УДК 004.056
DOI: 10.18101/978-5-9793-1397-9-92-96

ХАКЕРЫ В СОВРЕМЕННОМ МИРЕ

© **Нечкин Вадим Николаевич**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: nechkin@yandex.ru

© **Михайлов Роман Дмитриевич**
студент,
Бурятский государственный университет имени Доржи Банзарова
Россия, 670000, г. Улан-Удэ, ул. Смолина, 24а
E-mail: nechkin@yandex.ru

Интернет становится самым популярным средством коммуникации в современном мире, а хакерство — неотъемлемой частью информационного общества. В настоящее время эта проблема имеет глобальные масштабы и касается каждой развитой страны. В последние годы хакеры широко используют методы социальной инженерии. В условиях глобальной информатизации изучение субкультуры хакеров приобретает стратегическое значение. Предотвращение хакерских атак и привлечение хакеров к конструктивной деятельности — важнейшая задача обеспечения национальной безопасности в информационной сфере.

Ключевые слова: хакер; «белые шляпы»; хакерское сообщество.

Хакерство становится неотъемлемой частью современного информационного общества. По роду своей деятельности именно хакеры задают вектор и специфику развития информационного общества, создают, трансформируют, предопределяют его будущее.

Слово хакер произошло от английского «to hack» — рубить, кромсать. Раньше хакером называли высокопрофессионального компьютерного специалиста, который решал компьютерные проблемы нестандартным образом. Другими словами, это был компьютерный гений, который творчески подходил к решению запутанных, сложных задач и мог быстро исправить ошибки в программах нестандартным образом.

В настоящее время значение слова «хакер» изменилось, и сейчас обычные пользователи интернета считают хакера компьютерным взломщиком. В английском есть также слово «cracker», от «to crack» — раскалывать, разламывать. Но среди обычных пользователей распространение получило именно слово «хакер», обозначающее компьютерного взломщика [1].

Существуют понятия «белый хакер» и «черный хакер». Белые хакеры находят изъяны в компьютерных программах и пытатся их устранить. Чер-

ные хакеры тоже ищут уязвимости в программах, но используют их в корыстных целях.

Эксперты из «Лаборатории Касперского» насчитали несколько десятков тысяч хакеров в 14 объединениях. Самые многочисленные — финансовые киберпреступники, специализирующиеся на атаках на банковскую инфраструктуру, бизнес и физических лиц.

Самыми технически оснащенными и продвинутыми являются специалисты по шпионским программам, самыми рискующими — дропы — люди, ответственные за контакты с физическим миром, а также ботоводы, или операторы, которые дистанционно управляют вредоносным компьютерным ПО.

Многие хакеры не заинтересованы в нанесении какого-либо ущерба и разглашении конфиденциальной и тем более секретной информации, их мало привлекают данные, перерабатываемые компьютерной системой. Таких хакеров интересует сама система как сложный программно-аппаратный комплекс, способы проникновения в систему, исследование ее внутренних механизмов и возможности управления ими, а также использование этой системы для доступа к другим системам.

Габриэлла Колман более 10 лет изучает хакерскую субкультуру и занимается исследованием деятельности группы «Анонимус» (Anonymous — международная сеть активистов и хакеров). По ее мнению, хакеры — не киберпреступники, а зачастую люди с активной политической позицией и либертарианскими взглядами. Деятельность хакеров — это не страсть к разрушению, как любят считать многие журналисты, а осознанная политическая позиция, основанная на антиавторитаризме, недоверии к власти и поддержке свободного рыночного капитализма.

На сетевом сленге этичных хакеров часто называют «белыми шляпами», потому что образно они стоят на стороне добра и используют свои навыки для проверки безопасности компьютерных систем, в отличие «черных шляп» — хакеров, которые занимаются взломом ради наживы. Этичных хакеров находят с помощью специальных зарубежных платформ, самые популярные из них Bugcrowd, HackerOne, Synack и Cobalt.

По данным площадки Bugcrowd, возраст 94% зарегистрированных на ней этичных хакеров составляет от 18 до 44 лет. Многие из них все еще учатся в средней либо старшей школе. При этом 50% указали, что занимаются исключительно фрилансом и не собираются переходить на постоянную работу.

Крупные компании готовы платить большие суммы взломщикам по найму. Например, Tesla и IJet платят хакерам от 1 до 15 тыс. долл. за найденную ошибку или лазейку в системе в зависимости от ее сложности и серьезности проблемы, Mastercard — от 3 тыс. долл. Такая практика поиска ошибки за вознаграждение носит в профессиональном сообществе название Bug Bounty («баг баунти» — награда за найденный баг). В американских компаниях существует довольно распространенная практика создания отдельных Bug Bounty программ, когда любой пользователь может сообщить о дырах в безопасности.

В мире этичных хакеров есть и свои культовые фигуры, некоторые из них имеют криминальное прошлое, хотя это довольно редкое явление. Яркий пример — Кевин Митник, который провел почти 6 лет в тюрьме за многочисленные взломы. Среди его жертв были министерство обороны США, Sun Microsystems, Novell, Motorola, DEC, NASA, The Well, Netcom, DEC, CSCNS, MTI и многие другие. После освобождения Митник снял «черную шляпу» и стал экспертом в области информационной безопасности.

С каждым годом потребность в «белых хакерах» растет, компании нанимают их для проведения внешних и внутренних пентестов. Это предоставляет возможность проверить защиту инфраструктуры той или иной компании, чтобы в будущем найти эффективные пути для минимизации рисков хакерских атак и их последствий [2].

Многие IT-компании извлекают выгоду из деятельности хакеров. При этом фирмы, естественно, хотят иметь дело только с «белыми шляпами». Хакеры информируют производителей о слабых местах их продукта. Примером таких разработчиков может служить компания Microsoft, которая из «врага всех хакеров» превратилась в уважаемого партнера по переговорам в вопросах безопасности. Корпорация из Редмонда больше не чужается контактов с компьютерными гиками, разбросанными по всему миру. «Раньше мы придерживались правила “они против нас”. Хакеры были для нас исключительно противниками, которых мы в лучшем случае игнорировали», — рассказывает Сара Блэнкиншип, менеджер по стратегии безопасности Microsoft. Она руководит небольшим количеством сотрудников, которые поддерживают контакты с лучшими умами всемирного сообщества хакеров, проводят совместные конференции Black Hat, посвященные вопросам безопасности. Сегодня почти каждая уязвимость в продуктах Microsoft была ликвидирована благодаря сведениям, полученным концерном от исследователей систем безопасности. Однако корпорация из Редмонда не платит денег своим информаторам — слишком велик страх стать объектом шантажа.

Одним из тех, кто неоднократно оказывал помощь Microsoft, является американский «хакер в белой шляпе» Дэн Камински — 32-летний любитель футболок с кричащими сюжетами, который работал в этой компании в качестве консультанта. Он принадлежит к кругу выдающихся хакеров, которым софтверный гигант позволяет «копаться» в своих технологиях.

Платформа HackerOne, объединяющая уже более 300 тысяч специалистов в области информационной безопасности, опубликовала исследование 2019 Hacker Report, в котором подвела итоги ушедшего года. В отчете сообщается, что в 2018 г. «белые» или «дружественные» хакеры, помогающие компаниям выявлять и устранять уязвимости в киберзащите, в сумме получили за свои услуги 19 млн долл. США. Результат вдвое превысил показатель 2017 г. и почти сравнялся с общей суммой вознаграждений, выплаченной хакерам за предыдущие шесть лет, — подсчитали в HackerOne.

Также отмечается, что участники платформы — хакеры из более чем 150 стран мира — по состоянию на конец 2018 г. сообщили о более чем 93 тыс. ныне исправленных уязвимостей и совместно заработали 42 млн

долл. Цель платформы — к завершению 2020 г. довести суммарный результат до 100 млн долл., — отмечает Bleeping Computer.

Более половины (51%) представителей хакерского сообщества, которые в рамках мероприятий Bug Bounty за деньги находят слабые места в ПО и бреши в киберзащите сайтов, проживают в таких странах, как Индия, США, Россия, Пакистан и Великобритания. Однако в HackerOne отмечают расширение своей географии — в 2018 г. к платформе впервые присоединилось шесть африканских государств. О растущей глобализации говорит и то, что теперь индийские и американские хакеры составляют около 30% общего числа участников HackerOne, тогда как в предыдущем году их было 43%.

В последние годы хакеры широко используют методы социальной инженерии: «обмен опытом» на хакерских сайтах свидетельствует о повышенном внимании к способам манипулирования людьми и создания программируемой модели поведения человека. Данный социокультурный феномен, отличающийся собственным ценнностным строем, обычаями и нормами, существует уже несколько десятилетий, и накоплен значительный эмпирический материал. В условиях глобальной информатизации выдвижения на первый план методов информационной войны и промышленного шпионажа, изучение субкультуры хакеров приобретает стратегическое значение. Предотвращение хакерских атак и привлечение хакеров к конструктивной деятельности — важнейшая задача обеспечения национальной безопасности в информационной сфере [3].

Кроме изучения общих тенденций развития хакерской субкультуры важен анализ хакерства в рамках той или иной культурно-исторической традиции. Та сомнительная польза, которая приписывается некоторыми людьми явлению хакерства, перекрывается значительным вредом, которое оно приносит человечеству. И вряд ли можно говорить о каком-то особом «антихакерском» воспитании, однако в современном педагогическом процессе необходимо учитывать эти новые реалии и опасности. Важно прививать прочные привычки к безусловно честной и ответственной деятельности, при которой человек не станет отнимать средства у других людей, портить их имущество, результаты труда и настроение даже таким малозаметным способом, как преступное программирование.

Литература

1. Скородумова О. Б. Хакеры как феномен информационного пространства // Социологические исследования. 2004. № 2.

2. Терин В. П. Хакер — хулиган или преступник [Электронный ресурс]. URL: http://www.za-nauku.ru//index.php?option=com_content&task=view&id=6898 &Itemid=39 (дата обращения: 10.04.2019).

3. Фленов М. Компьютер глазами хаккера. СПб.: БХВ-Петербург, 2012.

HACKERS IN THE MODERN INFORMATION SPACE

Vadim N. Nechkin
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: nechkin@yandex.ru

Roman D. Mikhailov
Student,
Dorzhi Banzarov Buryat State University
24a Smolina St., Ulan-Ude 670000, Russia
E-mail: nechkin@yandex.ru

The Internet is becoming an increasingly common means of communication in the modern world, and hackers are an integral part of the information society. At the moment, the problem is global in scope and affects every developed country. In recent years, hackers have widely used social engineering methods. In the context of global informatization, the study of the subculture of hackers acquires strategic importance: in the conditions of intensifying hacker attacks, preventing the destructive activities of hackers and involving them in constructive activities is the most important task of ensuring national security in the information sphere. The article provides an analysis of the hacker community.

Keywords: hacker; «white hats»; hacker community.