4.3. Анализ концепции «этичный хакинг» (на примере платформы HackerOne)

Хакинг, как явление, возникло относительно недавно, получило развитие в условиях распространения информационно-коммуникационных технологий и глобальной сети Интернет. Данная деятельность представляет собой внесение изменений в состав программного обеспечения для достижения определенных (чаще всего, корыстных) целей. Данные несанкционированные измерения являются вредоносными и могут представлять серьезную угрозу личности, обществу и государству.

Для поиска и устранения уязвимостей, преднамеренно внесенных в программное обеспечение, производят тестирование программ, которое представляет собой процесс исследования, испытания программного продукта для проверки соответствия между реальным поведением программы и её ожидаемым поведением на конечном наборе тестов. Следует иметь в виду, что разработчики программных продуктов тоже ошибаются и, таким образом, необходима проверка на наличие ошибок до момента передачи программы заказчику или внедрения в состав информационной системы.

Состав хакерского сообщества весьма неоднороден. Кто-то из них специализируется на создании специальных вредоносных программ для мобильных приложений, другие создают программы-шифровальщики и т.д. Причем эта продукция поступает для продажи и обмена на «темные», нелегальные рынки (DarkMarkets).С составом и структурой подобных рынков, а также нелегальных информационных продуктов и услуг можноознакомиться в [1].

Таким образом, с одной стороны, существует сообщество, представители которой видят основную цель своей деятельности – внесение изменений в программное обеспечение для получения непричитающейся им выгоды. С другой стороны, создаются специализированные команды по поиску уязвимостей в программном обеспечении и их исправлению для приведения программ в необходимое состояние и отвечающее требованиям разработчиков и заказчиков. Члены первой группы называются хакерами, то вторая группа носит несколько названий – антихакеры, этические хакеры, пентестеры, охотники за уязвимостями (bughunters) и т.д. В настоящем материале нас будет интересовать именно деятельность второй группы и программы BugBounty [2,3], основной целью которых является обнаружение и устранение ошибок в программном обеспечении. Подобные программы BugBountyреализовывались ведущими компаниями, в их числе Yahoo, Google, Reddit, Apple, Microsoft и др.

Следует отметить, что в специализированной литературе, посвященной даннойпроблеме, можно выделить несколько направлений: борьба с хакерами [4,5], исторические аспекты развития хакерства и программных злоупотреблений [6,7], тесная связь с хакерскими атаками [8], этический хакинг [9,10], кибернетические риски [11], большая группа источников по практическому руководствухакингом [12,13], тестирование на проникновение [14], поиск угроз [15-17] и др.

Очень часто задают вопросы относительно характеристик хакеров, их половозрастном составе, образовании и т.д. В этом плане многие аналитические источники отмечают явление хакерской глобализации. Как правило, не существует официальной статистики, которая полностью характеризовала все аспекты деятельности хакеров. Следует иметь в виду, что чаще всего обращаются к так называемым «этическим хакерам», которые заняты поиском уязвимостей. Воспользуемсяотчетамии статистикой за несколько лет (2019-2022 гг.) известной фирмы HackerOne[18]. Эта фирма основана в 2012 г. и получила известность в области информационной безопасности за счет создания специальной платформы Bug Bounty (охота за ошибками), совмещающей бизнес и научно-исследовательскую деятельность в области информационной безопасности [19]. Представляет интерес определения таких категорий, как хакер и «программа BugBounty». Хакер – это тот, кто получает удовольствие от решения интеллектуальных задач и творческого преодоления ограничений. Программа Bug Bountyпоощряет хакеров, использовать стимулы, выявлять и сообщать о потенциальных уязвимостях безопасности, прежде чем они смогут быть использованы.

Взаимодействие фирмы и хакеров основано на программе выплаты вознаграждения за обнаружение проблем в безопасности сервисов и приложений отдельных компаний, которые, соответственно, являются заказчиками и определяют размер вознаграждения. Данные базируются на опросах респондентов, которые представляют хакерское сообщество, характеризует место проживания, мотивацию, основные цели и инструменты и т.д. Рассмотрим более подробно основное содержание данных разделов статистического отчета. Следует отметить, что собранная статистика базируется на результатах опроса пользователей и, по нашему мнению, не полностью отвечает требованию объективности. К сожалению, другие источники статистической информации полностью отсутствуют.

Статистический отчет состоит из нескольких разделов. Первый раздел «География» характеризует распределение хакеров по странам и континентам. Наличие хакеров отмечается практически повсеместно и зафиксировано в 150 странах. Наибольшая концентрация хакеров отмечается в Индии (27 % в 2018 г. против 23,3% в 2017 г.), затем США (11 % в 2018 г. против 19,9 в 2017 г.) и России (5 % в 2018 г. и 6,3% в 2017 г.) от общего количества хакеров.

Для нас представляет интерес данные о связи и уровне заработной платы хакеров и инженеров-программистов. В таблице 4.3 приведено сопоставление заработной платы хакеров и инженеров-программистов по отдельным странам. Следует обратить внимание на коэффициент (множитель), который характеризует отношение максимальной заработной платы к среднегодовой заработной плате инженера-программиста.

Сравнивая данные за ряд лет, следует отметить возросшее значение коэффициента, характеризующего отношение заработной платы хакера к среднегодовой заработной плате инженера-программиста для ряда стран. В частности, резко возрос коэффициент для таких стран, как Аргентина (с 15,6 в 2017 г. до 40,6 в 2018 г.), Египет (8,1 против 24,2), США (2,4 против 6,4), Китай (3,7 против 6,2). Для Индии данный коэффициент незначительно изменился в большую сторону (с 16,0 до 17,6).

Таблица 4.3

Соотношение максимальной заработной платы хакера и среднегодовой заработной платы инженера-программиста по странам в 2018 г. [20, p. 13]

№ п/п	Страна	Коэффициент, характеризующий отношение заработной платы хакера к среднегодовой заработной плате инженера-программиста
1	Аргентина	40,6
2	Таиланд	24,5
3	Египет	24,2
4	Индия	17,6
5	Гонконг	6,7
6	США	6,4
7	Швеция	6,3
8	Китай	6,2
9	Алжир	6,2
10	Канада	4,8
11	Пакистан	3,9
12	Марокко	3,8
13	Латвия	3,5
14	Бельгия	3,1
15	Филиппины	3.0
16	Австралия	3,0
17	Новая Зеландия	2,9
18	Германия	2,9
19	Португалия	2,9
20	Венгрия	2,7
21	Румыния	2,5
22	Чили	2,5
23	Эфиопия	2,5
24	Индонезия	2,4
25	Нидерланды	2,2

Дополнительно проанализируем раздел«Демография», в котором приведены данные о сообществе HackerOne. В частности, 9 из 10 хакеров моложе 35 лет, 8 из 10 являются самоучками, они пришли из различных отраслей, в том числе не связанных с информационными технологиями, более 40% хакеров тратят более 20 часов в неделю на поиск уязвимостей и обеспечивают интернет-приложения более безопасными.

Основу платформы составляет молодые люди в возрасте от 18 до 34 лет (84,1 %). Специалисты предпенсионного возраста составляют менее 1%. В то же время 6 % это молодые люди в возрасте 13-17 лет. Следует предположить, что именно данная группа имеет все перспективы превратиться в ведущих специалистов и увеличить численность возрастной группы 18-24 лет в будущем.

Уровень образования участников платформы Hackerone характеризуют следующие данные: прежде всего это студенты бакалавры – около 30%, студенты – около 25%, аспирантура – около 20%, непрерывное образование – 15%, другие формы – около 10%.

Каковы затраты времени хакерского сообщества Hackerone на свою деятельность? Ответ можно сформулировать следующим образом: затраты времени в неделю составляют от 1 до 10 часов – 35%, затраты от 10 до 20 часов – 25%, затраты времени в диапазоне 20-30 часов в неделю составляют 15%, от 30 до 40 часов – 10%, более 40 часов в неделю – 15%. Другими словами, затраты времени достаточно весомые – от 10 до 35% рабочего времени.

Анализ приведенных данных свидетельствует о том, что затраты времени практически по всем группам увеличились. Это может служить подтверждением роста временных затрат на поиск уязвимостей и других брешей в программном обеспечении.

Для нас представляет также интерес информация, которая характеризует опыт работы, накопленный участниками платформы. Участники с практическим опытом работы от 1 до 5 лет составляет большинство (более 70%). Группа с опытом 6–10 лет составляет около 20%, следующая группа (11–15 лет) составляет 6%, на долю персонала, имеющего опыт работы от 16 до 20 лет, приходится около 2%, столько же (2%) имеют работники с опытом свыше 21 года.

Следует отметить, что главенствующую группу составляют участники с опытом работы от 1 года до 5 лет (более 70%), что свидетельствует о наличии начинающих специалистов.

На какие объекты направлены усилия хакеров, свидетельствуют следующие данные. Основным объектом для взлома выступают вебсайты и это следует признать закономерностью. Последующими объектами для взлома являются следующие: технологии, которые используют пользователи и которые обрабатывают пользовательские данные; программный интерфейс приложений (API’s); программное обеспечение Интернета вещей; операционные системы; встроенное программное обеспечение для управления видеокамерами, микрокалькуляторов, сотового телефона, GPS-навигатора и т.д.; загружаемое программное обеспечение; операционная система и программная платформа для мобильных устройств, таких как смартфоны, планшетные компьютеры, телевизоры, медиаплееры, нетбуки и автомобили.

Сравнение соотношения объектов свидетельствует об устойчивом интересе хакеров к анализу вебсайтов (70,8% в 2018 г. и 72,3% в 2019 г.). Все остальные объекты характеризуются относительно небольшим объемом (от 1% до 7,50%). Но следует иметь в виду, что отмечается повсеместная тенденция роста внимания к взлому мобильных приложений.

Сложным и действенным вопросом является уточнение мотивации деятельности персонала. Следует подчеркнуть, что исследователи не всегда преследуют финансовую выгоду, любопытство – это постоянное качество в сообществе хакеров и их стремление сделать цифровые технологии более безопасными и доступными. Приведем список мотивов деятельности этических хаке-

ров: деньги; трудности при освоении программного обеспечения; изучение новых приемов; развлечения; выпендреж; в целях продвижения карьеры; помощь другим; делать добрые дела; защищать и защитить и многие др.

Следует отметить, что основные мотивы распределены практически равномерно. Отсутствует явный лидер в процессах мотивации. Финансовые стимулы, без сомнения, очень важны, но есть еще любопытство и искреннее желание помочь достижениям информационных технологий стать более безопасными для их пользователей. Щедрость и альтруизм также присутствуют, а также помощь и защита другим.

Особую опасность приобретает рост числа случаев мошенничества, связанное с мобильными технологиями и каналами связи [21]. Следует обратить внимание на возможность использования криминальными группами отдельных результатов этических хакеров в своей деятельности. Киберпреступность стала широко распространенной и прибыльной сферой деятельности. Обобщенная модель компьютерной преступности включает процессы создания вредоносного программного обеспечения и его использование во всех сферах, где используются достижения цифровой революции. Вполне очевидно, что в будущем пользователи, предприятия и организации, а также правительства будут сталкиваться с разрушительными атаками и их последствиями. Данная сфера криминальной деятельности получила название теневой цифровой экономики (ТЦЭ) и исследуется самым пристальным образомв [1].

Следует обратить внимание на перспективы ТЦЭ, которые напрямую связаны с развитием информационных и коммуникационных технологий и компьютерной преступностью. В частности, прогнозы до 2030 г., предложенные в [22], свидетельствуют о снижении преимуществ информационно-коммуникационных технологий (ИКТ) и росте издержек на ИКТ.

Следует принимать в расчет, что в составе затрат на ИКТ стоимость средств противостояния информационным угрозам будет постоянно возрастать и этот факт обязательно будет сказываться на снижении преимуществ и эффективности.

В заключение следует обратить самое пристальное внимание на разработку моделей и возможностей реализации процессов монетизации программных злоупотреблений. Необходимо исследование сценариев системы трансформации программных угроз в финансовыеидругие услуги, включая отмывание денег. Основное внимание необходимо направить на изучение сценариев проектирования программных злоупотреблений (например, программ-вымогателей), программных средств захвата и формирования сети ботнетов и т.д. Одновременно необходимо разрабатывать оценочные модели затрат на разработку программных злоупотреблений для получения сведений о потенциальной выгоде (прибыли) и системе противостоянияугрозам кибербезопасности.

Литература

1. Охрименко С., Черней В. Теневая цифровая экономика и ее основные сегменты. Человеческий капитал в модели устойчивого экономического роста России: Монография. – М.: Прометей, 2022. – 514 с.

2. Jackson J. Corporate Cybersecurity: Identifying Risks and the Bug Bounty Program. Wiley-IEEE Press, 2021.
3. SinhaS. Bug Bounty Hunting for Web Security: Find and Exploit Vulnerabilities In Web Sites And Applications. Apress/Springer, 2019. DOI 10.1007/978-1-4842-5391-5.
4. Lee T. Strategic Hacker. FeelzON, 2022.
5. Olson P. We Are Anonymous. Little, Brown and Company, 2012.
6. Middleton B. A History of Cyber Security Attacks: 1980 to Present. CRC Press, 2017.
7. Buchanan B. The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press, 2020.
8. Rakshit S.K.Ethical Hacker's Penetration Testing Guide: Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks, 2022.
9. HarperA.et al. Gray Hat Hacking: The Ethical Hacker's Handbook. McGraw Hill, 2022.
10. NexusR. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures. https://www.atlanticcouncil.org/wp-content/uploads/2015/09/risk-nexus-september-2015-overcome-by-cyber-risks.pdf (access date 27.09.23).
11. Ярошенко А.А. Хакинг на примерах Уязвимости, Взлом, Защита. 2-е издание. – СПб.: Издательство Наука и Техника, 2023. – 352 с.
12. Pease A. Threat Hunting with Elastic Stack: Solve Complex Security Challenges with Integrated Prevention, Detection, And Response. Packt Publishing, 2021.
13. Pruteanu A. Becoming the Hacker. Packt Publishing, 2019.
14. Pease A. Threat Hunting with Elastic Stack: Solve Complex Security Challenges with Integrated Prevention, Detection, And Response. Packt Publishing, 2021.
15. Bone J. Cognitive Hack. The New Battleground in Cybersecurity… the Human Mind. CRC Press, 2017.
16. Potter M. We Are All Targets. Hachette Books, 2023.
17. The 2019 Hacker Report. The Survey and Statistics of the Ethical Hacker Community. https://www.hackerone.com/ethical-hacker/2019-hacker-report-celebrating-worlds-largest-community-hackers (access date 28.09.23).
18. The 4th Hacker-Powered Security Report. https://www.hackerone.com/resources/reporting/the-4th-hacker-powered-security-report (access date 28.09.23).
19. Morbin T. Faces of Fraud 2023. The Evolution of Online Fraud in 2023 and Best Practicesto Plug the Gaps. https://www.bankinfosecurity.com/evolution-online-fraud-in-2023-best-practices-to-plug-gaps-a-23094 (access date 29.09.23).
20. The 2019 Hacker Report. The Survey and Statistics of the Ethical Hacker Community. P.11. https://www.hackerone.com/resources/the-2019-hacker-report (access date 24.09.23).
21. Overcome by cyber risks? Economic benefits and costs of alternate cyber futures. https://www.atlanticcouncil.org/images/publications/risk-nexus-september-2015-overcome-by-cyber-risks.pdf (access date 28.09.23).
22. OhrimencoS., OrlovaD., CerneiV. Cyber Threats Modeling: An Empirical Study. Business Management. D.A.Tsenov Academy of Economics, Svishtov, Year XXXIII, Book 3, 2023. – P. 90-106. DOI: https://doi.org/10.58861/tae.bm.2023.3.06.

Вклад авторов распределился следующим образом:
Орлова Д.Р. – 4.3; **Охрименко С.А.** – 4.3; **Черней В.А.** – 4.3.

(Введение, стр. 8)