Мораль (лат. *moralitas*, термин введен Цицероном от лат. *mores* «общепринятые традиции») – принятые в обществе представления о хорошем и плохом, правильном и неправильном, добре и зле, а также совокупность норм поведения, вытекающих из этих представлений.

Иногда термин употребляется по отношению не ко всему обществу, а к его части, например: христианская мораль, буржуазная мораль и так далее. В тех языках, где, как, например, в русском, помимо слова *мораль* употребляется слово *нравственность* (в немецком – *Moralität* и *Sittlichkeit*), эти два слова чаще выступают в роли синонимов или каким-то образом концептуализируются для обозначения отдельных сторон (уровней) морали, причем концептуализации такого рода носят по преимуществу авторский характер. Мораль, принятая и преобладающая в том или ином обществе, называется *общественной моралью*. Мораль изучает отдельная философская дисциплина – этика.

Совесть – психический (когнитивный) процесс, вызывающий эмоции и рациональные ассоциации, основанные на моральной философии или *системе ценностей* личности. Зачастую совесть является причиной появления чувства вины или «угрызений совести», раскаяния, когда человек совершает поступок, противоречащий его моральным ценностям. Моральные ценности индивида и их несоответствие семейным, социальным, культурным и историческим представлениям о морали служат предметом изучения в психологии. Степень, в которой совесть определяет суждение о моральной стороне действия перед его совершением, и вопрос о том, основаны ли (или должны быть основаны) такие моральные суждения на разуме, породили споры в философии.

В вышеупомянутой книге Стивена Леви «Хакеры: Герои компьютерной революции» была *отдельная глава про этику* хакеров. Основные постулаты, не относящиеся к технике, гласили: ***практический императив, свобода информации, децентрализация, отрицание полномочий, и самое главное – людей должно судить по их делам, а не по надуманным критериям, таким как звания, возраст, цвет кожи и положение в обществе***.

Говоря «научным языком», этика – это система моральных принципов, позволяющая человеку отличить «правильное» от «неправильного».

Сравните это определение «хакерской этики» с вышеприведенными определениями и, как говорится в популярной российской телевизионной рекламе, – «почувствуйте разницу!». Ведь что считать «этичному» хакеру *правильным*, а что *неправильным* – каждый из них решает для себя сам. Это же относится и к выбору «моральных принципов» хакера.

В подобных «этических кодексах» хакеров вы не найдете таких понятий, как «совесть», «добро», «нравственность», «смысл жизни», «самопожертвование» и т.п.

Более того, здесь необходимо привести и такой малоизвестный широкой публике факт, как достаточно высокий процент наличия среди «белых шляп» *людей с психическими отклонениями* от «нормы». Известно, по крайней мере, о двух хакерах, входящих в элитный клуб «топ-9» гениальных хакеров, у которых официально был подтвержден медицинский диагноз – болезнь (синдром) Аспергера. Здесь не место обсуждать, что такое «норма» и что считать «отклонением от нормы», тем более что среди больных с этим и подобными диагнозами известно множество талантливых художников, писателей, ученых.

Мы просто констатируем тот факт, что медики считают тот же «синдром Аспергера» болезнью (инвалидностью), одной из форм аутизма легкой – пятой степени.

Ярчайший пример – уже упомянутый Гэри Маккиннон. Гэри Маккиннон причастен к «величайшему компьютерному взлому в истории». Он сумел взломать компьютеры военного ведомства США, тем самым нанеся серьезнейший урон всей организации. При этом он руководствовался собственным «этическим кодексом» и собственными «моральными принципами». По словам Гэри, он всего лишь хотел получить неизведанные данные о НЛО и скрытую информацию, которая может быть полезна для человечества. Для этого шотландский хакер взломал всю систему NASA, выведя из строя около 2 тыс. компьютеров. В течение 24 часов на официальном сайте космического управления висел баннер – «Ваша безопасность – абсолютная чушь», что вывело из себя военное ведомство США. Если верить Маккиннону, факты контактов с НЛО на самом деле скрывались от общественности. Он говорит, что на сервере хранятся файлы проекта «Раскрытие», где описываются более 4 сотен случаев, доказывающих существование пришельцев или их технологий.

На момент выхода книги дело Маккиннона до сих пор находилось в суде, так как США требует его экстрадицию. Английское правительство дало согласие на вывоз хакера, но столкнулось с умелой защитой адвокатов Гэри и волной общественных протестов, требующих судить хакера исключительно в Великобритании. По слухам, американская судебная система уже приготовила приговор, в виде лишения свободы на 70 лет в лагере для террористов и военных преступников – Гуантанамо. Как всем известно, эта тюрьма одна из самых страшных тюрем в мире. Адвокаты Маккиннона активно используют информацию о «болезни Аспергера», оспаривая в суде решение об экстрадиции защищаемого клиента.

Аналогичный медицинский диагноз был поставлен и № 2 вышеупомянутого «топ-9» гениальных хакеров – Адриану Ламо, который известен тем, что в 2003 году взломал NY Times, Microsoft, Yahoo и др.

По своей «хакерской этике» Ламо взламывал эти сайты исключительно ради самоудовлетворения и приобретения популярности, всегда сообщая «жертвам» об обнаруженных им уязвимостях. На суде в 2017 г. адвокаты также представили информацию, что он проходил длительный курс лечения от синдрома Аспергера.

Чтобы завершить тему «терминологической эквилибристики», следует напомнить тот факт, что на момент выхода этой книги существует множество различных классификаций современных хакеров, которые основываются на различных «классификационных признаках».

Так, на сайте https://www.securitylab.ru/blog/company/PandaSecurityRus/342530.php была представлена, на ваш взгляд, наиболее полная такая классификация хакерских сообществ, являющаяся переводом оригинала статьи «Are All Hackers Bad? Types of Hackers», подготовленной Panda Security.

1. Хорошие ребята

Существует тип людей, которые имеют регулярную (официальную) оплачиваемую работу, но иногда используют свои хакерские навыки для поиска дыр безопасности в различных бизнес-системах. В большинстве случаев они это делают не ради

финансовой выгоды. Они делают это, потому что в состоянии сделать это и потому что они беспокоятся о людях, которые могут использовать эти уязвимые сервисы. Несколько хакерских организаций претендуют на то, чтобы их называли такими «хорошими ребятами», например, German Chaos Computer Club.

2. Консультанты

Это тип людей, которые осуществляют поиск эксплойтов, после чего предлагают свои услуги компаниям, которые в них нуждаются. Технически они не делают чего-либо незаконного, потому что они не шантажируют и не эксплуатируют недостатки системы. Они всего лишь уведомляют компании, что их продукты могут быть более безопасными, если они их наймут на работу. Они не являются хорошими или плохими, они просто бизнесмены. Некоторые великие предприниматели современности начинали именно как хакеры.

3. Плохие ребята (злобные хакеры)

Не все готовы подчиняться законам, у них не хватает терпения или способности договариваться с предприятиями, а потому они всегда готовы воспользоваться огрехами в системе. Это такой тип людей, чья главная цель в жизни состоит в том, чтобы украсть вашу конфиденциальную информацию и испортить вам жизнь. Ими движут деньги и сомнительная мораль. Они живут ради денег, а потому они могут без сожаления шантажировать и обманывать всех, кто стоит на их пути. Очень часто они думают, что они выше других... пока их не поймают.

4. Хактивисты

Это тип хакеров, которые совершают атаки в основном ради того, чтобы попасть в новости. Они нарушают закон, чтобы собирать информацию, которая может помочь им поддержать определенное дело. Они считают себя Робинами Гудами современного общества. Зачастую они не знакомы со всей картиной происходящего, а потому их действия в конечном итоге могут вызвать хаос, т.к. они пытаются раскрыть «правду», которая может быть даже вредна для обычных людей – тех, кого они искренне пытаются защитить. Anonymous – это прекрасный пример такой группы.

5. Поддерживаемые государством

Как мы отмечали выше – современная кибервойна не регулируется какими-то законами и правилами. Каждая развитая страна в мире сегодня имеет собственную армию хакеров, которая работает на правительство своей страны, а иногда эти же люди используются для вмешательства в жизнь других стран. Конечно, публично правительства отрицают такое вмешательство, но существует множество косвенных доказательств тому, что такие кибермии существуют не только для защиты граждан собственной страны, но также и для манипуляции других стран и сбора разведданных для поддерживающего и даже финансирующего их правительства.

6. Самозванцы

Это тип хакеров со средним уровнем ИТ-знаний, которые «ходят по чатам» и угрожают обычным людям без видимых на то причин. Самозванцы иногда способны достичь чего-то значительного, например, узнать пароль к WiFi у своих соседей, но они не могут удержаться от того, чтобы не рассказать о своих достижениях

друзьям. Самозванцы требуют общественного внимания и в большинстве случаев в принципе безобидны для общества.

7. Хакеры-бездари

Это те хакеры, которые не имеют понятия о том, что они делают, а потому оставляют свои «следы» везде, куда они «ходят». В большинстве случаев вы легко можете получить следы таких хакеров, осуществив соответствующие запросы в поисковиках. Иногда им удается выжить и двигаться вверх по иерархической лестнице, но обычно это те ребята, кого мы часто видим в новостях как пойманных за киберпреступления.

Ученые-филологи знают, что *термины* (от латинского terminus – граница, предел) это специальные слова или словосочетания, принятые в определенной среде (профессиональной сфере) и употребляемые в особых условиях. Говоря «научным языком» – термин представляет собой словесное обозначение понятия, входящего в систему понятий определенной области профессиональных знаний.

В данном анализируемом случае ***«белые шляпы», называя себя «этичными хакерами», просто используют термин «этика», как говорят ученые, «в отрыве от контекста», т.е. неправомерно***.

А если уж говорить о «моральных принципах» – мы знаем достаточно много случаев, когда такие «этичные» хакеры легко «меняли шляпы» – вместо «белых» надевали «черные шляпы» и наоборот, соответственно, и при этом легко изменяли и свой «этический кодекс», и эти «моральные принципы».

Литература к главе 1

1. Васильев М.В. Кибертерроризм как элемент гибридной войны. URL: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny
2. Туронок С.Г. Современный терроризм: сущность, причины, модели и механизмы противодействия. – М., 2008.
3. Григорьев Н.Н. Современный кибернетический терроризм и его социальные последствия // Вестник университета. – 2016. – № 5. – С. 228–232.
4. Почему не взорвалась Игналинская АЭС // Финансовая Россия. – 2001. – № 34.
5. Бухарин О. Проблемы ядерного терроризма. URL: http://terroristica.info/node/133 (дата обращения: 24.02.2018).
6. Кибератаки на атомные станции // Цифровая подстанция. URL: http://digitalsubstation.com/blog/2016/01/19/kiberataki-na-atomnye-stantsii/ (дата обращения: 24.02.2018).
7. Угроза взрыва на Игналинской АЭС // Коммерсантъ. – 1994. – 15 ноября. – № 216.
8. Хакнуть АЭС намного проще, чем вы думаете. URL: https://geektimes.ru/company/icover/blog/262972/ (дата обращения: 24.02.2018).
9. Как липецкие школьники «отравились ультразвуком» // РИА Новости. URL: https://ria.ru/society/20171201/1509966174.html (дата обращения: 24.02.2018).
10. Жуйков А.А. Трансформация представлений об информационной безопасности в условиях виртуализации социума в начале XXI века // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 11. – С. 102–105.
11. ФСБ опасается возможных кибератак террористов на электронные сети госструктур // Российская газета. URL: https://rg.ru/2009/04/15/fsb-sedov-anons.html (дата обращения: 24.02.2018).

12. Ильинский А. Кибертеррор стал частью гибридной войны. Анонимные хакеры показали свою силу. URL: http://www.km.ru/v-rossii/2017/05/20/khakery-i-problema-bezopasnosti-kompyuternykh-setei/803472-kiberterror-stal-chas (дата обращения: 24.02.2018).
13. Корецкий А. Хакеры получили доступ к английским военным спутникам. URL: http://bookre.org/reader?file=351183 (дата обращения: 24.02.2018).
14. Васенин В.А. Информационная безопасность и компьютерный терроризм // Центр исследования компьютерной преступности. URL: http:// www.crime-research.ru/articles/vasenin (дата обращения: 23.02.2018).
15. Хакерская группа объявила кибервойну России. URL: http://lenta.ru/news/2012/11/03/blackstar/ (дата обращения: 25.02.2018).
16. Фарвазова Ю.Р. Совершенствование информационной безопасности как части антитеррористической стратегии России // Вестник Казанского юридического института МВД России. – 2014. – № 1. – С. 116–120.
17. ИГИЛ обзавелось 45 тысячами аккаунтов в Twitter для вербовки и пропаганды // Региональная антитеррористическая структура Шанхайской организации сотрудничества. URL: http://ecrats.org/ru/situation/status/4880 (дата обращения: 22.10.2017).
18. WannaCry 2.0: наглядное подтверждение того, что вам обязательно нужно правильное решение для надежного бэкапа. URL: https://habrahabr.ru/company/acronis/blog/328796/ (дата обращения: 24.02.2018).
19. Васильев М.В. Современные медиатехнологии на службе международного терроризма // Актуальные проблемы исследования коммуникационных аспектов PR-деятельности и журналистики. Сборник материалов международного научного семинара (Псков, 19 февраля 2016 г.). – Псков, 2016. – С. 18–41.
20. Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта // Общественные науки. Право. – 2015. – № 2. – С. 29–34.
21. Томас Т.Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма. Материалы международной конференции. – М., 2002.
22. Тиханычев О.В. Ограничение распространения кибероружия как фактор обеспечения безопасности в информационном мире. URL: https://e-notabene.ru/nb/article_25377.html
23. Шарп Д. От диктатуры к демократии. Концептуальные основы освобождения. – Институт им. Альберта Энштейна, 2010. – 72 с.
24. Sharp Gene. The Politics of Nonviolent Action. – Boston, MA: Porter Sargent. 1973. – 72 p.
25. Выпасняк В.И., Тиханычев О.В., Гахов В.Р. Кибер-угрозы автоматизированным системам управления // Вестник Академии военных наук. – 2013. – № 1 (42). – С. 103–109.
26. Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В. Информационное управление в условиях глобализации и геополитического противоборства // Национальная безопасность / nota bene. – 2015. – № 2. – С. 202–243. DOI: 10.7256/2073-8560.2015.2.14622
27. Чварков С.В., Лихоносов А.Г. Новый многовекторный характер угроз безопасности России, возросший удельный вес «мягкой силы» и невоенных способов противоборства на международной арене // Вестник академии военных наук. – 2017. – № 2.

28. Анисимов Е.Г., Анисимов В.Г., Сауренко Т.Н., Чварков С.В. Военная экономика и оборонная промышленность. Экономическая политика в системе национальной безопасности Российской Федерации // Вестник академии военных наук. – 2017. – № 1. – С. 137–144
29. Безкоровайный М.М., Лосев С.А., Татузов А.Л. Кибербезопасность в современном мире: термины и содержание // Информатизация и связь. – 2011. – № 6. – С. 27–33.
30. Лебедева Е.В. Информационная безопасность государств СНГ: этапы реализации // Национальная безопасность / nota bene. – 2016. – № 4. – С. 500–508. DOI: 10.7256/2073-8560.2016.4.17585
31. Владимирова Т.В. Об обеспечении информационной безопасности в условиях киберпространства // Вопросы безопасности. – 2014. – № 3. – С. 132–157. DOI: 10.7256/2306-0417.2014.3.12525. URL: http://e-notabene.ru/nb/article_12525.html
32. Кибернаемники и легальное вредоносное ПО. KasperskyClub Daily URL: https://www.kaspersky.ru/blog/legal-malware-counteraction/5539/
33. United States European Command. Theater Strategy. Gen Philip M. Breedlove, USAF Commander. URL: http://www.eucom.mil/
34. Roger N. McDermott. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic. International Centre for Defence and Security. – Tallinn, 2017. – 122 p.
35. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
36. Национальная стратегия США по достижению безопасности в киберпространстве («National Strategy to Secure Cyberspace»). URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
37. Элементы для создания глобальной культуры кибербезопасности. Приняты резолюцией 57/239 Генеральной Ассамблеи ООН от 20 декабря 2002 года. URL: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml
38. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Шестьдесят восьмая сессия Генассамблеи ООН. Пункт 94 предварительной повестки дня. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement
39. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666
40. Нестеров А.В. Интернет-поле VS киберпространства // Вопросы безопасности. – 2015. – № 4. – С. 13–27. DOI: 10.7256/2409-7543.2015.4.16743. URL: http://e-notabene.ru/nb/article_16743.html
41. Постановление Правительства Российской Федерации от 24 июля 1995 г. № 737 «О присоединении Российской Федерации к международному Режиму контроля за ракетной технологией».
42. Указ Президента Российской Федерации о контроле за экспортом из Российской Федерации оборудования, материалов и технологий, применяющихся при создании ракетного оружия от 16 августа 1996 года №1194.
43. https://ru.wikipedia.org/wiki/%D0%AD%D1%82%D0%B8%D0%BA%D0%B0
44. https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B2%D0%B5%D1%81%D1%82%D1%8C

45. https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%80%D0%B0%D0%BB%D1%8C
46. https://zen.yandex.ru/media/id/5d4196d7e6cb9b00ae2b72ba/top-9-genialnyh-hakerov-kotorym-udalos-nevozmojnoe-5d8808d27cccba00ace0dacc

Дополнительная литература

1. Васильев М.В. Кибертерроризм как элемент гибридной войны. URL: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny
2. Туронок С.Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. – 2011. – № 4. – С. 131–140.
3. Голубев В.А. «Кибертерроризм» – миф или реальность? // Центр исследования компьютерной преступности. URL: http://www.crime-research.org/library/terror3.htm (дата обращения: 23.02.2018).
4. Владимир Путин обсудил с членами Совета безопасности России меры борьбы с киберугрозами // Новости. Первый канал. URL: https://www.1tv.ru/news/2017-10-26/335153-vladimir_putin_obsudil_s_chlenami_soveta_bezopasnosti_rossii_mery_borby_s_kiberugrozami (дата обращения: 23.02.2018).
5. Богачев В.Я., Редин В.В. Информационная безопасность как составная часть национальной безопасности Российской Федерации // Стратегия гражданской защиты: проблемы и исследования. – 2012. – Т. 2. – С. 785–797.
6. Вирус поразил компьютерную сеть АЭС в США // Военное обозрение URL: https://topwar.ru/119114-virus-porazil-kompyuternuyu-set-aes-v-ssha.html (дата обращения: 24.02.2018); Кибератаки на ядерные объекты. История вопроса // Коммерсантъ. URL: https://www.kommersant.ru/doc/3196397 (дата обращения: 24.02.2018).
7. Крысько В.Г. Секреты психологической войны (Цели задачи, методы, формы, опыт). – Минск, 1999.
8. Америка вступает на путь государственного кибертерроризма // Вести.RU. URL: http://www.vesti.ru/doc.html?id=2818428 (дата обращения: 24.02.2018).
9. «Лаборатория Касперского» рассказала о «Красном октябре» URL: http://www.kaspersky.ru/news?id=207733920 (дата обращения: 25.02.2018).
10. Акопов Г. Политический «хактивизм» в эпоху информатизации социума. URL: http://www.relga.ru/Environ/WebObjects/tgu-www.woa/wa/Main?textid=3764&level1=main&level2=articles (дата обращения: 25.02.2018).
11. ФСБ поручено создать антихакерскую систему // Вести.RU. URL: http://www.vesti.ru/doc.html?id=1010793 (дата обращения: 25.02.2018); В российской армии официально созданы кибервойска // Вести.RU. URL: http://www.vesti.ru/doc.html?id=2858596 (дата обращения: 25.02.2018).
12. Тиханычев О.В., Тиханычева Е.О. Некоторые аспекты моделирования этносоциальных процессов. – М.: Эдитус, 2016. – 70 с.
13. Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Samarin V.I., Simonyan R.A., Kardashyan M.A. Enhancing Operational Efficiency of the Fuzzy Image of the Attacker's Method of Iterations // Modeling of Artificial Intelligence. – 2016. – № 4 (12). – С. 187–193.
14. Акопов Г.Л. Хактивизм – вызов национальной безопасности в информационном обществе // Национальная безопасность / nota bene. – 2015. – № 4. – С. 557–562. DOI: 10.7256/2073-8560.2015.4.15834

15. Каберник В.В. Проблемы классификации кибероружия // Вестник МГИМО-университета. – 2013. – № 2 (29). – С. 72–78.
16. How to avoid hacking to Critical Infrastructure. Сайт pandasecurity.com. URL: https://www.pandasecurity.com/mediacenter/pandalabs/whitepaper-critical-infrastructure/
17. Тиханычев О.В., Гахов В.Р. «Кибервойны» как реальная угроза системам государственного управления (по взглядам иностранных специалистов) // Сборник трудов второй МНТК «Компьютерные науки и технологии» (КНиТ-2011). – Белгород: Белгородский ГНИУ, 2011.
18. Соболев В.Е. Боевые кибернетические системы с высокочастотной перцепцией информации // Вопросы безопасности. – 2016. – № 6. – С. 1–6. DOI: 10.7256/2409-7543.2016.6.21467. URL: http://e-notabene.ru/nb/article_21467.html
19. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation // Bruce Dang, 2014.
20. The Practice of Network Security Monitoring: Understanding Incident Detection and Response // Richard Bejtlich, 2013.
21. Threat Modeling: Designing for Security //Adam Shostack, 2014.
22. Android Hacker's Handbook // Joshua J. Drake, 2014.
23. The Art of Computer Virus Research and Defense // Peter Szor, 2005.
24. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software // Michael Sikorski, 2012.
25. Reversing: Secrets of Reverse Engineering // Eldad Eilam, 2005.
26. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities // Mark Dowd, 2006.
27. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler // Chris Eagle, 2011.
28. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory // Michael Hale Ligh, 2014.
29. Бирюков А.А. Информационная безопасность – защита и нападение. – 2013.
30. Сердюк В.А. Организация и технологии защиты информации. – 2011.
31. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах. – 2011.