Профессиональное образовательное учреждение
«Челябинский юридический колледж»

РЕФЕРАТ
По дисциплине «Информатика»
На тему «Известные кибер-преступники. Кто такой хакер и антихакер. Ответственность за хакерство»

Студент гр. ЗМ-1-22 _____ Ф.А. Золотухин

«__»_____2023 г.

Руководитель _____ Н.В. Яковец

«__»_____2023 г.

Челябинск 2023

Оглавление

Введение

В наше время кибер-преступление распространены из-за развития компьютерных технологий. В этом докладе я постараюсь рассказать о известных преступниках в кибер сфере, о том, кто такие хакеры и антихакеры

1. **Джонатан Джеймс**
2. Джонатан стал первым несовершеннолетним хакером, осужденным в США за киберпреступления. На момент первого совершенного преступления ему было всего лишь 15 лет. Несмотря на свой юный возраст подростку удалось взломать ряд серьезных американских правительственных организаций, включая системы Bell South, школьную систему Miami-Dade и даже сервер подразделения Министерства Обороны США. Так Джонатан получил доступ к персональным данным американских жителей и конфиденциальной информации государственных органов.
3. А в 1999 году он взломал пароль сервера NASA и украл файл первоначального кода международной орбитальной станции. По заявлению NASA, ущерб от хакерской атаки составил около 1,7 миллионов долларов. 16-летний возраст Джонатана смягчил наказание несовершеннолетнего преступника, но полностью избежать тюрьмы не помог.
4. Отбыв наказание, молодой человек стал вести образ жизни законопослушного гражданина. Однако в 2007 году его вновь обвинили в совершении незаконной хакерской атаки. На этот раз его предполагаемой жертвой стала американская многонациональная корпорация универсальных магазинов TJX. По слухам, обвинение было несправедливым, так как Джонатан не был причастен к взлому. Годом позже в 24 года он не выдержал давления общественности и совершил самоубийство, застрелившись из огнестрельного оружия.

2. Кевин Митник

Кевин Митник признан одним из самых неуловимых киберпреступников в Соединенных Штатах Америки. В 80-е годы редко можно было встретить компанию, в систему которой не проникал Митник. На его счету взлом данных Novell, Motorola, Sun Microsystems, NASA и других корпораций. Громче всего имя хакера прозвучало в 1983 году, когда ему удалось получить доступ к компьютеру Пентагона.

За содеянное мужчину многократно арестовывали, однако ему удавалось выходить «сухим из воды» до тех пор, пока за него не взялось ФБР. Тогда Кевин вынужден был «залечь на дно». Однако серьезное наказание не заставило себя долго ждать — в середине 90-х Митник получил серьезный срок за свои преступления. В этом ему помог хакер по имени Цутом Шимомура, который стал одной из жертв Кевина Митника. Обиженный Шимомура сделал все для того, чтобы помочь правоохранителям наказать оппонента по всей строгости закона.

Пять лет и восемь месяцев заключения сделали из Митника полезного члена общества. Он разработал несколько защитных компьютерных систем, а также стал наставником для подрастающего поколения IT-специалистов. Сейчас он читает лекции и проводит консультации по компьютерной безопасности.

3. Альберт Гонсалес

Самым известным хакером 21 века называют Альберта Гонсалеса. Именно он стал создателем ресурса Shadowcrew, который позволял преступникам обмениваться данными украденных банковских карт. Сервис также позволял злоумышленникам продавать и покупать некоторые категории товаров друг у друга. Так называемая биржа собрала порядка четырех тысяч мошенников.

Позже ФБР вышло на Гонсалеса, и хакер пошел на сделку со следствием, предоставляя правоохранителям данные зарегистрированных на портале киберпреступников. Однако на этом преступная деятельность Гонсалеса не закончилась — он создал программу, перехватывающую Wi-Fi-трафик. С помощью разработки он незаконно получил данные более 40 миллионов кредитных карт.

В 2008 году его арестовали за хищение и перепродажу данных 170 миллионов банковских карт. Преступник был приговорен к 20 годам лишения свободы.

Джулиан Ассандж

Свои первые хакерские атаки Джулиан Ассанж, действующий под ником Mendax, совершил еще в 16 лет. В течение четырех лет он взломал системы огромного числа организаций и корпораций. Среди них NASA, Пентагон, Lockheed Martin, Стэндфордский университет.

В 2006 году он разработал и запустил платформу под названием WikiLeaks. На сервисе публиковались секретные данные, которая была получена либо из анонимных источников, либо в результате утечки информации. Позже Ассандж был обвинен в шпионаже.

Адриан Ламо

Одна из самых известных атак Ламо пришлась на 2002 год, когда он попал во внутреннюю сеть The New York Times, назвавшись обозревателем. Также известно, что хакер взламывал сети корпораций Yahoo и Microsoft. В 2004 году Андриан Ламо признался в содеянном и получил наказание в виде шести месяцев домашнего ареста.

Общемировую известность киберпреступник получил после ареста военнослужащего армии США Брэдли Мэннинга, который сотрудничал с Wikileaks. Мэннинг рассказал Ламо, что передал в Wikileaks некоторые секретные материалы. После этого Андриан поделился этой информацией с властями Штатов.

Последние годы перед своей смертью киберпреступник работал частным аналитиком по безопасности. 37-летний Ламо скончался в 2018 году.
С 2012 года киберпреступник жил в Эквадоре, который предоставил ему политическое убежище. Однако это длилось лишь до 2019 года – именно тогда Ассанжа арестовали и поместили в британскую тюрьму.

Кто такие хакеры

Хакер (от английского to hack — «рубить, обтесывать») в широком и положительном смысле — человек, превосходно разбирающийся в устройстве и функционировании вычислительных систем, умеющий быстро найти и элегантно устранить ошибки в их работе. Однако сейчас этим словом также обозначают киберпреступника, который с помощью высоких технических знаний и навыков взламывает информационные системы ради удовольствия, с корыстными или иными целями.

Впервые слово «хакер» было использовано в Массачусетском технологическом институте (MIT) в 1960-х годах задолго до широкого распространения компьютеров. Так называли человека, предложившего грубое решение какой-либо технологической проблемы, не обязательно связанной с компьютерной техникой.

Примерно в то же время руководство этого учебного заведения разрешало использовать студентам университетские компьютеры и ПО в учебных целях только за определенную плату. Некоторые учащиеся были не согласны с такой политикой и стали взламывать программы для бесплатного пользования. Их также начали называть хакерами.

Третье значение термина заключалось в поиске ошибок в аппаратном и/или программном обеспечении для их устранения. При этом хакер не просто сообщал о них, но и предлагал простые и элегантные решения, которые назывались «хак». Похожее значение имеет распространенное сегодня слово «лайфхак».

С развитием телекоммуникационных и компьютерных сетей широкого пользования стал распространяться взлом для развлечения, по идеологическим или корыстным соображениям. Людей, которые занимались правонарушениями, также стали называть хакерами. Хрестоматийный пример взломщика — Кевин Митник, взломавший в США телефонные сети

телекоммуникационных корпораций, правительственных и учебных учреждений.

Виды хакеров

По идеологии

Со временем компьютерные хакеры образовали своеобразную субкультуру, членов которой объединяли любовь к технике, глубокие познания в ней и нестандартное мышление. Однако идеологически сообщество очень неоднородно, поэтому сейчас принято подразделять хакеров на следующие типы:

- **White hats («Белые шляпы»).** Это специалисты, которые ищут ошибки и уязвимости объекта (программы, сайта, компьютерной сети и т.д.) для устранения и повышения информационной безопасности. Как правило, они работают с разрешения владельцев проверяемого объекта или даже являются его сотрудниками.
- **Black hats («Черные шляпы»).** Это злоумышленники, которые взламывают информационные системы (компьютеры, серверы, сайты, программы и т.д.) для прекращения ее работы, вымогательства, кражи данных, с целью личной мести, материальной или другой выгоды, а также по идеологическим и политическим соображениям. Очевидно, он делает это без разрешения владельца объекта, старается скрыть свою личность от него и органов правопорядка, чтобы избежать ответственности.
- **Gray hats («Серые шляпы»).** Обычно так называют хакеров, которые взламывают информационные системы без разрешения владельцев, но потом открыто указывают им на уязвимости и предлагают решения за определенную плату или для своей популярности. Такое хакерство не поощряется, так как в любом случае приносит определенные неудобства, хотя часто оказывается полезным.

Термины сильно размытые и могут трактоваться по-разному как самими хакерами, так и широким сообществом. Кроме того, некоторые известные взломщики (тот же Кевин Митник), будучи осужденными за свои преступления, со временем стали открыто предлагать свои услуги правозащитным государственным органам или владельцам информационных систем за вознаграждение или по доброй воле, перейдя из «Черных шляп» в «Серые» или «Белые». Неопределенным считается и статус различных идеологических формаций хакеров, использующих незаконные методы для достижения благих (в их понимании) целей.

По навыкам

Сообщество хакеров разделяется также по навыкам и компетенциям на следующие категории:

- Script-kiddie — новичок, использующий утилиты, разработанные другими хакерами, для совершения незначительных проделок, и не располагающий глубоким пониманием принципов работы информационных систем;
- Cracker — специалист среднего уровня, который умеет взламывать защиту ПО с помощью чужих утилит (например для личного пользования), но не умеет находить уязвимости сам и создавать свои собственные инструменты;
- Hacker — собственно хакер, эксперт в области аппаратного и программного обеспечения, умеющий самостоятельно находить уязвимости и создавать инструменты для их использования и/или устранения.

В русскоязычной среде также есть аналогичный script-kiddie ироничный термин «кулхацкер» (от неправильного прочтения английского cool hacker), которым обозначают некомпетентного новичка, плохо разбирающегося в технической стороне дела, но сознательно копирующего сленг, манеру поведения профессионального хакера. Зачастую его представление о хакерах-профи основано не на реальности, а на киберпанк-романах и фильмах.

Что умеет хакер?

К важнейшим навыкам хакера можно отнести:

- понимание принципов работы информационных систем на экспертном уровне;
- знание о последних достижениях в области компьютерной и телекоммуникационной техники, программного обеспечения, информационной безопасности;
- понимание не только технических, но и социальных аспектов информационной безопасности — например, стереотипного поведения пользователей и т.д.;
- умение разрабатывать собственные инструменты для поиска уязвимостей и их использование;
- способность нестандартно мыслить для поиска элегантных решений, но при этом избегать сложных методов.

Основные хакерские навыки и умения, а также ценностные установки прописаны в различных неофициальных документах, таких как «Манифест хакера» (США) или «Конвенция самодисциплинирования хакеров» (Китай). В целом, независимо от взаимоотношения общества, закона и хакеров, спрос на услуги последних всегда остается высоким.

Кто такие антихакеры

В первую очередь ошибка состоит в том, что те, кто полагается на сугубо технологическую защиту (условно назовем их антихакерами), недооценивают интеллект «продвинутой» части злоумышленников. Кевин Митник, знаменитый в прошлом хакер, а ныне глава компании Mitnick Security Consulting, не скрывает, что он активно применял в своей практике методы социальной инженерии — умение влиять на людей (в России подобные методы активно применяют «лохотронщики», политтехнологи, а также всевозможные продавцы и маркетологи). Выступая в середине февраля на конференции по информационной безопасности, организованной издательством «Открытые системы» и компанией IDC, Митник подчеркнул, что никакие технологические средства не могут защитить от проникновения в компьютерные системы, если злоумышленники используют методы социальной инженерии. Эти люди обходят системы защиты, воздействуя на тех, кто обладает правами санкционированного доступа к информационным ресурсам, либо используют порой очевидные организационные просчеты и промахи пользователей и системных администраторов.

Увы, антихакеры не хотят ничего об этом слушать, они уверены в возможностях технологий. Митник называет подобную позицию иллюзией безопасности: есть немало людей, которые считают, что беда может случиться с кем угодно, только не с ними.

Бывший хакер номер один не устает подчеркивать, что самое слабое звено в любой системе безопасности (не только информационной) — это человек. Следовательно, чтобы более надежно защитить организацию или предприятие, необходимо постоянно работать с персоналом: регулярно проводить аудит (включая проверки на воздействие социоинженеров), тренинги, тщательно изучать бизнес-процессы на наличие слабых звеньев, и пр.

Ну и, разумеется, необходимо четко распределить зоны ответственности. К сожалению, далеко не на всяком предприятии (зарубежные — не исключение) имеется персона, отвечающая за обеспечение информационной безопасности. Даже там, где она есть, нередко приходится сталкиваться с тем, что организации эффективной защиты препятствуют барьеры между подразделениями и иерархические пирамиды. Чтобы информационная безопасность была по-настоящему действенной, она должна стать делом всей организации, начиная с акционеров и топ-менеджеров и заканчивая рядовыми сотрудниками.

В некоторых организациях директор по информационной безопасности — самостоятельная фигура в обойме топ-менеджеров. Однако гораздо чаще он находится в прямом подчинении начальника службы безопасности или ИТ-директора. В первом случае политика в области информационной безопасности наверняка приведена в соответствие с политикой общей

безопасности предприятия, но нет уверенности в том, что она в полной мере находит отражение в ИТ-инфраструктуре предприятия. Во втором случае информационная безопасность становится неотъемлемой частью инфраструктуры ИТ, но, как правило, слабо связана со стратегией общей безопасности компании и ее реализацией. И то и другое негативно сказывается на эффективности защиты информации. Без использования горизонтальных (не иерархических) связей внутри организации тут не обойтись. Чтобы их задействовать, потребуется талант тонкого политика и умелого организатора. В вашем окружении есть подходящая кандидатура?

Иван Новиков — хакер. Но не киберпреступник. Помимо black-hat-хакеров, взламывающих сайты и приложения ради наживы, есть ещё светлая сторона — white hat, «этичные», или, как их ещё называют, «белые хакеры». Это специалисты в сфере компьютерной безопасности, которые находят уязвимости в системах, чтобы сообщить о них владельцам. Новикова называют одним из самых известных white-hat-хакеров России.

В последние несколько лет 28-летний Новиков чаще выступал в другом качестве — как предприниматель. Сначала — как основатель консалтинговой компании OnSec, работавшей с «Яндексом», Parallels и другими. Теперь — как создатель Wallarm, разработчика решения для поиска уязвимостей и защиты веб-приложений от хакерских атак (Web Application Firewall или WAF).

В этом 2016 году Wallarm прошёл в акселератор Y Combinator и объявил о привлечении $2,3 млн инвестиций. Новиков переехал в Калифорнию и хочет захватить американский рынок защиты веб-приложений. С российским рынком у него всё в порядке уже сейчас — Wallarm один из лидеров: продуктом пользуются «Яндекс», QIWI, «Юлмарт» и другие.

«Секрет» рассказывает, как студенческий фриланс превращается в большой бизнес.

Хакеры с физфака

«Программирую я довольно плохо», — признаётся Иван Новиков. Тем не менее в 2006 году ему, студенту первого курса физфака МГУ, хватало умений, чтобы работать программистом. Спустя два года Новиков даже стал тимлидом в небольшой российской компании, но вскоре решил завязать с разработкой. К этому времени он уже занимался поиском уязвимостей как фрилансер и вёл блог Onsec.ru, где описывал найденные бреши.

В 2009 году на компьютерном фестивале Chaos Construction Новиков занял первое место в конкурсе «Битрикса»: компания предлагала обойти своё решение WAF и взломать сайт, созданный на её платформе. Ссылка на Onsec.ru появилась в новостях, к студенту стали всё чаще обращаться с заказами на аудит системы безопасности. В том числе и «Битрикс» стал регулярно платить за такую работу.

Onsec была зарегистрирована уже тогда, но Новиков был её единственным сотрудником — клиентам было удобнее заключать контракты с юридическим лицом. Параллельно он устроился в Bearing Point (один из крупных игроков на европейском рынке IT-консалтинга). «Надо было узнать, как работает большой хороший консалтинг», — объясняет Новиков. В Bearing Point он неплохо зарабатывал, но продолжал заниматься

консалтингом на стороне — специализировался именно на веб-приложениях, тогда как большинство конкурентов предлагали аудит всего сразу.

В 2010 году Новиков смог позволить себе нанять сотрудников — искал талантливых школьников и студентов на специализированных конкурсах. С расширением команды стали появляться крупные заказы. Один из первых — тяжёлый проект для Parallels в 2011 году, который длился четыре месяца (до этого средний срок проекта был несколько недель). «Мы их не знали, они пришли холодными, — вспоминает предприниматель. — Все отказывались от огромного аудита их исходных кодов, но мы ребята упоротые — взяли и сделали».

Решение уйти с работы и посвятить всё время своей компании пришло после очередного конкурса. В 2011 году Новиков занял первое место в «Месяце поиска уязвимостей "Яндекса"» и понял, что «надо делать что-то интересное, а не фигню». Под интересным он подразумевал некий продукт — в идее большой консалтинговой компании на 300 человек Новиков к этому времени уже разочаровался. По его мнению, такие фирмы развиваются только за счёт бесконечного найма людей — выручка растёт пропорционально их количеству. Но профессионалов в индустрии Новиков видел мало. А учить людей с нуля казалось слишком затратным и долгим процессом. Так он решил стать производителем софта.

«На самом деле я уже лет семь занимаюсь проектом Wallarm — просто я раньше не знал, что именно им», — говорит Новиков. В 2012 году, когда он уволился из консалтинговой фирмы, у его команды уже были наработки технологий. По сути, их просто предстояло объединить в один продукт, но для этого надо было найти новых людей и деньги (OnSec был прибыльным, но не настолько).

Глава 2. Наказание за кибер-преступление

Эксперты «АГ» проанализировали самые популярные составы киберпреступлений, дали рекомендации по их выявлению и рассказали о тонкостях квалификации. Специалисты обратили внимание на неутешительную статистику раскрываемости, единогласно назвав в качестве одной из ее причин неподготовленность кадров в правоохранительных органах. Эксперты сошлись во мнении, что число киберпреступлений в будущем будет лишь возрастать, поскольку злоумышленники быстро адаптируют современные технологии, чтобы повысить свою эффективность.

Сводная статистика за весь период действия норм

Согласно отчету, опубликованному Генпрокуратурой, и расширенным данным, которые были предоставлены ведомством по просьбе «АГ», в 2017 г. число преступлений в сфере информационно-телекоммуникационных технологий увеличилось на 37% (с 65 949 в 2016 г. до 90 587 в 2017 г.). При этом доля таких преступлений от числа всех зарегистрированных в России составляет 4,4%: это почти каждое 20-е преступление.

Саркис Дарбинян, партнер Центра цифровых прав, считает, что рост связан с доступностью и популярностью цифровых технологий. По его мнению, все большее количество людей начинает использовать различные платформы, электронные средства и даже криптовалюты, в связи с чем интерес к киберпространству растет и у преступников, увеличивается количество взломов целых платформ и личных аккаунтов, а также утечек данных со стороны крупных IT-компаний.

Заключение

В заключении хочу сказать, что кибер-преступления будут расти параллельно развитию компьютерной сферы. Но так же будут расти и меры противодействия.

С появлением хакеров появляются антихакеры и соответствующие наказания.

Список литературы

1. https://www.advgazeta.ru/novosti/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/
2. https://secretmag.ru/business/trade-secret/wallarm.htm
3. https://blog.skillfactory.ru/glossary/haker/
4. https://dzen.ru/a/YCPX2P8QoEY3Qffe