чтобы создать юридические условия, которые позволят проводить такие мероприятия максимально прозрачно и, что важно, оперативно. При появлении юридической базы мы готовы использовать этот механизм в будущем», — говорят в «Ростелекоме».

На ту же проблему указывает директор Национального киберполигона компании «Ростелеком-Солар» Дмитрий Малинkin. В компаниях государственного сектора и на объектах КИИ тестирования с участием независимых исследователей в формате bug bounty практически не проводятся. Это объясняется отсутствием четкого законодательного определения деятельности по поиску уязвимостей.

«Строгость действующего законодательства в области КИИ и отсутствие четких границ, нормативно определяющих такие действия, служат барьером как для самих заказчиков исследований, так и для потенциальных исполнителей», — поясняет он.

Основные ограничения, затрудняющие использование bug bounty, связаны с отсутствием определения в законодательстве как самих исследований, так и их границ. Кроме того, в этой области отсутствует и правоприменительная практика. Поэтому проведение подобных мероприятий, особенно на объектах КИИ, может трактоваться неоднозначно с юридической точки зрения.

Юридические риски сейчас присутствуют как для заказчиков bug bounty из госсектора и субъектов КИИ, так и для белых хакеров: действия последних по поиску уязвимостей могут быть квалифицированы как неправомерный доступ к компьютерной информации в соответствии со ст. 272 УК РФ.

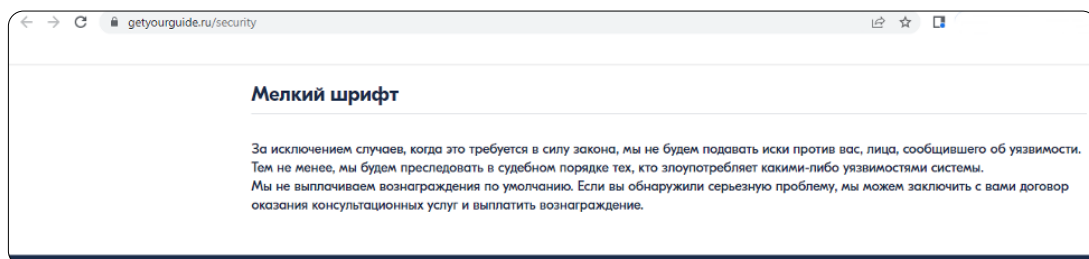


Рисунок 7. Скриншот с сайта проекта GetYourGuide

Роль государства

В распространении bug bounty сейчас заинтересованы профильные ведомства, в первую очередь Минцифры, что создает перспективы для снятия ряда юридических барьеров и более широкого применения этой практики, в том числе в госсекторе и на объектах КИИ.

Так, в мае 2022 года директор департамента обеспечения кибербезопасности Минцифры Владимир Бенгин (с 2019 года занимал в Positive Technologies должность директора департамента по развитию продуктового направления) в рамках форума Positive Hack Days 11 анонсировал планы запустить программу bug bounty для госсистем. А в начале октября министр цифрового развития Максют Шадаев на конференции TAdviser IT Government Day рассказал, что ведомство планирует провести до конца года bug bounty, в частности для «Госуслуг».

В июле 2022 года в СМИ появилась информация о том, что Минцифры работает над возможностью ввести понятие программы bug bounty в правовое поле. А в начале октября 2022-го Владимир Бенгин в интервью TAdviser сообщил, что ведомство уже прорабатывает вопрос внедрения практики применения программ bug bounty для всех владельцев государственных информационных систем.

В Минцифры рассчитывают, что в дальнейшем это должно стать примером и для госкомпаний, таким образом расширив область применения подобных услуг. Услуги белых хакеров могут использоваться здесь как расширение процессов управления уязвимостями в дополнение к сканерам безопасности и периодическим пентестам. Интерес к bug bounty в госсекторе, госкомпаниях и на объектах КИИ в Минцифры оценивают как очень высокий, говорил Бенгин в интервью.

Надо сказать, что идеи, связанные с тем или иным применением bug bounty, для Минцифры не новы. Они витали в ведомстве еще тогда, когда оно звалось Минкомсвязью. Например, в 2016 году в министерстве рассматривали возможность привлечения хакеров по модели bug bounty для поиска уязвимостей в софте, внесенном в реестр отечественного программного обеспечения.

На этот раз информация об активной работе ведомства по внедрению в массы практик bug bounty появилась вскоре после выхода Указа Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». В Минцифры говорили, что под действие этого указа попали сотни тысяч российских организации. В их числе — госорганы, госфонды, госкорпорации, системообразующие организации экономики, субъекты КИИ и ряд других.

Указ существенно меняет процессы ИБ на предприятиях, попадающих под его действие. Одно из нововведений — предприятия должны защитить себя от недопустимых событий, то есть событий, которые не должны быть реализованы и которые должны быть предотвращены в первую очередь.

Это означает, что в организации:

- Сформулирован перечень недопустимых событий и негативных последствий (ущерба) для организации.
- Проведена оценка возможности возникновения и реализации недопустимых событий путем моделирования целевых атак.
- Проводятся мероприятия по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- Проводится контроль эффективности (результативности) мероприятий по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).

А 13 мая 2022 года вышло Постановление Правительства РФ № 860 «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений». Он проводится с 16 мая 2022 года по 30 марта 2023 года, и ответственность за организацию и мониторинг



Некоторые эксперты в сфере ИБ после выхода указа № 250 обращали внимание на то, что понятие недопустимых событий в нем являются аналогом понятия негативных последствий по ФСТЭК.

работ, проводимых в рамках эксперимента, возложена на Минцифры. Один из пунктов эксперимента — участвующие в нем организации должны определить у себя недопустимые события.

Участие в эксперименте добровольное, но после его окончания, согласно постановлению № 860, предполагается распространить данный подход на все организации, подпавшие под Указ Президента РФ № 250.

На этом фоне Минцифры планирует создать реестр недопустимых событий в области кибербезопасности, который будет открыт для всех организаций. Об этом стало известно в августе 2022-го.

Услуги, связанные с реализацией недопустимых событий, Positive Technologies предлагает на своей платформе bug bounty, запущенной в мае 2022-го. Другие ИБ-компании вне платформ bug bounty также оказывают услуги, которые могут помочь организациям выполнять требования указа № 250. Так, в «Киберполигоне» и «Синклите» тоже работают с объектами, подпадающими под указ № 250, рассказал TAdviser Лука Сафонов. После выхода данного указа у предприятий возникло много вопросов касательно нововведений. Это, а также необходимость соответствовать новым требованиям, подталкивает их обращаться за услугами к профессионалам.

Надо сказать, что в целом последние обновления нормативной базы в области ИБ резонируют с концепцией создания качественно и количественно измеримых систем защиты информации, о которой не первый год говорят в разных компаниях в сфере ИБ. Так, например, «Лаборатория Касперского» еще в 2017 году представила свой принцип кибериммунитета. Основатель «Лаборатории Касперского» Евгений Касперский считает, что кибериммунитет должен прийти на смену принципу кибербезопасности. Кибериммунитет предполагает такой уровень защиты, при котором стоимость разработки атаки на компанию (или устройство, или пользователя) превысит сумму возможного ущерба.

«Безопасность должна лежать в основе каждой системы, а не быть надстройкой над ней, как это происходит сейчас. В таком случае у нас есть шанс сделать стоимость атаки настолько дорогой, что ее реализация будет просто бессмысленной. Это и будет основа безопасного цифрового мира», — говорил он.

В «Ростелеком-Солар» тоже озвучивают идею, что нужен новый подход к кибербезопасности, ориентированный на результат. «Бизнес не мыслит категориями функций ИБ и ИТ, для него значим только конечный результат — киберустойчивость», — высказывал мнение в интервью TAdviser в октябре гендиректор «Ростелеком-Солар» Игорь Ляпунов. Новый подход предполагает серьезный пересмотр подходов к менеджменту в области кибербезопасности. В этой парадигме Сколково запустило образовательную программу по управлению кибербезопасностью бизнеса для топ-менеджеров «Построение киберустойчивого бизнеса», где «Ростелеком-Солар» выступает партнером.

В 2021 году также Positive Technologies также озвучивала идею качественной и количественной измеримой системы защиты информации, когда рассказывала о планах запустить в России платформу по поиску уязвимостей и проводить программы bug bounty не только в традиционном, но и в новом формате. Последний предполагает формирование реестра недопустимых событий и выплату вознаграждения за цепочку атак, которая однозначно приведет к неприемлемому ущербу.

Говоря непосредственно о bug bounty, сейчас, по информации хорошо осведомленного источника TAdviser в индустрии ИБ, идеи распространения этой практики поддерживает не только Минцифры, но и ФСТЭК и еще ряд ведомств. Тот же источник говорит, что сейчас обсуждается, каким образом мог бы быть реализован ресурс для использования bug bounty госорганами.

Один из рассматриваемых вариантов — создание специальной площадки, что-то вроде государственной платформы bug bounty, где операторами выступали бы три уже известных игрока: Bugbounty.ru, Positive Technologies, BI.ZONE.

В случае с госорганами может потребоваться более сложная схема реализации программ bug bounty, чем для бизнес-заказчиков, говорит собеседник TAdviser. Например, может быть необходима авторизация через ЕСИА и допуск в закрытый контур так называемой государственной bug bounty только верифицированных хантеров с контролем их действий — чтобы кто-то из них что-нибудь не утаил или не «докрутил». Оператор сможет увидеть подобные вещи.

Теоретически подобная площадка могла бы быть создана под патронажем ФСТЭК (на базе БДУ ФСТЭК) или на базе НКЦКИ.

Источник TAdviser в Минцифры подтверждает, что обсуждается идея создания подобной площадки, и считает, что использование bug bounty могло бы радикально повысить защищенность госсистем и способствовать развитию рынка bug bounty. Вместе с тем, говорит он, в ведомстве неоднозначно относятся к созданию отдельной государственной платформы bug bounty из соображений, что чрезмерное вмешательство государства ни к чему и заказчики больше выиграли бы от свободной конкуренции.

Профессиональные площадки смогли бы более эффективно привлечь исследователей к госпрограммам bug bounty и провести триаж найденных уязвимостей. Поэтому альтернативой государственной bug bounty могла бы стать, например, разработка требований к госпрограммам bug bounty, а дальше госзаказчики действовали бы в соответствии с Федеральным законом № 44-ФЗ (о госзакупках), рассказывает источник.

Точные сроки, в которые планируется разработать и принять правовую базу, открывающую больше возможностей для применения bug bounty в новых сегментах, публично не озвучивались. Однако, судя по решительному настрою регулятора, вероятность, что эта инициатива будет доведена до конца, очень велика.

Выводы

Рынок bug bounty в России начал зарождаться примерно 8–10 лет назад. Среди первопроходцев на нем были крупные интернет-компании, затем пул пользователей таких программ расширился. Российский рынок сейчас можно назвать формирующимся, если сравнивать его с некоторыми другими странами, такими как, например, США, где к практике bug bounty прибегают уже не только крупный и средний бизнес, но и госсектор и небольшие компании. Более 50% программ bug bounty в России пока закрытые. При этом есть предпосылки для дальнейшего роста рынка: и благодаря государственным инициативам и регуляторным мерам в области ИБ, и из-за роста количества и сложности киберугроз.

Пользователи программ bug bounty в России сейчас представлены в основном частным бизнесом, преимущественно крупным и работающим в массовых сегментах, таким как интернет-сервисы, электронная коммерция, финсектор. Заметными пользователями программ также являются IT-компании. Тех, кто сейчас активно применяет bug bounty, характеризует наличие собственной разработки ПО и довольно зрелых процессов в области ИБ в компании.

При устранении юридических ограничивающих факторов, на которое сейчас направлена работа регуляторов, рынок bug bounty в России мог бы по аналогии с зарубежным опытом органически расти за счет появления программ bug bounty в большем спектре секторов экономики, чем сейчас. В том числе в госсекторе, в госкомпаниях, а также на объектах КИИ как расширение процессов управления уязвимостями. Предпосылки к этому уже есть. Способствовать тому, чтобы метод bug bounty стал более массовым, могло бы и расширение аудитории исследователей за счет вовлечения зарубежных белых хакеров.

Интерес к bug bounty в КИИ в первую очередь лежит в плоскости общего повышения защищенности КИИ. Вместе с тем новые регуляторные требования в области ИБ, в том числе обозначенные в майском Указе Президента № 250, создают предпосылки того, что субъекты КИИ будут более активно обращаться за услугами, связанными с реализацией недопустимых событий.

