ЕТИЧНОТО ХАКЕРСТВО

ХРИСТИНА АМБАРЕВА

Институт за изследване на обществата и знанието, БАН

ambareva@yahoo.com

ETHICAL HACKING

HRISTINA AMBAREVA

Institute for the Study of Societies and Knowledge, BAS

Abstract
The purpose of this article is to examine the concepts of "ethical hacker" and "hacker ethics". The concept of "hacker" is presented in historical perspective and its development since the 1960-s is traced shortly. The article also mentions the different types of hackers, the ethical principles that consolidate hacker subculture and comments on a case, related to ethical hacker occupation (the hacker attack against the National Income Agency in June 2019 in Bulgaria). In conclusion, the article confirms the necessity of more conservative usage of the word "hacker" and recommends the choice of ethically neutral way of reference to the occupation of the "ethical hacker" like "penetration tester."
Keywords: types of hackers, ethical hacker, hacker ethics, counterculture

Теза

Целта в настоящата статия е да разгледам понятията „етичен хакер" и „хакерска етика" и да обясня защо, въпреки лексикалната прилика, етичният хакер не се явява последовател на хакерската етика. За да обясня тезата си, накратко ще представя видовете „хакери" в историческа перспектива, техните постижения и етическите принципи, около които се обединява хакерската субкултура. В техния контекст ще коментирам и противоречията на названието „етичен хакер".

Хакерската етика и видовете хакери

Известно е, че думата „хакер" се използва в публичното пространство основно в значение „човек, който действа извън закона", има експертно знание за компютрите и компютърните мрежи, може да прониква в добре охранявани системи и да влияе на работата им. Обратно обаче на популярното мнение, че хакерите се занимават с

противозаконни дейности, историята им показва, че те имат напълно легален и похвален принос за развитие на информационната епоха. Нещо повече, хакерската субкултура е проводник на основни идеи на контракултурното движение на 1960-те години в САЩ, което по това време обединява идеалите на много млади хора за по-добър свят.

Историята на хакерската субкултура дължи много на културното наследство на американските академични центрове за развитие на компютърните изследвания и изкуствения интелект. Такива са създадени в края на 1950-те години на 20 век с финансиране от Министерството на отбраната на САЩ в големи университети като МИТ, Станфорд и др. Министерството отпуска пари за технологични проекти и изследвания, около които се събират и от които се вдъхновяват талантливи млади хора – сред тях първите хакери.

Историята на хакерската субкултура, също, дължи много на факта, че Станфорд се намира в район, който е център на контракултурното движение през 1960-те години. През този размирен период в Сан Франциско, днешната Силициева долина, се развива хипи-движението и бунтът на новите леви. Съчетанието на технологично ориентирани университетски центрове с бохемството на контракултурата е ключов фактор, действал при формиране културата на компютърните хакери. Носители на хакерската субкултура стават студенти, някои от които изобщо не завършват. Консолидирането ѝ се дължи на поредица от постижения на хакерството, които водят развитието на дигиталната епоха към това, което познаваме днес (виж: Brand, 1995 и Markoff 2005).

Първо важно постижение е създаването на персонален компютър от Стив Возниак и неговото успешно маркетизиране от Стив Джобс. Голямата мания на хобистите – всеко момче да има компютърно устройство, с което да си играе – се превръща в компютърна революция за всички. Съществуването на персоналния компютър става етап от развитието на съвременната дигитална епоха. Големите мейнфрейм компютри са били прекалено скъпи и трудни за подръжка, да не говорим, че технологията за споделяне на времето (един компютър за няколко потребителя едновременно) не е била достатъчно удобно решение за младежкия ентусиазъм. Персоналният компютър отваря неограничени възможности за експерименти и самообучение в новата технология. Хакерите с изразени инженерни наклонности като

Стив Возниак, които експериментират със създаването на технически устройства могат да се разглеждат като представители на ***хардуеърните хакери*** (Jordan&Taylor, 2004).

По време на създаването му, никой освен хобистите с технически познания и интереси, не е могъл да ползва компютъра на Стив Возниак и Стив Джобс. **Второ постижение**, което същевременно помага за консолидиране на хакерската общност, **е разработването на софтуеър**, който да работи на тези компютри и да ги направи по-достъпни и полезни. Хакерите имат сериозен принос за развитие на програмните езици оттогава до днес. Първоначално става дума за езици като LISP (създаден през 1958 г.) и BASIC (1964). Във времето ентусиастите, които се увличат от писането на код, оформят групата на ***софтуеърните хакери*** (Jordan&Taylor, 2004), създали различни полезни приложения, като се започне от имейла и се мине през протокола за обмен на файлове TCP/IP, хиперлинка (основата на Световната мрежа), Visiculk (предтечата на Excel) и т.н.

Трето постижение на хакерството, което помага за консолидиране на хакерската общност е установяването на общ код за поведение – т.нар. хакерска етика.

Тя е спонтанен резултат от дейността, навиците и разбиранията на хакерите, който е обобщен и описан от журналиста С. Леви (Levy, 1984). Хакерската етика служи и като отправна точка, която определя идеята за хакера. Нейните първоначални принципи са следните:

- *Достъпът до компютри – и всичко, което може да те научи на нещо относно начина, по който работи света – трябва да бъде неограничен и пълен. Винаги се придържай към правилото „учене чрез правене”.*
- *Цялата информация трябва да бъде свободна.*
- *Недоверие към авторитета – промотиране на децентрализацията.*
- *Компютрите могат да направят живота по-добър.*
- *Хакерите трябва да бъдат оценявани по уменията им, а не по съмнителни критерии като степени, възраст, раса или позиция.*
- *Можеш да създаваш изкуство и красота на компютъра.*

Според Леви, тези, които се придържат към всички основни принципи на хакерската етика, се възприемат като ***бели хакери***. Тези, които не спазват целостта на кода за поведение, са ***черните хакери***. Същото се отнася за названията „бели шапки“ и

„черни шапки“ (Himmanen, 2001). „Белите” създават решения за проблемите на хакерската общност, „черните” рушат постигнатото, като създават зловредни програми, които могат да развалят труда на други хора. Оттук названието „чупещи” или ”**crackers**” за тях. През призмата на хакерската етика се оформят полюсите на „добрите” и „лошите”, като названието „**хакер**”, разбира се, остава само за първите.

Произходът на хакерството от контракултурата, от една страна, и университетските кампуси, от друга, влияе на формирането на изброените етически принципи. Някои от тях остават непроменени във времето и се вливат в мейнстрийм културата, като своеобразно наследство от културната революция, трансформирано в дигитална форма (виж: Амбарева, Х. 2019).

Обединяващата сила на идеите се проявява изключително убедително през 90-те години, когато в рамките на хакерската субкултура се утвърждава ***Общността на отворения код***. Това става при създаване на операционната система Линукс с доброволния труд на хиляди хакери. **Написването на Линукс през 1990-те години е четвърто постижение на хакерите**, което дава рещаваща подкрепа за Движението за отворен код и свободен софтуеър от 1980-те. Споделянето на кода позволява на хакерите да ползват готови решения като налично знание за своите собствени решения и иновации и допълнително стимулира разрастването на хакерската общност. Свободният софтуер става концепция за безплатно разпространение на софтуера, така че всеки да има достъп до него и може да го ползва – което отваря пътя към персоналния компютър за масовия потребител. Това също стимулира разрастването на днешните хакерски общности.

Движението за отворен код и свободен софтуер има важни икономически и социални измерения, които все още са в процес на развитие. Хакерската субкултура и отвореният код пренаписват икономиката на съвременната епоха и значително променят практиките за защита на интелектуалната собственост с лицензи като ГНУ, Криейтив Комънс и др. Създават се колаборативни проекти, около които се изграждат силни общности и се утвърждават множество лицензи на отворения код. Въпреки предизвикателствата на пазарната икономика, практиките на отворения код все още се ползват с кредит на доверие, който крепи нови колаборативни проекти.

Не на последно място, обединяваща идея на хакерството е тази **за създаване на**

нов по-хуманен свят (напр. виж Декларация за независимостта на киберпространството). Първите хакери са били анархисти, левичари, либертарианци – деца на контракултурата, изправени срещу статуквото като стил на живот (неформалност и бохемство) или като готовност за участие в про-демократични политически събития. През 1990-те години отчетливо се оформят хакерски групи от т. нар. ***хактивисти*** (Jordan &Taylor, 2004). Те започват да се включват активно в политически действия като организират виртуални аналози на физически протести и стачки предимно чрез DDoS атаки към правителствени и корпоративни сайтове. Те са много активни в края на 90-те и първото десетиление на 21 век и взимат участие в събития като войната в Косово, протести на движението „Окупирай Уолстрийт", протестите в Египет през 2011 г. и др. Хактивизмът днес се разраства благодарение на достъпни за всички дигитални инструменти (социални мрежи и др.), и отстояващото гражданство е основна концепция за политическо действие в дигиталното общество (Dalton &Welzel, 2013).

Защо на фона на всички приноси, които има хакерската субкултура към създаване на дигиталното общество днес, хакерството все още се мисли негативно?

Вероятно част от отговора е, че през годините, с развитие на компютърните технологии и интернет, възможностите за компютърни престъпления нарастват. Онлайн търговията, банковата информация, онлайн комуникацията и електронните правителства стават източник на доходи (пряко или косвено), които прехвърлят престъпността от физическия във виртуалния свят. Престъпниците в дигиталната епоха също имат хакерски умения. Медиите са прословути с любовта си към лошите новини. Логично е с развитието на интернет, в медийното пространство думата „хакер" да се обвърже изключително с нелегалното проникване в компютърни мрежи и системи, кражби на номера на кредитни карти, кражби на данни, източване на сметки и др. Това е път, по който се утвърждава негативно понятие за хакера. Медиите дълги години не правят разлика между хакер и престъпник и популяризират употреба на думата, с която много хакери не са съгласни.

Въпреки, че информацията е достъпна и свободна, историята на хакерската субкултура не е достатъчно позната и не представлява предмет на особен академичен интерес. Тя също не се възприема като свързана с мейнстрийм културата, което е

парадоксално, предвид приноса ѝ в нейното оформяне. Днес идеята за хакерството все още страда от суеверия за свръхспособности и митове за екшънгерои.

Етичното хакерство

След цялото разнообразие от хакери, за които стана дума и към които може да се добавят още цветове – *сиви* [1]*,червени* [2]*, сини*[3]*, зелени*[4]- идва ред и на понятието за етичен хакер.

Етичният хакер е специалист по киберсигурност, чиято задача е да идентифицира и поправи слабости в киберзащитата на компютри и компютърни мрежи.

Използването на това понятие има няколко позитивни и няколко проблемни страни.

Позитивни страни

Въвеждането на израза „етично хакерство" противодейства на негативния образ на хакера. То цели да представи хакерството като конструктивна дейност, която се е помирила със закона и служи на компаниите и правителствата да подобрят сигурността на системите си. Етичното хакерство е относително нова концепция, употребявана равнозначно с тази за „белия хакер" или в смисъл на наследник на белите хакери.

Етичното хакерство се учи. Това е много положителна стъпка към разбирането за хакера, защото отхвърля сянката на „гениалността" или „изключителността" от него, както и всякакви митологеми. Етичното хакерство като концепция е демократична и показва, че всеки може да учи и да стане изключителен професионалист.

Етичното хакерство вкарва хакерството в мейнстрийм културата, където му е мястото. То ясно заявява, че хакерът не е престъпник, а човек, необходим на времето. Поради недостиг на ИТ специалисти днес, има много обучителни курсове за етичен хакер, включително и такива, които официално се сертифицират с името на Европейския съвет.

Проблеми на названието „етичен хакер"

Предвид факта, че в учебниците или курсовете за „етично хакерство" не става дума за етика, думата „етичен" е доста подвеждащ момент. Нещо повече, практически употребата му показва проблеми не само по отношение на закона, но и на морала.

През последните две години (2018 – 2019) обект на хакерски атаки в България са частни компании и държавни институции. Сред тях – сайтът на Търговския регистър, Министерството на образованието и Националната агенция за приходите. Хакерска атака, която има последствия за стотици хиляди хора, е атаката срещу НАП през юни 2019 г. Обвиняем по следствието стана частна компания за киберсигурност, в която работят именно „етични хакери". В хода на разследването за НАП свидетели твърдят, че действието на обвиняемата компания се вписва в нейния бизнес модел, а няколко частни фирми, които са били обект на неоторизирано влизане в системите им, потвърждават, че то е било последвано от предложение за подобряване на защитата. Известно е също, че компанията е продавала за големи суми информация от хакнатите бази данни. Тоест в действията си етичните хакери от частната охранителна компания не показват етични съображения, а финансови мотиви и действат като „кракери". Това не накърнява техните професионални умения, но създава проблем с определението „етичен" и „хакер". Кибератаката срещу НАП е добър повод да се разсъждава за думите и нещата.

Етичният хакер владее инструментите и похватите на злонамерения „хакер" и тествайки защитата на набелязаната цел, той всъщност извършва хакерска атака. Етичните хакери са етични само при определено условие, а именно, когато хакерската атака следва, а не предшества, юридическото съгласие на собствениците на компютъра, мрежата или компютърната системата да бъдат подложени на „хакерска атака". Така названието „етичен хакер" няма за цел да описва моралните качества на киберспециалиста. То описва юридическите правила на професия, в която няма ясни морални ангажименти. Ако търсим етическото като характеристика на самата професия „етичен хакер", ще се сблъскаме с противоречия.

За разлика от първоначалните хакери, които са свободни „хобисти", етичните хакери служат на целите на институции или частни компании. Свободата е характеристика на дейността на хакера, която в съвременните опити да се определи един киберспециалист като „етичен хакер" се пренебрегва. Ако етичният хакер служи

на своето правителство, това не означава, че действията му са морални, а може дори да не са законни. Малко са тези като Сноудън, които от етични съображения ще захвърлят блестяща кариера, за да изобличат незаконни действия на своята институция. От друга страна, всяко етическо действие се тълкува с оглед на предварително изградена рамка за цел и смисъл на живота, без да поставя под въпрос рамката. Радикалните ислямисти също имат морални основания да работят като етични хакери за своя Ислямска държава.

Не на последно място, „етичен" е твърде противоречиво определение дори за оригиналния хакер. Исторически той е наследник на политическия и ценностен бунт на новите леви и хипитата, тоест на опита за релативизация и либерализиране на ценностите. Либертарианската или анархистична ориентация на много от първите хакери съвсем не се съгласува със служба за традиционния морал, държавата и закона.

Заключение

През първите десетилетия от развитието на хакерската субкултура (1960-1990) хакерите са действали като откриватели, изобретатели, социални иноватори, бунтари, а някои от тях и мечтатели за по-добър свят. Случаят с НАП, както и много други, показват твърде голямата лекота, с която днес „хакер" се използва за всеки финансово-мотивиран извършител на киберпрестъпление.

С оглед на приносите на конструктивното хакерство към дигиталната епоха, е нужен много консерватизъм в употребата на думата „хакер". Безспорно, балансът между хакерството и законността винаги е бил крехък, но хакерската етика има набор от принципи и практики, създаващи определен ценностен контекст за изграждане на хакера, включващ разбиране за историята на хакерите, техните институции и практики като общност.

Може ли етичният хакер да се разглежда поне като наследник на белия хакер?

„Белият хакер" е етическо определение в духа на хакерската етика. Идеята за етичния хакер е опит да се копира това определение, като проблемът е, че то се прилага в исторически нова среда. Хакерската субкултура се е превърнала в мейнстрийм култура. Гаражът – в транснационална компания. Хобито на хакерите вече е най-популярната професия в дигитализираните общества. Белият хакер е свободен, етичният хакер е наемник. Не е невъзможно етичният хакер да бъде наследник на белия

хакер, просто не всеки, който работи като „етичен хакер" по подразбиране е „бял" и „хакер".

С оглед на противоречията около понятието „етичен хакер", е добре да се говори етически неутрално за личността и професията и да се оценява само качеството на действието. Тоест изразът „ethical hacking", етично хакване, работи далеч по-добре от „ethical hacker", етически хакер.

Понятието „етично хакерство" набира популярност в момента, но е подвеждащо название с много потенциални противоречия – и етически, и юридически. Извън митологемата за съществуването на „етичен хакер", за професионалиста е най-правилно да се говори отвъд доброто и злото, като се нарича „penetration tester" на английски, или „специалист по киберсигурност" на български.

БЕЛЕЖКИ

[1] Сиви хакери са тези, които не причиняват вреда, но се забавляват да хакват нелегално различни системи. Това е статистически най-популярната и общо-взето безвредна форма хакерски атаки.

[2] Червените хакери са описвани като любители на чувствителна и секретна информация.

[3] Сините хакери са асоциирани с Майкрософт.

[4] Зелените хакери са „новобранци".

ЛИТЕРАТУРА

Амбарева, Х. (2019). *Културата на интернет и как тя променя света*. С., Авангард Прим.

Brand, S. (1995). We owe it all to the hippies. *TIME Magazine Domestic.* Special Issue, Spring 1995 Volume 145, No. 12.

Dalton, R., C. Welzel. (2013). *The Civic Culture Transformed: From Allegiant to Assertive Citizenship.* Cambridge University Press.

Himmanen, P. & al.. (2001). *The Hacker Ethics and the Spirit of the Information Age*. New York and Canada: Random House.

Jordan, T., P. Taylor. (2004). *Hacktivism and cyberwars : rebels with a cause?*. London ;

New York : Routledge.

Levy, S. (1984). *Hackers, Heroes of the Computer Revolution*. Published by Dell Publishing a division of Bantam Doubleday Dell Publishing Group, Inc. 1540 Broadway New York, New York 10036.

Markoff, J. (2005). *What the Dormouse said: How the sixties counterculture shaped the personal computer industry.* Penguin Books.

Петров, Р. (2018). *Основи на етичното хакерство*, част I. София.

Документи, изнесени в медиите, от прокуратурата във връзка с хакерската атака срещу НАП през юни 2019.