Актуальность темы исследования обуславливается тем, что проблема хакерства изучалась многими учеными, и не имела социокультурного подхода к проблеме. Появляется новая социокультурная профессиональная среда, складываются ранее неизвестные модели поведения и способы социализации. В настоящее время появляется необходимость осмысления процесса формирования киберкультткры, появившейся в результате информатизации общества.

Хакер - чрезвычайно квалифицированный ИТ-специалист, человек, который понимает самые глубины работы компьютерных систем.

Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда элегантным или профессиональным способом

Хакеры бывают разные

Например, О.Б. Скородумова выделяет следующие группы хакеров: "шутники" — осуществляют взлом компьютерной системы для достижения известности, не склонны причинять серьезного вреда системе и выражают себя внесением различных юмористических заставок, вирусов с различными визуально-звуковыми эффектами (музыка, дрожание или переворачивание экрана, рисование всевозможных картинок и т.п.); "фрикеры" - осуществляют взлом телекоммуникационных сетей, подключаются к чужому оборудованию по передаче голоса посредством телефонных, компьютерных, сотовых и спутниковых сетей в личных целях и для обогащения; "сетевые хакеры" — осуществляют взлом интрасети в познавательных целях для получения информации о топологии сетей, используемых в них программно-аппаратных средствах и информационных ресурсах, методах защиты; "взломщики- профессионалы" — осуществляют взлом компьютерной системы с целью кражи или подмены хранящейся там информации; "вандалы" — осуществляют взлом компьютерной системы для ее разрушения: порчи и удаления данных, создания вирусов или "троянских коней".

У хакеров, как и у ИТ-специалистов в целом, есть специализации. Например, фишеры собирают данные аккаунтов (в том числе банковских) через формы на фальшивых сайтах или поддельные приложения. Затем они перехватывают

контроль над аккаунтом и, к примеру, опустошают банковский счет жертвы.

Есть хакеры, которые занимаются брутфорсом (перебором паролей). Чтобы ускорить процесс, они могут создавать целые ботнеты - сети компьютеров, которые совместно занимаются решением одной задачи. Обычно владельцы таких компьютеров даже не подозревают об этом - технику поражает вирус и использует её ресурсы в своих целях. К слову, разработчики вирусов - тоже хакеры.

Зачем хакеры похищают информацию

Данные похищают не из спортивного интереса. Чаще всего их можно дорого продать - особенно если речь идет о промышленном шпионаже в крупных корпорациях. Но данные из личных почтовых ящиков или аккаунтов в социальных сетях также имеют свою цену. Например, компрометирующие фото или переписку можно использовать в суде при разделе имущества супругов. Некоторые охотятся за интинмыми фотографиями знаменитостей, чтобы получить за них выкуп или заработать на продаже таблоидам.

Хакеры как социальная группа

В портретах и историях хакеров можно проследить общие черты, некоторые психологические характеристики. Например, не подлежит сомнению, что большинство хакеров обладает исключительно высоким уровнем интеллекта. Высокие познавательные способности просто необходимы хакерам, так как для успешного доступа на удаленные компьютеры нужны блестящие знания телефонного, компьютерного оборудования и систем. Другой общей чертой всех героев книги является настойчивость, упорство в достижении цели.

Другая типичная картина в историях и биографиях хакеров - неудачный опыт взаимодействия с обществом в детстве: неполные семьи, несложившиеся отношения со сверстниками, одиночество.

Добрые белые хакеры

Есть хакеры, которые занимаются взломом систем для повышения их безопасности. Это белые, или этичные хакеры. Они пытаются найти дыры в системе и способы её взлома, а затем передать данные об этом разработчикам.

Белые хакеры не зарабатывают на продаже краденных данных. Они часто работают добровольно или за плату, которую изначально установил заказчик. Этичные хакеры могут участвовать в программах - когда создатели ПО

гарантируют награды за поиск уязвимостей в новой системе.

Как стать хакером?

Для этого нужно иметь глубокие знания. При этом получать их придется самому, потому что на хакера в университетах не учат. Важно владеть разными языками, уметь мыслить нестандартно, быть креативным и уметь быстро находить решения непростых задач.

Моё мнение о хакерах

польза от них ровно в том, что они являются естественным барьером перед полноценным внедрением всех этих контролирующих функций: хакеры регулярно взламывают базы данных различных крупных компаний и выкладывают в сеть. Да, редко когда информация представляет собой серьёзное открытие, однако это и является сдерживающим фактором: все компании, понимая, что никогда не смогут добиться абсолютной защиты своих проектов, не могут работать на полную, понимая, что если где-то перегнут палку и это просочится в интернет — это приведёт к серьёзным последствиям и к недоверию.

Спасибо за внимание!