Как мы уже отмечали ранее в книге «Viruses, Hardware and Software Trojans», спецслужбы разных стран мира активно (обычно негласно) сотрудничают с различными хакерами, попавшими в их «поле зрения» (как «белыми», так и «черными», и «серыми»). Формы такого «сотрудничества» могут быть самыми разными, например, известно, что у некоторых киберпреступников в результате их «профессиональной деятельности» под контролем могут находиться одновременно от 500 тысяч до 1 миллиона «взломанных» компьютеров по всему миру. А ведь это не только доступ к банковским данным, но и к личной переписке, фото/видеоархивам, международным картам и т.д.

И пока киберпреступник похищает деньги и некую целевую секретную информацию, очень часто «за его спиной» стоят власти (точнее их специалисты), использующие вскрытую ими масштабную преступную схему для проведения своих специальных разведывательных операций, таким образом не утруждая себя сложной работой по организации взлома защищенных компьютерных сетей. Ведь на такой «взломанный» компьютер можно посылать запросы о получении любой другой информации, представляющей интерес для государственных разведывательных структур, причем установить – кто именно посылает эти запросы, практически невозможно.

А ведь в числе взломанных таких компьютеров почти наверняка бывают и компьютеры правительственных чиновников, военных, дипломатов, политиков, менеджеров и сотрудников крупных компаний. Одной из первых о возможности такого «технического симбиоза» еще в 2017 году сообщала газета The New York Times (https://www.nytimes.com/2017/03/12/world/europe/russia-hacker-evgeniy-bogachev.html), приведя в качестве примера случай с Евгением Богачевым, обвиняемым в США в многочисленных случаях взлома сетей самых различных организаций и банков и похищения с банковских счетов сотен миллионов долларов. Такие хакеры обычно «работают по совместительству», выполняя просьбы разведки, будь то в целях экономического шпионажа или «обычного» шпионажа.

Как говорят независимые эксперты (https://meduza.io/feature/2019/12/11/ruchnye-hakery-ekstravagantnye-millionery), ***первые столкновения кибермошенников со спецслужбами почти никогда не заканчиваются тюрьмой***, приводя в качестве примера историю так называемой российской хакерской группы Evil Corp. Например, спецслужбы могут обращаться к ним по поводу освобождения денег с заблокированных в связи с санкциями банковских счетов за рубежом и для оказания целого ряда аналогичных «деликатных услуг».

1.6. Этичные хакеры и хактивисты – мифы и реалии

1.6.1. Этичный хакинг – что это такое?

Здесь мы очень кратко рассмотрим тему «белых шляп», или как они часто себя называют – ***этичных хакеров, а также так называемых хактивистов,*** и покажем, что некоторые из них также представляют собой угрозу кибербезопасности в силу «своеобразного» понимания ими термина «этика». Как сказано в википедии – **Этичный хакер**, или **белый хакер**, а также на сетевом сленге **белая шляпа** (от англ. *White hat*) – специалист по компьютерной безопасности, который специализируется

на тестировании безопасности компьютерных систем. В отличие от черных шляп (черных хакеров), белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищенным.

В отличие от черных хакеров, чьи действия подпадают под статьи 272 (Неправомерный доступ к компьютерной информации), 273 (Создание, использование и распространение вредоносных программ для ЭВМ), 274 (Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети) УК РФ, ***действия белых хакеров не подпадают под статью УК***.

Одним из первых примеров этического взлома была «проверка безопасности» ОС Multics, проведенная в ВВС США. Их оценка показала, что «безопасность Multics была значительно выше, чем у других систем в то время». Они провели тесты, направленные на сбор информации, а также непосредственные атаки на безопасность ОС, направленные на вывод ее из строя. Также известно о других этических взломах в вооруженных силах США, официальных отчетов о которых не опубликовано.

Идея использования методик «этического взлома» с целью повышения безопасности в Интернете и локальных сетях была предложена Dan Farmer и Wietse Venema. Они вручную проанализировали множество систем с целью получения данных и контроля над жертвой. После чего они собрали все инструменты, которые они использовали для взлома в одной программе. Их программа получила название SATAN, или «инструмент администратора безопасности для анализа сетей» (от англ. Security Administrator Tool for Analyzing Networks).

Самые известные белые хакеры: Eric Corley, Przemysław Frasunek, Raphael Gray, Barnaby Jack, Митник Кевин (*Kevin Mitnick*), Agha S (*Aexa C*), Моррис Роберт Тэппэн (*Robert Tappan Morris*), Поулсен Кевин (*Kevin Poulsen*).

Этичный хакинг, также известный как «вайт хет хакинг» или «взлом белой шляпы», представляет собой процесс вторжения в систему или сеть с целью обнаружения образцов вредоносных программ и уязвимостей, которые могут быть обнаружены вредоносными скриптами или эксплойтами, что приводит к серьезным убыткам в виде потерянных данных.

Считается, что основная цель этичного хакинга – повысить уровень безопасности. Образцы вредоносных программ и уязвимости, обнаруживаемые этичными хакерами, часто исправляются во время тестирования. Несмотря на то что этичные хакеры часто применяют те же инструменты и методы, которые используются киберпреступниками и злоумышленниками, этичные хакеры имеют разрешение уполномоченной стороны на выполнение взлома. Кроме того, все обнаруженные уязвимости, как ожидается, будут сообщены руководству в процессе тестирования.

Этичные хакеры, также называемые *тестировщиками проникновения* или *хакерами в белой шляпе*, действительно являются опытными хакерами-профессионалами, которые выявляют и используют слабые места и уязвимости в целевых системах/сетях. В отличие от «злонамеренных» хакеров (*черных шляп*), вместо того, чтобы воспользоваться преимуществами обнаруженных уязвимостей, этичные хакеры работают с разрешения авторизованного руководства и должны соблюдать все правила управления и законы страны.

Стоит отметить, что этичные хакеры нередко становятся белыми шляпами, уже будучи злонамеренными хакерами, решая использовать свои навыки и приемы для

достижения позитивных целей. Тем не менее хакеры в белых шляпах также нередко легко меняют свои белые шляпы на черные.

Этичные хакеры часто ***руководствуются тремя основными принципами — конфиденциальность, целостность и доступность***. Эти три принципа составляют *Треугольник ЦРУ*. Они используются для достижения гармонии трех принципов для повышения уровня безопасности организации. Первоначально Триада ЦРУ была разработана для руководства политиками информационной безопасности в организации. Эта модель также упоминается как *триада AIC*.

Этичные хакеры должны обладать «огромным количеством технических знаний о ИТ-системах и программном обеспечении и, в частности, о том, как использовать их уязвимости». Ряд сертификатов, таких как наиболее распространенные сертификаты EC-Council Certified Ethical Hacker Certification или Communication-Electronics Security Group (CESG), также необходимы для выполнения какого-либо теста на проникновение в организацию (http://bedynet.ru/%D1%87%D1%82%D0%BE-%D0%B2%D0%B0%D0%BC-%D0%BD%D1%83%D0%B6%D0%BD%D0%BE-%D0%B7%D0%BD%D0%B0%D1%82%D1%8C-%D0%BE-%D1%8D%D1%82%D0%B8%D1%87%D0%BD%D0%BE%D0%BC%D1%83-%D1%85%D0%B0%D0%BA%D0%B8%D0%BD%D0%B3%D1%83/).

Существуют также различные сертификаты тестирования начального уровня, разработанные для тех, кто желает работать в команде тестирования и управляться руководителем группы.

Согласно PrepAway, топ-7 сертификатов этичного взлома включают сертификат этичного хакинга (CEH), сертификат тестера проникновения GIAC (SANS GPEN), сертификат специалиста по безопасности (OSCP), CREST, Foundstone Ultimate Hacking, сертификат по взлому инженера-тестера (CTPC) и сертификат инженера по тестированию хакинга (CPTE). Сертификаты квалифицируют человека как сертифицированного этичного хакера и предоставляют различные преимущества для отдельных лиц, поскольку это помогает понять риски и уязвимости, влияющие на организации, показывают инструменты торговли, технических хакеров, различные виды средств для подбора отпечатков пальцев, контрмеры и инструменты для снятия отпечатков пальцев и многое другое.

Этичные хакеры чаще всего используют свои умения и экспертизу для обнаружения уязвимостей в цифровых системах и их устранения в рамках баунти-программ или же полноценного коммерческого контракта. Главным отличием таких хакеров является то, что ***они взламывают системы с разрешения владельцев***, что делает процесс законным. В криптовалютной индустрии такие специалисты помогают возвращать украденные у пользователей средства или же устранять уязвимости еще до того, как ими успеют воспользоваться.

Существуют и «свободные художники», которые тестируют цифровые системы на предмет устойчивости к различным атакам без разрешения их владельцев, однако делают это для саморазвития или же в надежде получить компенсацию в случае обнаружения багов (*баунти-хантеры*). Чаще всего они не эксплуатируют найденные уязвимости, однако в некоторых случаях могут опубликовать информацию о них в общем доступе.

Этичные хакеры, непосредственно не задействованные в преступлениях и кибертерроризме, исповедуют так называемые ***этические принципы (стандарты)***. Эти стандарты были по большей части выработаны в Массачусетском технологическом институте (MIT), и считается, что впервые сформулированы в книге «Хакеры: герои компьютерной революции« журналиста Леви Стивена:

1. Делиться знаниями, вся информация должна быть доступной.
2. Не доверять конкретным авторитетам (обладающим властью), способствовать децентрализации и свободному доступу к компьютерным технологиям.
3. Делать мир лучше (защищать демократию и фундаментальные права).
4. Оценивать других представителей сообщества только по их достижениям, а не вероисповеданию, расе, политическим убеждениям или наградам.

Похожими принципами руководствовались в свое время и *«шифропанки»* в США, когда боролись за отмену ограничений на экспорт криптографических технологий, которые долгое время использовались исключительно в военных целях и поэтому засекречивались в соответствии с всевозможными бюрократическими правилами.

1.6.2. Наиболее известные группировки хактивистов

Значительной части сообщества хакеров свойственны определенные политические убеждения в контексте защиты свободы слова, свободы информации и других прав человека в целом. Они используют свои знания и умения для продвижения этих ценностей, хотя нередко подвергаются критике за радикализм даже со стороны самого хакерского сообщества. Эта философия получила название ***хактивизм*** (акты гражданского неповиновения и протеста в сети), а ее методы часто схожи с кибертерроризмом, хотя цели здесь стоят совершенно другие.

У этого идеологического направления есть и прямой конкурент: ***патриотический хакинг***. Участники этого движения твердо уверены в существовании неких врагов государства: будь то террористы, слишком надоедливые критики или даже другие государства. Используя свои хакерские навыки, они стремятся максимально навредить таким субъектам или же заблокировать их ответные атаки. В любом случае – если только это не *патриоты, находящиеся на службе в соответствующих ведомствах*, их действия обычно считаются незаконными.

Хорошим примером в этом контексте является широко известный ныне бывший успешный сотрудник АНБ и ЦРУ Эдвард Сноуден, который долгое время «верил в американское правительство» и помогал ему создавать цифровые системы для массовых слежек за людьми по всему миру вплоть до того момента, когда *совесть* не вынудила его последовать одному из основополагающих хакерских принципов (информация должна быть открытой) и рассказать обо всем миру.

В мире сегодня существуют десятки хакерских группировок, а также тысячи специалистов-одиночек. Тем не менее большинство этих «распределенных сообществ» известны лишь в узких кругах и спецслужбам. Однако есть и те, кто заявили о себе на весь мир. Более подробную информацию о них можно посмотреть, например, на сайте https://forklog.com/anatomiya-hakerskih-gruppirovok-kto-i-zachem-vzlamyvaet-tsifrovye-sistemy/.

И здесь группировка ***Anonymous*** является если не крупнейшей сетью хактивистов в мире, то уж точно одной из наиболее известных. Большинству телезрителей и пользователей интернета маска Гая Фокса знакома по фильму «V – значит вендетта»; стало ли это причиной, по которой сторонники Anonymous выбрали ее в качестве одного из символов своего движения, неизвестно, однако сам факт уже говорит о том, какие именно убеждения отстаивают эти люди.

Их лозунг: *«Коррупционеры боятся нас, честные поддерживают нас, а герои к нам присоединяются»*.

Anonymous ратует за анонимность и тотальную свободу в Интернете, не приемлет никаких ограничений государства на деятельность в сети. У группировки нет ярко выраженного лидера, иерархии или структуры сообщества, однако в нужный момент их действия всегда отлично скоординированы и беспощадны.

«Мы – Anonymous. Мы – Легион. Мы не прощаем. Мы не забываем. Ждите нас», – так звучит еще один девиз сообщества».

Примечательно, что целью акций Anonymous являлись не только правительственные сайты по всему миру, но и корпорации, частные лица и даже Церковь Сайентологов. Известно, что группировка ополчилась на всех участников блокады WikiLeaks после публикации на сайте организации разоблачающих данных об американском правительстве. Тогда досталось Mastercard, PayPal, Visa, Amazon, некоторым политикам, адвокатам и властям Швеции. Операция получила название «Расплата«.

Anonymous также осуществляли атаки против правительства Египта, российского молодежного движение «Наши», а также других проправительственных сайтов в РФ, против Интерпола, Ватикана, Европарламента и «Исламского государства». Группировка также активно защищала сервисы Pirate Bay, MegaUpload Кима Доткома и EX.UA, выступая против антипиратских кампаний.

Еще одной бесспорно известной группировкой хактивистов являлась ***LulzSec***. В отличие от Anonymous, в этой организации, вероятно, состояло всего шесть человек и у нее был лидер, который в итоге сдал участников властям. Изначально организация совершала атаки смеха ради, однако впоследствии переориентировалась на политически мотивированные действия.

Ее жертвами стали Сенат США, ЦРУ, корпорация Sony, социальная сеть LinkedIn и другие. Группа также принимала участие в операции Antisec совместно с Anonymous и другими хакерами.

Примечательно, что некоторые обозреватели считают хактивистами и группу ***Lizard Squad*** («Отряд ящериц»), однако ее представители так и не объяснили, с какой целью совершали атаки против онлайн-игр, северокорейского интернета и малайзийских авиалиний.

Если говорить о России, то наиболее известной хакерской группировкой, осуществляющей атаки на цифровые системы РФ и политических деятелей страны, является ***«Анонимный интернационал»*** или ***«Шалтай-Болтай»***.

Среди группировок, которые так или иначе причисляются к хактивистам, числятся также ***RedHack***, ***Cult of the Dead Cow***, ***Chaos Computer Club*** и многие другие. Стоит отметить, что в последнее время хакерские группы, распространяющие секретную информацию о деятельности спецслужб западных стран, в частности – США, а также осуществляющие атаки против соответствующих ведомств и политиков,

в международных СМИ часто обвиняют в связях с российским правительством. Однако доказать такую аффилированность довольно сложно и пока никто не предоставил достаточно убедительных свидетельств существования спонсируемой государством программы.

1.6.3. Манифесты хактивиста Phineas Fisher

В ноябре 2019 г. издание Vice Motherboard сообщило, что известный взломщик и хактивист Phineas Fisher прервал длительное молчание и вышел на связь со СМИ (https://xakep.ru/2019/11/19/phineas-fisher-is-back/).

Напомню, что человек или группа лиц, которые скрываются под этим псевдонимом, широко известны благодаря сразу нескольким громким «деяниям». В частности, в 2016 году именно Phineas Fisher слил Wikileaks документы правящей партии Турции и скомпрометировал профессиональных разработчиков и поставщиков шпионского ПО, компании FinFisher и Hacking Team. Затем Phineas Fisher выставил на всеобщее обозрение похищенные у компаний документы, исходные коды и даже эксплоиты.

После перечисленных инцидентов и нескольких других атак Phineas Fisher опубликовал ряд манифестов, в которых мотивировал других хакеров совершать политически мотивированные атаки. Затем, в 2017 году он сообщил, что временно уходит на покой, и с тех пор о хактивисте ничего не было слышно более двух лет, но затем он прервал свое молчание.

Phineas Fisher в ноябре 2019 г. опубликовал новый манифест, в котором предложил подогревать интерес к хактивизму, поощряя его финансово. Фактически хакер предложил учредить новый вид bug bounty – вознаграждать хакеров за политические атаки, совершающиеся во имя общественных интересов. Свою программу он назвал Hacktivist Bug Hunting Program и сообщил, что готов заплатить другим активистам до 100 000 долларов в криптовалюте (Bitcoin или Monero). Журналисты отмечают, что фактически эта программа напрямую стимулирует преступную деятельность.

«Я считаю, что хакерство – это мощный инструмент, и хактивизм использует только часть своего истинного потенциала. Небольшие инвестиции могут помочь ему развиваться, лучшие времена [хактивизма] еще впереди», – пишет Phineas Fisher.

В качестве примера он перечисляет и возможные цели для хактивистов: горнодобывающие и животноводческие компании в Южной Америке, израильский разработчик спайвари NSO Group и нефтяная компания Halliburton.

«Взлом с целью получения и слива документов, представляющих общественный интерес, является одним из лучших способов использования хакерских способностей на благо общества. Я не пытаюсь никого озолотить, я лишь пытаюсь выделить достаточно средств, чтобы хакеры могли достойно зарабатывать на жизнь, делая хорошую работу», – гласит манифест.

Кроме того, в этом заявлении Phineas Fisher сообщил, что еще в 2016 году он взломал оффшорный банк Cayman Bank and Trust Company, похитив деньги (и отдав их, куда и кому именно – не уточняется), документы и электронные письма сотрудников. Точную сумму хакер разглашать отказался, но уточнил, что речь

идет о «нескольких сотнях тысяч долларов». Приводя этот пример, Phineas Fisher призвал других хактивистов следовать тем же путем и присоединяться к борьбе с неравенством и капитализмом.

В своем манифесте хакер по традиции описывает, как проник в систему. Таким образом он стремится научить других, как проводить подобные атаки, и показать, как использовать определенные техники для ограбления банков. Так, он пишет, что использовал против банка тот же эксплоит, что некогда помог ему скомпрометировать Hacking Team: атаковал уязвимый VPN и брандмауэр.

«В цифровую эпоху ограбление банка является ненасильственным актом, наименее рискованным, а вознаграждение выше, чем где-либо еще. Ни об одном из финансовых хаков, которые я совершал и о которых мне было известно, никогда не сообщалось. Этот [взлом] будет первым, и не потому, что так захотел банк, а потому, что я сам решил предать это огласке, – заявляет Phineas Fisher. – Мировая финансовая элита – это угнетатели, а не жертвы [...]. Взлом этой элиты и возвращение крошечной доли похищенного ими богатства не делает их жертвами. Это киберпреступление. А также это активизм, мотивированный стремлением к социальным переменам. Я не получаю от этого никакой выгоды и прибыли».

Хотя у авторов на момент сдачи рукописи в издательство и нет достоверной информации о создании и реальном функционировании в даркнете такого «фонда», но можно быть уверенным, что и в этой криминальной англоязычной среде действует аналог русского слогана: «*пацан сказал – пацан сделал*».

1.6.4. Этика общечеловеческая и этика хакерская – «почувствуйте разницу»!

В завершении этого раздела попробуем сформулировать некие общие выводы относительно *этических аспектов* хакерских сообществ, прежде всего имея в виду «этичных» хакеров и хактивистов. Но для этого нам придется воспользоваться терминами уже не «техническими», а скорее из области философии и психологии.

Ведь хакер – это не специальность и не профессия, скорее – это образ жизни человека.

И здесь нам никак нельзя обойтись без упоминания таких «нетехнических» терминов, как «этика», «мораль», «совесть», «моральный долг» и т.п.

Посмотрим, как современные словари и энциклопедии определяли эти понятия.

Этика (греч. ἠθικόν, от др.-греч. ἦθος – этос, «нрав, обычай») – философская дисциплина, предметами исследования которой являются нравственность и мораль.

Первоначально смыслом слова «этос» было совместное жилище и правила, порожденные совместным проживанием, нормы, сплачивающие общество, способствующие преодолению индивидуализма и агрессивности. По мере развития общества к этому смыслу добавляется изучение *совести, добра и зла, сочувствия, дружбы, смысла жизни, самопожертвования и так далее. Выработанные этикой понятия – милосердие, справедливость, дружба, солидарность* и другие, направляют моральное развитие социальных институтов и отношений.

В науке в широком смысле под этикой понимают область знания, а под моралью или нравственностью – то, что она изучает.