# ВЧЕРА

## ИСТОРИЯ КИБЕРПРЕСТУПНОСТИ

Ученые, как вы знаете, зачастую оптимисты и идеалисты. Они нередко видят в своих разработках только лучшее. Люди науки ждут, что их разработки будут применяться только на благо человечества. История повторилась во время создания сети «Интернет». Никто во время создания сети не предполагал, что она будет использоваться кибервзломщиками, мошенниками, компьютерными террористами и продавцами детской порнографии.

Первым шагом к созданию Интернета стала «Сеть Управления перспективных исследовательских программ» ARPANet, созданная по заказу Министерства обороны США. Целью разработки, прежде всего, являлось повышение обороноспособности Америки, а не пересылка котиков или стримы сериалов по подписке. Идея была в том, чтобы создать распределенную компьютерную сеть без ярко выраженного центра. Если бы СССР применил против США ядерное оружие, прообраз Интернета должен был продолжить работать, даже когда поражены некоторые его узлы. Главной задачей, стоящей перед специалистами, было создать сеть связи, которая будет работать даже в условиях ядерной войны. В то время обмен ядерными ударами казался неизбежной реальностью, поэтому в разработке приняли участие лучшие умы США.

Предполагалось, что выход из строя одного узла не отразится на работе остальных, потому что они взаимозаменяемы. Это отличалось от телефонных сетей, где узлы имели иерархичный характер, и выход из строя сегмента верхнего уровня означал невозможность связи со всеми узлами уровнем ниже из остальной сети. Если бы в случае ядерного удара был поврежден главный коммуникационный узел телефонной сети какого-либо штата или региона, то никто бы не смог связаться с этим регионом или штатом по телефону. Прообраз сети «Интернет» был лишен такого недостатка благодаря большей устойчивости к выходу из строя его частей. Если какой-то узел уничтожался, это не сильно влияло на работу всей сети, поскольку коммуникации автоматически перенаправлялись через другой узел. В сети отсутствовала ярко выраженная иерархия, и поэтому она могла продолжать работать, даже если многие из ее узлов были выведены из строя.

Эта особенность архитектуры Интернета до сих пор создает проблемы для правоохранителей любого государства. Иногда доказательства раскиданы буквально по всему миру, и, чтобы собрать улики, приходится обращаться с запросами к правоохранителям разных государств. Кроме того, поскольку связь в Интернете имеет неиерархичный характер, есть возможность использовать запутанное подключение (маршрутизацию), чтобы привести в замешательство следствие. Во время взлома хакер проникает в компьютерную систему через целую цепочку промежуточных узлов. И правоохранительным органам, чтобы установить личность и местоположение хакера, приходится проходить эту цепочку с помощью юридических процедур. Каждый раз надо направлять запрос, получать ордер или напрямую договариваться с полицией других государств, чтобы получить новые доказательства.

Особенности глобальной сети не позволяют заблокировать доступ к противоправной и преступной информации без значительных технических усилий. Потребители и покупатели противоправных услуг и товаров практически всегда, используя специальные средства, смогут посещать ресурсы, объявленные вне закона. Также невозможно

отрезать преступников от принадлежащих им сайтов и ресурсов, так как всегда существует альтернативный путь (маршрутизация).

Ученые в сфере компьютерных наук были сосредоточены на эффективности передачи данных и надежности каналов связи и практически игнорировали риски вмешательства злоумышленников в работу их изобретения. В то время никому не приходило в голову, что сеть будет умышленно использоваться преступниками. На страницах журналов и в интервью на телевидении компьютерные гении пели хвалебные оды новорожденной компьютерной сети. Поскольку никто из ученых мужей даже предположить не мог, что компьютерная сеть в будущем будет наводнена злоумышленниками и киберугрозами, изначально в архитектуре сети не закладывалось каких-либо мер защиты от незаконного использования.

На тот момент сетью пользовались научно-исследовательские институты, которые сами следили за правомерным ее использованием. Предполагалось, что посторонние люди за пределами научных и образовательных учреждений не могли попасть в эту сеть физически. Никто в то время не шифровал данные с целью укрыть их от злоумышленников или государственного вмешательства. Любой, кто имел доступ к сети, мог легко просмотреть всю информацию, передаваемую между узлами. Вопрос шифрования для защиты информации не стоял так остро, потому что на тот момент среди пользователей сети не было «случайных людей». Многие из ученых исследовательских центров были связаны политикой организации, которую они представляли, а также различными соглашениями о неразглашении и законами о государственной и коммерческой тайне.

В тот момент доступ к сети был у лучших из лучших. Компьютерным гениям из лучших университетов США не могло прийти в голову использовать Интернет не по назначению, которое закладывалось на этапе разработки. Естественно, так как это были крайне ответственные люди, которые понимали недопустимость неправомерного использования сети, то зафиксированных инцидентов и правонарушений не было. Такой результат был скорее вызван высокими

моральными качествами пользователей того времени, чем строгими законами и эффективностью правоохранительных органов.

Эта идиллия не могла продолжаться вечно в связи с тем, что количество пользователей сети росло день ото дня. Идея использования компьютеров, соединенных в сеть, очень быстро стала набирать популярность. Такой подход начали использовать как государственные учреждения, так и коммерческие структуры. С распространением персональных компьютеров и появлением модемов, которые могли присоединяться к сети посредством обычной телефонной линии, преимуществами интернет-коммуникации начали пользоваться обычные люди. Сети больших организаций, которые изначально были обособленными, стали объединяться между собой. Стали появляться узлы, которые находились за пределами Соединенных Штатов Америки. Сеть постепенно становилась глобальной и общедоступной.

Естественно, при увеличивающемся количестве пользователей уже нельзя было надеяться на их благоразумность, высокие нравственно-этические идеалы. В сеть пришли подростки и домохозяйки, религиозные деятели и анархисты, компьютерные гики и новички в использовании техники. В Интернете стали обитать люди с совершенно разными целями и задачами, а что еще важней, с разными нравственно-этическими устоями. Многие воспринимали киберпространство как территорию абсолютной свободы, на которой не работали обычные человеческие нормы. У многих пользователей не было моральных качеств, которые бы не позволили им использовать компьютерную сеть для правонарушений.

Использование сети «Интернет» в преступных целях было предрешено, несмотря на оптимизм и веру в светлое будущее ее разработчиков. Это не первый случай в истории, когда создатели технологии не видят рисков ее применения во вред человечеству. Например, мирный атом, который не задумывался как оружие, превратился в «атомную бомбу». Создатели в последующем сожалели о своем изобретении и даже писали петиции о недопустимости применения ядерного

оружия. После первых испытаний и применения атомной бомбы американскими войсками против Японии ее изобретатели оправдывали свое участие в разработке тем, что даже не подозревали о далеко идущих последствиях использования своего детища[1].

Создатели сети «Интернет» также не думали о негативных последствиях своего изобретения. Они и широкая общественность были крайне удивлены, когда преступники взяли сеть в оборот. Новость о первом серьезном интернет-преступлении разлетелась в прессе подобно взрыву атомной бомбы. В 1983 году в Соединенных Штатах в штате Милуоки произошел первый арест интернет-преступника, о котором написали все газеты. Первый интернет-взлом, который привлек внимание прессы, был совершен группой из шести человек, называвшей себя «группа 414» (414 — междугородний телефонный код Милуоки). В течение девяти дней хакеры взломали 60 компьютеров, среди которых были компьютеры центра исследования ядерного оружия в Лос-Аламосе. В состав преступной группы не входили маргиналы или выходцы из неблагополучных семей. Они были профессионалами в компьютерных технологиях и ранее не имели проблем с законом. Один из членов группы хакеров дал показания, и остальные ее участники получили условные сроки наказания на основании показаний первого.

Как выяснили позже, группа состояла в основном из подростков, которые взламывали компьютерные системы ради развлечения и самоутверждения. Они не были матерыми уголовниками, мотивом для них была борьба со скукой в компании единомышленников. В конце концов группу поймал специально созданный отряд ФБР, который подключили к расследованию деятельности хакеров после взлома дюжины правительственных и промышленных систем. Несмотря на то что в результате взлома никакие секретные данные не утекли за границу, схемы ядерных бомб не стали достоянием широкой

[1] Лицо на фоне общего гриба https://nplus1.ru/material/2021/01/03/nuclear-bomb-pt2

общественности, а финансовые средства не пострадали, преступление вызвало огромный общественный резонанс. Правонарушение, совершенное подростками, породило споры в различных кругах. Для всех было очевидно, что государство и общество просто не готовы к возникшей угрозе. В Соединенных Штатах компьютеры использовались повсеместно, но не было даже закона для того, чтобы наказать компьютерных преступников. Также не было специальных подразделений для борьбы с преступлениями против компьютеров и компьютерных сетей.

Стало ясно, что чем выше уровень проникновения компьютерных технологий в государственные и коммерческие структуры, тем более уязвимыми для хакеров они становятся. Подключение любого компьютера к глобальной сети означало, что он становится мишенью для любого киберпреступника по всему миру. Да, благодаря технологиям в Соединенных Штатах произошел взрыв экономического роста и эффективности труда. Да, заслуга информационных систем, что жить стало удобней и интересней. Да, благодаря достижениям в сфере телекоммуникаций в университеты в Соединенные Штаты Америки приехали лучшие умы в сфере компьютерной инженерии и компьютерных наук со всего мира. Но в то же время стало очевидно, какой уязвимой для кибератак эти технологии делают Америку. Цифровизация стала одновременно драйвером развития и в то же время серьезным вызовом для США и их последователей в сфере цифровизации.

Череда громких взломов, которые взбудоражили Америку, привела к тому, что в 1986 году в США был принят первый закон о компьютерных преступлениях (англ. — The Computer Fraud and Abuse Act). Прежде всего, упомянутый нормативный акт уделял внимание защите от киберпреступлений государственных и финансовых учреждений. За компьютерный взлом устанавливались существенные сроки лишения свободы. Так как общественность была всерьез напугана проникновением в компьютеры секретной лаборатории ядерного оружия, отдельно в законе устанавливалась уголовная ответственность

за посягательства на любые учреждения, задействованные в разработке ядерного оружия и других ядерных технологий.

Хакеры напугали всех. Теперь ни государство, ни общество не относились к киберпреступности как к чему-то несерьезному. Еще вчера к их проступкам относились как к обычным шалостям. Осознание того факта, что преступники могут проникнуть в компьютеры ключевых исследовательских и оборонных ведомств, заставило воспринимать киберпреступность всерьез.

В полиции и спецслужбах стали появляться специальные подразделения для борьбы с хакерами. Это оказалось нетривиальной задачей, так как привлечь лучших компьютерных специалистов на зарплаты госучреждений достаточно сложно. Нередки были случаи привлечения специалистов по кибербезопасности и даже кибервзломщиков на краткосрочной основе для расследования конкретных инцидентов. Первое время хакеры существенно превосходили в профессионализме тех, кто за ними охотился.

Все было так плохо, что, как рассказывает известный автор в сфере киберпреступности Марк Гудман в своей книге «Future Crimes», он стал начальником отдела по борьбе с киберпреступлениями в Нью-Йоркской полиции просто потому, что умел включать компьютер и пользоваться программой для печати текстов. Коллеги считали его гуру компьютеров за знания и навыки, которыми сейчас обладает любой школьник. Он руководил поимкой преступников, которые выросли на программировании и изучении компьютерных систем. Зная на момент прихода в полицию только как включать компьютер и пользоваться офисными программами, Марк построил головокружительную карьеру борца с киберпреступлениями. Его скудные знания компьютерных технологий выделялись на фоне абсолютного отсутствия понимания принципов работы компьютеров у его коллег.

Так как нередко для совершения киберпреступлений уже недостаточно знаний одного хакера, стали появляться крупные хакерские группы. Сначала как сообщества единомышленников, обменивающихся тонкостями хакерского искусства, а затем сообщников

по сложным взломам и атакам на продвинутые системы киберзащиты. Стал формироваться целый компьютерный андеграунд, где киберпреступники искали сообщников, делились информацией об уязвимостях и средствами для совершения взломов.

Список киберпреступлений не ограничивался только взломом. Стали возникать новые виды компьютерных преступлений. Первый компьютерный вирус появился уже в 1980-х гг. В 1984 году Фред Коэн (Fred Cohen) опубликовал статью о возможности разработки первых вредоносных саморазмножающихся компьютерных программ. Исследователь придумал называть такие программы «компьютерным вирусом». Он написал программу, которая заражала один компьютер от другого, а также описал возможность появления антивирусных программ. Первый нелабораторный вирус для персональных компьютеров появился в 1986 году. Вредоносная программа с названием «Brain» («Мозг») заражала с помощью дискет. Вирус был создан в Пакистане двумя программистами с целью защиты от бесплатного копирования их программ. Вредоносная программа заражала компьютер пользователя, который использовал программы разработчиков, не заплатив за них деньги. Получается, что первый компьютерный вирус был создан с благой целью, он применялся для защиты лицензионных программ.

Еще один громкий взлом, который заставил обратить на себя внимание, случился в 1998 году, когда 12-летний хакер проник в компьютерную систему, которая контролировала водоспуск плотины Теодора Рузвельта в Аризоне. В случае открытия сливных ворот вода могла затопить города Темп (Tempe) и Месэ (Mesa) с общим числом жителей 1 млн человек. Получается, что продвинутый школьник смог создать угрозу жизни и здоровья множества людей. Инцидент в целом закончился хорошо, и все обошлось без жертв, но после этого случая в прессе появились термины «интернет-терроризм», «компьютерный терроризм» и «кибертерроризм». Стало понятно, что с помощью доступа к информационным сетям можно не только получить секретную информацию или завладеть чужими деньгами, но и вывести

из строя критическую инфраструктуру, а также причинить вред множеству людей.

Но все-таки больше всего внимания общества и СМИ в те годы привлек самый известный киберпреступник эпохи Кевин Митник. Его криминальная история началась еще в 80-х, когда Кевина признали виновным во взломе сети производителя компьютеров Digital и краже их программного обеспечения. После того как никому не известный в то время преступник предстал перед судом, его посадили в тюрьму на год. В местах лишения свободы он проходил принудительное лечение у психиатра, который обратил внимание, что хакинг для Кевина — это естественная потребность, смысл его жизни и способ самореализации. Киберпреступник отсидел не весь срок и вышел на свободу. Согласно условиям своего досрочного освобождения преступник три года должен был находиться под надзором правоохранительных органов. Также суд потребовал, чтобы Кевин никогда не приближался к компьютерам, подключенным в сеть. Ближе к концу срока под наблюдением Митник не выдержал и совершил новое преступление, на котором его поймали. Хакер попался на взломе Pacific Bell, и был выдан ордер на его арест.

С этого момента начинается история, за которую Кевин стал иконой мира киберпреступников. Оказавшись перед угрозой возвращения в тюрьму, Митник решил податься в бега. Преступник не затаился, а вместо этого еще более активно занялся хакерством. В течение следующих трех лет он взломал и украл информацию у десятков организаций[2]. Более того, он отслеживал переговоры сотрудников полиции и ФБР, чтобы эффективно уходить от преследования. Стражи закона и порядка не могли понять, почему преступнику вновь и вновь удается обвести их вокруг пальца. За хакером закрепился образ неуловимого злоумышленника, который действует, на шаг опережая сотрудников правоохранительных органов.

---

[2] A Short History of Law Enforcement and Cyber Crime https://medium.com/threat-intel/cyber-crime-takedowns-66915be7307e

Кто знает, сколько бы еще хакер оставался непойманным, если бы он не перешел дорогу другой иконе мира кибербезопасности Цутоме Шимомура. Их битва стала основой сценария нескольких фильмов. Схватка супергероя и суперзлодея киберпространства до сих пор упоминается во многих книгах по взлому и защите от него. Сначала все развивалось в пользу Кевина, он успешно взломал компьютерную систему Шимомуры, но поймать его не удалось. Когда он осознал, в чью систему проник, в Кевине взыграл азарт, и хакер специально стал атаковать системы, находящиеся под защитой Шимомуры. Киберпреступник настолько обнаглел, что даже прислал своему визави сообщение с угрозами[3]. Специалист по защите компьютерных систем не без труда вычислил местонахождение хакера и передал данные правоохранительным органам. В 1995 году Кевина арестовали в квартире, которую он снимал. Для того чтобы хакер не узнал о готовящемся аресте, полицейские целого городка хранили молчание в эфире до самой поимки преступника.

Кевин Митник вышел из тюрьмы в 2001 году в возрасте 36 лет. Воспользовавшись своей невероятной популярностью, он основал успешную компанию в сфере кибербезопасности. Также знаменитый хакер написал и опубликовал два бестселлера «Искусство обмана» и «Искусство вторжения», где он поделился своим опытом и описал, как происходит взлом и как проникают в системы, используя человеческие слабости. Известного кибервзломщика за большие гонорары стали приглашать на самые статусные ИТ-мероприятия выступить с докладом или лекцией. Читатель может легко найти его видео в сети[4].

Основной посыл, который проходит красной нитью через все выступления и книги хакера, заключается в том, что причиной взлома зачастую становится человеческая глупость и невнимательность. Жертвы сами сообщают необходимые для взлома данные или просто

[3] Кевин Митник: Биографии гиков https://habr.com/ru/post/68273/

[4] World's Most Famous Hacker Kevin Mitnick & KnowBe4's Stu Sjouwerman Opening Keynote https://www.youtube.com/watch?v=iFGve5MUUnE

пускают киберпреступников в свои системы. По словам Кевина, для человеческой глупости нет патча и можно вкладывать огромные средства в развитие технических средств защиты от взлома, но в системе все равно останется слабое звено — человек.

К сожалению, на смену выдающимся хакерам эпохи Кевина Митника пришли еще более злые и профессиональные киберпреступники. Взломы суперхакера 90-х выглядят невинно перед киберпреступлениями следующего поколения. За взломом отдельных компаний и персональных компьютеров последовали преступления, своими масштабами охватывающие весь мир. Разразилась глобальная буря киберпреступности.

Так, разработчикам вируса «ILOVEYOU» удалось к 2022 году заразить 45 миллионов компьютеров по всему миру. Для заражения использовалась та же уязвимость, о фатальности которой заявлял Кевин Митник. Вредоносная программа полагалась на человеческую глупость и невнимательность для того, чтобы передаваться по сети. Жертвы сами заражали свои компьютеры и распространяли вирус дальше. На электронную почту приходило электронное письмо с вложением, которое называлось «LOVE-LETTER-FOR-YOU» («Любовное послание для тебя»). Пользуясь желанием получателя прочитать любовное послание, ему предлагалось открыть приложенный к электронному письму файл. Собственно вложение и являлось вредоносной частью, код вируса перезаписывал файлы, крал пароли и рассылал свои копии всем контактам электронной почты жертвы[5].

Вредоносная программа раскрыла реальный потенциал атак, совершаемых киберпреступниками. Вирус стал настоящим откровением. До этого момента невозможно было представить, что с помощью нажатия кнопки на клавиатуре можно совершить преступление, которое затронет десятки миллионов людей по всему миру. Тем более было удивительно, что такое глобальное преступление было совершено

[5] «Я понял, что многие хотят любви»: журналисты нашли создателя червя ILOVEYOU https://habr.com/ru/news/t/500362/

обычным филиппинским студентом-программистом. Хакер не был профессиональным преступником и не скрывался, поэтому его легко нашли. Так как на Филиппинах отсутствовал закон, по которому его могли привлечь к уголовной ответственности, правоохранительные органы не стали преследовать его. В многочисленных интервью филиппинца-программиста не раз заявлялось, что он мог запустить вирус случайно[6].

Случайность привела к перегрузке систем электронной почты тысяч организаций. Некоторым компаниям пришлось отключать часть инфраструктуры, чтобы остановить распространение вируса. Ущерб от действий хакера оценивали в миллиарды долларов США. Британскому парламенту пришлось на продолжительное время закрыть свою почтовую сеть. В числе пострадавших от вируса были и оборонные структуры, например Пентагон. Вирус вошел в Книгу рекордов Гиннесса как самый разрушительный[7].

Ни один преступник в мире даже не мог и мечтать о том, чтобы его деяние затронуло миллионы людей по всему миру. В то же время обычный студент из Филиппин, не прилагая особых усилий, смог вписать себя в историю криминального мира в киберпространстве. Джин выбрался из бутылки, и его было не засунуть обратно. Киберпреступность стала явлением глобальным, так как давно вышла за пределы отдельных государств или регионов. Как всемирная угроза преступность в Интернете бросила вызов всеобщей стабильности и безопасности.

С каждым разом кибератаки удивляли все большим и большим размахом. В октябре 2002 года была совершена атака, целью которой была остановка работы всей инфраструктуры глобальной сети. Более десяти основных DNS-серверов, от которых зависит работа всего Интернета, подверглись DoS-атаке (Dos сокр. от Denial of Service — атака на отказ работы), начавшейся одновременно с множества компьютеров

---

6 Love Bug's creator tracked down to repair shop in Manila https://www.bbc.com/news/technology-52458765

7 Вирус «I Love You» занесен в книгу рекордов Гиннесса https://securelist.ru/virus-i-love-you-zanesen-v-knigu-rekordov-ginn/4823/

по всему миру. Только нескольким из корневых серверов удалось устоять, и поэтому работа интернет-сервисов DNS не была остановлена. Замысел создателей, которые рассчитывали на устойчивость данной коммуникации даже в условиях ядерной войны, позволил выдержать беспрецедентную атаку на Интернет. Большой уровень избыточности, присущий структуре сети, позволил избежать остановки Интернета, несмотря на выход из строя двух третей основных узлов. Несмотря на то что у атакующих не получилось «сломать» Интернет, данный случай породил общественную дискуссию о выросших возможностях хакеров.

Эта атака обнажила новую угрозу: мир стал зависеть от глобальной сети все больше. Финансовые институты, торговые площадки, государственные учреждения, платформы досуга и развлечений — все полагались на надежную работу сети «Интернет». Рост количества киберпреступлений во многом был связан с тем, что глобальная сеть стала неотъемлемой частью человеческой жизни.

Произошла цифровизация и политической сферы. Кибератаки постепенно стали средством давления на противника в ходе вооруженных конфликтов. Так, конфликт в Косово считается первой интернет-войной. Компьютерные активисты использовали сеть «Интернет» для осуждения действий, предпринимаемых как Югославией, так и НАТО. Самым распространенным способом стал тот, при котором совершались умышленное нарушение работы правительственных компьютеров и получение контроля над сайтами с последующим изменением содержимого, так называемый «дефейс» (англ. — «deface»). В Интернете распространялись истории об ужасах данного вооруженного конфликта с обвинением сторон[8]. Нередко в результате таких атак на официальных сайтах ведомств можно было увидеть оскорбления в адрес ведущих политиков стран или каких-либо политических групп.

[8] Kosovo Being Called First Internet War https://www.sfgate.com/news/article/Kosovo-Being-Called-First-Internet-War-Web-2936299.php

Апогеем кибервойны стали атаки на правительственные сайты Соединенных Штатов Америки. Так, группа под названием «Hong Kong Danger Duo» полностью удалила сайт Белого дома (www.whitehouse.gov), оставив вместо официальных страниц с информацией сообщение «Протестуйте против нацистских действий США! Протестуйте против жестоких действий НАТО!». Сообщения подобного характера появились еще на сотнях сайтов правительственных и коммерческих структур в Соединенных Штатах и других странах НАТО. Некоторые серверы пытались защититься, блокируя весь трафик с доменов.cn и.yu. В какой-то момент правительства США и стран НАТО пригрозили, что отключат югославский домен «.yu» от международной сети[9]. Конфликт в сети не закончился даже после прекращения огня, атаки на киберструктуры США и НАТО продолжались на протяжении десятилетия после конфликта. Инциденты, связанные с принудительным разделом Югославии, случаются в сети до сих пор.

В дальнейшем любой международный политический или военный конфликт сопровождался атакой на правительственные онлайн-структуры. Например, в 2005 году волна интернет-атак была спровоцирована школьным учебником истории, вышедшим в Японии. Учебное пособие искажало события в Китае в 1930–1940-х гг. XX в. Учебник умалчивал о военных преступлениях японских войск во время интервенции, о геноциде против китайского народа и истреблении миллионов ни в чем не повинных граждан. Ложь об историческом событии возмутила общественность в Китае и подтолкнула к активным действиям прокитайских хакеров. В списке атакуемых оказались ведущие японские министерства и ведомства, сайты крупнейших японских корпораций и национальные интернет-ресурсы, посвященные Второй мировой войне. Хакеры буквально «прошлись» по всем ключевым правительственным сайтам Японии, публикуя оскорбления

[9] Case of the cyber war: Kosovo conflict https://inspiratron.org/blog/2014/07/01/case-cyber-war-kosovo-conflict/

и ругательства на английском и японском языках. Личность хакеров так и не была установлена, но, по мнению многих зарубежных изданий, за такими атаками стоят китайские хакеры, финансируемые правительством[10]. Данное предположение косвенно подтверждалось слаженностью и синхронностью действий большого числа отдельных киберпреступников.

Несмотря на то что в таких войнах в киберпространстве не было человеческих жертв, они приносили огромные убытки. Государственные структуры и частные компании несли расходы на восстановление поврежденных сайтов. Расследование инцидентов и усиленные меры кибербезопасности требовали дополнительного финансирования. Люди не могли зайти на информационные ресурсы и получить информацию либо доступ к услуге. Кроме того, подобные атаки сеяли в обществе уверенность, что хакеры могут все, и даже государство не может с ними справиться. Не уверен, пугали ли в то время детей хакерами перед сном, но их стали принимать всерьез и бояться.

С середины 2000-х годов киберпреступления стали все чаще и чаще совершаться из корыстных мотивов. Прошло время киберпреступников, которые просто хотели привлечь внимание или заявить о себе. Ушли на задний план идеалисты, которые боролись за свободу информации. Стали сходить на нет истории с вирусами, заражавшими все и вся. Чаще преступления в сети «Интернет» стали совершаться с целью обогащения. Так, самыми известными и распространенными вирусами конца 2000-х и начала 2010-х годов стали вирусы, зарабатывающие деньги для своих владельцев и разработчиков.

Например, известный вирус «Zeus» («Зевс»), созданный российским хакером, инфицировал компьютерные системы через сообщения электронной почты или поддельные уведомления. Пользователь заражал свой компьютер данным вирусом после открытия ложного

[10] 2019: Cyber War — Part 1 https://www.forbes.com/sites/rajindertumber/2018/12/31/2019-cyber-war-part-1/

сообщения. Проникая в систему, вредоносный программный код похищал логины, пароли и пин-коды кредитной карты жертвы. «Зевс» делал это посредством записи всех нажатий клавиш, которые нажимает пользователь на клавиатуре[11]. Фактически зловред отслеживал абсолютно всю вводимую на клавиатуре компьютера информацию. Кроме того, вирус незаметно для жертвы мог менять данные для входа на различные сайты, например контрольный вопрос для восстановления пароля. В отличие от более ранних вирусов «Зевс» распространялся дальше незаметно для пользователя. Он рассылал сам себя с зараженного компьютера посредством электронной почты. После рассылки вирус удалял информацию об отправленных сообщениях, поэтому пользователь не мог догадаться, что его компьютер заражен и участвует в дальнейшей рассылке вредоносного кода.

Данный вирус не стремился к максимальному мировому охвату компьютерных систем или к тому, чтобы сделать своего создателя знаменитым. Он просто крал деньги со счетов жертв, пытаясь оставаться максимально незаметным. По оценкам некоторых экспертов в сфере кибербезопасности, одна из групп хакеров, использующая вирус в Европе, нанесла суммарный урон жертвам в размере 36 млн евро[12]. Широкомасштабное заражение вирусом охватило такие европейские страны, как Испания, Италия, Германия и Нидерланды. Кроме персональных компьютеров вирус заразил много телефонов и других мобильных устройств.

Следует отметить, что вирус до сих пор применяется и развивается. Предполагаемый автор разработки «Зевса» создал программу-конструктор, которая позволяет адаптировать исходный код вируса под конкретные задачи преступников. Создатель (создатели) вируса продает(ют) конструктор для разработки модифицированных версий всем желающим. К программе прилагаются подробные инструкции, кроме того, за дополнительную плату предоставляется техническая

[11] Охота за российским хакером https://tjournal.ru/stories/42272-ohota-za-rossiyskim-hakerom

[12] https://ru.wikipedia.org/wiki/ZeuS

поддержка вредоносного программного обеспечения[13]. Таким образом, вирусописателей с определенного времени стали интересовать преимущественно деньги, и прекратились истории, когда вирус распространялся случайно или просто для привлечения внимания к персоне хакера. Значимость любого программного средства для профессионального хакера стала оцениваться не охватом и вызванным резонансом, а возможностью заработать и скрыться от преследования.

Когда традиционный преступный мир стал осознавать, насколько Интернет эффективное и удобное средство для совершения преступлений, популярность его использования в противоправных целях стала расти. Кроме стандартных для хакеров взломов компьютерных систем и распространения вирусов к списку распространенных киберпреступлений добавилось компьютерное мошенничество. Данный вид преступной деятельности благодаря использованию сети «Интернет» стал автоматизированным и приобрел трансграничный характер.

Например, одним из первых распространенных глобальных способов отъема денег у доверчивых граждан стали «нигерийские письма». Суть данного метода обмана в том, что преступник рассылает текст сообщения, предлагая под тем или иным ложным предлогом перевести на счет мошенника деньги. «Как правило, мошенники просят у получателя письма помощи во многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются определенные суммы денег под предлогом оформления сделок, залогов, уплаты сборов и т.д.»[14]. Схема, придуманная в то время, с некоторыми доработками актуальна и сейчас.

Мне, например, на электронную почту несколько лет назад пришло письмо якобы бывшего короля одного из африканских государств. Мошенники предлагали стать миллионером, если я помогу им вывести

---

[13] Небольшой обзор исходного кода трояна zeus https://habr.com/ru/post/119780/

[14] Фадина Ю. П. Уголовно-правовая характеристика мошенничества в сети «Интернет» // Вестник Югорского гос. ун-та. 2017. № 1–2 (44). С. 117–121.

миллиарды долларов из страны, в которой произошел вооруженный переворот и смена власти. Так как это касалось темы моего исследования, и мне были интересны дальнейшие действия преступников, я, конечно, ответил, что всю жизнь хотел быть миллионером. Следующим письмом мне, как и полагается по сценарию данного криминального сюжета, предложили перевести небольшую сумму взноса для того, чтобы обналичить деньги. На этом моменте и закончилась моя переписка с преступниками, потому что мне было известно, что произойдет дальше. Преступники продолжили бы выманивать из меня небольшие суммы под разными предлогами до тех пор, пока я бы не остановился или у меня не закончились деньги. При этом для меня не было смысла обращаться в правоохранительные органы, так как преступники были за границей и вряд ли их когда-нибудь бы привлекли к ответственности.

Интернет предоставил преступникам уникальную возможность эффективно добираться до своих жертв в любых уголках мира. Например, даже самый усердно «работающий» уличный грабитель вряд ли бы смог ограбить больше 20–30 человек в день. Его преступная деятельность была бы ограничена территориально, а поэтому местное население знало бы о злоумышленнике и избегало бы мест, в которых промышляет преступник. При этом его интенсивная работа была бы сопряжена с огромным риском, так как жертвы могут сопротивляться, да и органы полиции не всегда дремлют. Описанные ограничения и трудности не действуют в киберпространстве. Осуществляя преступную деятельность в Интернете, преступник буквально мог не вставать со своего кресла. Потенциальными жертвами стали миллионы людей по всему миру, подключенные к глобальной сети. А самое главное — киберпреступление не предполагает никакого непосредственного контакта с жертвой и рисков, сопутствующих этому. Если у кибермошенника не получилось обмануть одного человека, всегда можно найти простофилю в любой другой точке мира.

Как только киберпреступность стала трансграничной и глобальной, оказалось, что вообще непонятно, как привлекать преступников

к ответственности. Некоторые авторы упоминают данную трудность как «Бангладешская проблема»[15]. Смысл ее в том, что любой закон ограничен в пространстве. Например, если совершено противоправное действие в отношении вас в киберпространстве, может оказаться, что правонарушитель избежит тюрьмы, так как он совершал деяние с территории Бангладеш, где, согласно законам страны, это вообще не считается правонарушением либо может отсутствовать механизм привлечения к ответственности правонарушителя из-за рубежа. Ведь мало заявить, что кто-то преступник, необходимо добиться его выдачи в государство, где на него заведено уголовное дело. Возможно, что в стране, откуда действует преступник, нет технических возможностей найти его и задержать. В этом вся суть «Бангладешской проблемы»: преступникам достаточно выбрать нужную страну, и это поможет им избежать тюрьмы.

Ярким примером являются упомянутые ранее «нигерийские письма». Поскольку долгое время нигерийские киберпреступники по своим возможностям значительно превосходили правоохранительные органы их страны, в Нигерии отмечался стремительный рост случаев кибератак и кибермошенничества против жертв в странах Европы и Соединенных Штатах Америки. Укомплектованные до зубов правоохранительные органы развитых цифровых экономик ничего не могли сделать против хакеров, защищенных беспомощностью своей киберполиции. Такая безнаказанность, а также худшее по сравнению со странами Европы и Северной Америки материальное положение жителей Нигерии толкали к совершению киберпреступлений все новых и новых нигерийцев. Существовали даже семейные преступные группировки, передававшие свои знания о киберпреступном ремесле своим родственникам.

Как справедливо заявил по поводу проблемы разгула киберпреступности один из специалистов, «ключом (к киберпреступности)

[15] Lemley M.A., Volokh E. Law, virtual reality, and augmented reality // University of Pennsylvania Law Review. 166(5). 2018. P. 1071–1172

в действительности является отсутствие правоохранительной среды, ощущение, что вы можете делать почти все что угодно, и это сойдет вам с рук. Они (отдельные киберпреступники) смогли вырасти и превратиться в организованные предприятия»[16]. Таким образом, отсутствие возможностей правоохранительных органов некоторых стран бороться с киберпреступлениями породило возникновение своеобразных мировых центров киберпреступности, где значительная часть населения была вовлечена в противозаконную деятельность в киберпространстве.

Стала складываться практика, что организованные группы киберпреступников работали с территории стран, в которых редко привлекают к уголовной ответственности за компьютерные преступления. А жертв, наоборот, выбирали из развитых стран, где было обеспеченное население, которое легко могло удовлетворить запросы злоумышленников. Соответственно жертвы таких преступлений чаще всего были из стран Западной Европы и Соединенных Штатов Америки. Как вы понимаете, у Нигерии, стран Восточной Европы и некоторых других государств не было ресурсов и возможности преследовать компьютерных преступников, потому они в течение десятилетия чувствовали себя абсолютно безнаказанно.

Преимуществами Интернета стали пользоваться не только мошенники. Трансграничность глобальной сети пришлась по вкусу злоумышленникам, которые распространяли преступную информацию. Особенно активно в 2000-х годах стали распространяться порнографические материалы, в том числе детская порнография. Часто студии и сайты, участвующие в создании и распространении запрещенных материалов, располагались в азиатских и африканских государствах либо на территории стран Содружества Независимых Государств. Вебпорнография стала популярным бизнесом. По оценкам некоторых экспертов, раскрученный порнографический сайт в то время приносил

[16] Is Nigeria Really the Headquarters of CyberCrime in the World? https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/

доход до 2 млн долларов ежегодно. А владельцы самых известных ресурсов заявляли, что их прибыль составляет от 500 до 1000%[17]. Такая сверхприбыль, о которой не могли мечтать даже мексиканские наркокартели, привлекла организованные криминальные группировки со всего мира. Подобный бизнес стал сопровождаться незаконным удержанием людей (чаще всего женщин и детей), сексуальным рабством и принуждением к сексу.

При этом отследить киберпреступников в сети становилось все сложнее. Поскольку в то время стали складываться системы оплаты, которые были не так прозрачны, как обычные деньги, правонарушителям стало еще проще скрываться от правоохранительных органов. Финансовые потоки в нелегальных видах интернет-бизнеса оказались скрыты от государства благодаря появлению такого феномена, как интернет-деньги. В 2000-х появилось много всевозможных денежных интернет-систем: PayPal (от «pay palace» — «дворец оплаты»), eGold (от «electronic Gold» — «электронное золото»), WebMoney (рус. — «сетевые деньги») и RuPay (от «Russian Pay» — «русская оплата») и т.д. Чтобы создать счет в подобной системе в то время, не нужно было ни паспорта, ни каких-либо других идентификационных документов.

В 2009 году появилась система платежей «Биткоин», которая была независимой от каких-либо государств или коммерческих структур. Безопасность транзакций обеспечивалась за счет шифрования (криптографии). Ни один банк или другая финансовая организация, принадлежащая государству или какому-либо международному органу, не могла отменить или блокировать транзакцию. Биткоин и большинство криптовалют, которые появились позже, обеспечивают высокую степень анонимности сторонам. Информация о транзакциях хранится на компьютерах участников сети криптовалюты, и все транзакции между всеми адресами общедоступны, но при этом отсутствует информация о лицах, осуществляющих транзакции. Для

[17] Репецкая А. Л. Российский криминальный рынок услуг: структура и характеристика отдельных видов // Криминологический журнал Байкальского ун-та экономики и права. 2008. № 1. С. 33.

совершения финансовой операции в биткоинах необходим только номер электронного кошелька. Естественно, преступный мир быстро отреагировал и перешел на новый вид оплаты, который был далеко за пределами власти правительств.

Криптовалюты стали средством платежа для любых видов преступлений. Например, такая сфера преступной деятельности, как отмывание денег, перешла на криптовалюты. Поскольку обращение криптовалюты осуществляется в обход международных и национальных правил валютного контроля, биткоин и подобные ему валюты становятся идеальным средством для проведения незаконных операций незаметным для государства способом. Как справедливо отмечается в некоторых работах, в результате размещения преступных денег в криптовалютах уничтожается большинство доказательств, которые позволили бы надзорным и правоохранительным органам отследить инкриминируемые средства до их источника[18]. Кроме того, в результате перевода денег из одной криптовалюты в другую или с одного криптосчета на другой обнуляется история происхождения средств, полученных преступных путем.

Преступник, который занимается отмыванием преступных денег, способен создать длинную цепочку переводов между различными криптовалютами. Единственным следом длинной последовательности транзакций в таком случае будет информация на личном ноутбуке или компьютере преступника. Таким образом, злоумышленник способен в любой момент устранить все уличающие его доказательства. Многие преступники специально ставят на свои рабочие компьютеры программы, которые по одному нажатию уничтожают все данные без возможности их восстановления. Для этого достаточно нескольких десятков секунд ожидания, после этого все улики будут уничтожены.

Следует отметить, что киберпреступность в России развивалась по закономерностям, отличающимся от стран Западной Европы и Северной Америки. В то время когда в США хакеры уже атаковали

[18] Teichmann F.M.J., Falker M.-C. Cryptocurrencies and financial crime: solutions from Liechtenstein // Journal of Money Laundering Control, 2020. DOI: 10.1108/JMLC-05-2020-0060

секретные правительственные объекты, в России сеть «Интернет» отсутствовала в принципе. Поскольку не были распространены персональные компьютеры, преступления в сфере компьютерной информации были большой редкостью.

Интернет появился в России в начале 90-х гг. С этого времени стал быстро увеличиваться русскоязычный сегмент сети. Это отражалось как в растущем количестве пользователей, так и в объеме размещаемой информации. Когда количество компьютерной техники и пользователей Интернета в России достигло критической массы, стало расти количество преступлений, связанных с информационными технологиями. С 2000 по 2005 год произошел бурный всплеск киберпреступности, и количество зарегистрированных преступлений в сфере компьютерной информации выросло с 800 в год до 10 000[19]. Страна только выходила из криминального кризиса 90-х гг., и правоохранительным органам было совсем не до каких-то «чудаков в мятых свитерах» с немытыми волосами. Общество требовало борьбы с другими видами преступных деяний (заказные убийства, ОПГ), и именно им были посвящены все усилия.

Чтобы вы понимали, насколько у правоохранительных органов были другие приоритеты в 90-х и насколько им должно было наплевать на хакеров, приведем несколько цифр. Например, одной из причин игнорирования киберпреступности стал резкий рост насильственных преступлений в 1990-х гг. Смертность от убийств в России в то время стремительно росла. Громкие убийства стали постоянной темой выходивших в то время газет. В начале 1990-х гг. среднегодовой прирост убийств составил 20%, в то время как вся преступность выросла на 13%. При этом взлет количества убийств нельзя было оправдать демографией, поскольку прирост населения составил всего 0,4%[20]. Особо большой рост наблюдался в числе заказных убийств[21].

---

[19] Дремлюга Р. И. Интернет-преступность. Владивосток, 2008. 240 с.

[20] Badov A. Geography of crime in Russia: Changes during the post-soviet period // Vestnik Moskovskogo Universiteta. Seriya 5: Geografiya. 2. 2009.

[21] Chervyakov V., et al. The changing nature of murder in Russia // Social Science and Medicine. 55 (10). 2002.

В то время организованная преступность представляла реальную угрозу существованию российского государства. По официальной информации, на территории России действовало более 150 преступных сообществ, которые контролировали до 40 000 государственных предприятий и более 90% частных предприятий[22]. В начале 1990-х гг. банковская преступность занимала первое место среди организованной преступной деятельности, и при содействии банковских работников на основе поддельных документов собирались огромные средства[23]. Это отвлекало основные ресурсы правоохранительных органов и общества от проблемы киберпреступности. Были созданы специальные структуры для противодействия экономической и организованной преступности, а также кредитно-денежным преступлениям. Как раз в это время в США и странах Европы начинали возникать специализированные подразделения силовых структур по борьбе с киберпреступностью, но России было совсем не до этого.

Я сам проводил исследования общественного отношения к компьютерной преступности в середине 2000-х. Многие опрошенные не принимали такой вид преступности всерьез, более того, они сочувствовали киберпреступникам и считали, что компьютерный взлом — это неотъемлемый атрибут свободы слова и демократии. Проведенный мной опрос показал, что преступная деятельность в киберпространстве зачастую не рассматривалась как преступление, за исключением распространения порнографии (75,8%), детской порнографии (90,8%), вербовки в террористические организации (80,4%) и распространения информации о том, как сделать взрывчатку (62,1%) или наркотики (81,6%)[24].

Государство в 90-х и начале 2000-х полностью игнорировало проблему киберпреступности в России. Например, в Федеральной

---

22 Kuznetsova N. Crime in Russia: Causes and prevention // Demokratizatsiya. 2 (3). 1994; Chervyakov V., et al. The changing nature of murder in Russia // Social Science and Medicine. 55 (10). 2002.

23 Kuznetsova N. Crime in Russia: Causes and prevention // Demokratizatsiya. 2 (3). 1994.

24 Dremliuga R. Subculture of hackers in Russia // Asian Social Science. 10 (18). 2014. Available from: http://www.ccsenet.org/journal/index.php/ass/article/view/39698

программе Российской Федерации по усилению борьбы с преступностью на 1994–1995 гг. не было ни одного положения или даже упоминания о компьютерных преступлениях, киберпреступлениях или преступлениях в сфере компьютерной информации. Федеральная программа была посвящена борьбе с организованной преступностью и терроризмом, противодействию преступлениям против личности и собственности, преследованию экономических преступлений и коррупции, борьбе с преступлениями в Вооруженных силах, и она должна была обеспечить международное сотрудничество в борьбе с преступностью. Подобное можно было наблюдать и в других государственных документах. Власти страны не интересовали хакеры и виртуальные преступления, государство утопало в крови в результате заказных убийств и было связано по рукам и ногам оргпреступностью и коррупцией.

Беспрецедентный рост количества киберпреступлений не был обусловлен только пренебрежением со стороны общества и государства. Катализатором роста стало увеличение числа пользователей Интернета в России. С 1996 по 2000 год число российских интернет-пользователей увеличилось в четыре раза. Наибольший рост интернет-аудитории наблюдался среди пользователей 16–24 лет. У молодого человека меньше опыта, он еще формирует свои моральные ориентиры и не понимает, что хочет от жизни. Молодежь понимает характер своих действий и их последствий. Рост подростковой аудитории Интернета без должного государственного контроля привел к росту компьютерной преступности среди молодежи.

Все это совпало с кризисом образовательной системы. Некому было объяснять молодому человеку, что такое хорошо, а что такое плохо. Родителям также было не до воспитания детей, поскольку надо было адаптироваться к условиям глубокого политического и экономического кризиса. Многие опросы показывали, что парни мечтают об участии в организованной преступной группировке, а девушки не прочь стать содержанками. На этом фоне карьера киберпреступника выглядела как что-то гораздо более социально одобряемое.

Изучая уголовные дела во время своей учебы в аспирантуре по юриспруденции, я наткнулся на материалы по преступлению, совершенному парнем с моего потока, с которым я учился на ИТ-специальности. Из текстов допроса обвиняемого и других материалов дела было очевидно, что мой знакомый не осознавал последствия и даже не понимал, что он совершает преступление. Действительно, его деяние было не настолько опасно, чтобы внушать страх. Он, воспользовавшись чужим паролем, подключался в Интернет, причинив убытки владельцу доступа на 500 руб. Поразительно, что, доказывая свою невиновность, горе-хакер апеллировал к тому, что все делают так же, как он. Справедливости ради, так и вправду делали многие, что следует из материалов дел по другим преступлениям, которые мне попадались в то время.

Большинство российских киберпреступников не имели устойчивой внутренней установки на совершение преступления. Многие совершали правонарушения из любопытства или потому, что считали их деяние незначительным для наказания. Одну фразу из допроса обвиняемого в самом первом деле, попавшем мне в руки, я помню до сих пор. Молодой парень, который являлся студентом одного из известных мне университетов, после описания, что и как он совершил, описал момент визита сотрудников правоохранительных органов следующим образом: «В один прекрасный день ко мне пришли сотрудники милиции и удивили меня тем, что я, оказывается, совершил преступление».

Компьютерная информация не считалась в обществе чем-то таким, что должно охраняться уголовным законом. Так, в России начала 2000-х процветало компьютерное «пиратство». Более 90% продаваемых компьютерных программ распространялось без соблюдения авторских и смежных прав. В любом городе можно было найти рынок или ларек, в котором продавали незаконно скопированные операционные системы (чаще всего Windows), офисные программы, игры и многое другое, что стоило приличных денег официально. А средств у населения страны, не отошедшей от экономического кризиса 90-х, было не много. Размах нарушения авторских и смежных прав лишь отчасти был связан с недостаточно высокими доходами населения.

Нелицензионные программы широко использовались не только отдельными лицами, но и целыми организациями и учреждениями, в том числе государственными. Несмотря на повсеместное использование нелицензионных программ, вы найдете в архивах не так много уголовных дел, связанных с компьютерным пиратством.

Несмотря на угрожающую статистику киберпреступлений, вряд ли цифры отражали реальное состояние дел в компьютерной преступности 90-х и 2000-х. Как показывает практика, большинство возбужденных дел были безобидными, а действительно опасные правонарушения оставались незамеченными[25]. Ловили тех, кто не имел опыта сокрытия улик и навыков обеспечения анонимности в сети. Были и другие причины, почему опасные случаи не попадали в поле зрения общественности. Например, зачастую банки и другие коммерческие предприятия не делились информацией об успешных кибератаках и не сообщали о преступлениях в полицию, поскольку беспокоились о своей репутации[26]. Такое укрывательство компьютерных инцидентов было характерно и для зарубежных стран.

Другой очевидной причиной того, что в основном выявлялись неопасные киберпреступления, была низкая техническая оснащенность правоохранительных органов, а также нехватка людей, которые бы могли выявлять и расследовать высокотехнологичные инциденты. В то время российские правоохранительные органы были оснащены ничуть не лучше, скажем, нигерийских. Как говорилось ранее, неспособность силовых структур справиться с киберпреступниками рождает в них уверенность в своей безнаказанности и привлекает в их ряды новых злоумышленников.

Автор объяснял выше, почему борьба с киберпреступностью — нетривиальная задача. Во-первых, требуются квалифицированные кадры, которым надо хорошо платить. В 90-х и начале 2000-х государство не имело достаточно ресурсов, чтобы привлекать

---

[25] Ястребов Д. А. Вопрос о латентности неправомерного доступа к компьютерной информации в Российской Федерации // Юридический мир. № 10. 2008.

[26] https://www.crime-research.ru/articles/Sabodash0304

в правоохранительные органы лучшие кадры в сфере ИТ-безопасности. Во-вторых, общество не поддержало бы идею привлечения дополнительных ресурсов на борьбу с киберпреступностью, когда в стране был разгул организованной преступности и высокий уровень убийств. Также следует не забывать, что специалистов в сфере именно кибербезопасности было не так много, в России отсутствовала ИТ-индустрия, где могли бы вырасти такие профессионалы. Несмотря на то что в нашей стране всегда было много людей, разбирающихся и интересующихся техникой и программированием, чтобы вырастить из них профессионалов кибербезопасности или специалистов цифровой криминалистики, требовались время и деньги. Кроме того, чтобы успешно противостоять преступникам в глобальной сети, нужна была современная материально-техническая база, которая у российских правоохранительных органов отсутствовала.

Ситуация с киберпреступностью постепенно стала меняться в лучшую сторону в середине 2000-х. Когда жизнь в России стала экономически и политически стабильней, государство обратило внимание на преступников в киберпространстве. Стали очевидны масштабы угроз, исходящих от киберпреступности, для устойчивого развития российской экономики и стабильности российского общества. Государство постепенно пришло к идее, что развитие высокотехнологичных отраслей невозможно без обеспечения кибербезопасности, охраны особо важной компьютерной информации и понятной для общества политики в сфере борьбы с компьютерной преступностью.

С 2010 года стал активно меняться российский уголовный кодекс. Изменения касались киберпреступлений. В уголовном законе с момента его принятия в 1996 году присутствовали нормы, посвященные преступлениям против компьютерных систем. Они были собраны в одной Главе 28 под названием «Преступления в сфере компьютерной информации». В главе было три статьи, посвященные отдельным видам киберпреступлений: неправомерному доступу к компьютерной информации (ст. 272), распространению вредоносных программ

(ст. 273) и нарушению правил эксплуатации компьютерной техники (ст. 274). Так вот с момента принятия уголовного закона текст этих статей практически не менялся. Лишь в 2010 году законодательные органы России приступили к активной модернизации Уголовного кодекса РФ, чтобы он соответствовал времени.

Слабый контроль над сетью в 90-х и начале 2000-х означал, что кроме преступлений и преступной информации среди граждан могут спокойно распространяться антивластные и экстремистские призывы. Преступная информация оставалась в сети даже после привлечения преступника к уголовной ответственности. Более того, отсутствие юрисдикции над операторами иностранных сайтов приводило к ситуациям, когда часть информации не могла быть запрещена уголовным преследованием ее распространителя.

Поэтому следующим шагом стало создание органа, задачей которого было контролировать сеть и блокировать нежелательные ресурсы. Очевидным решением было создание правовой базы, обязывающей интернет-провайдеров ограничивать доступ к таким сайтам. Таким государственным органом, отвечающим за ограничения в киберпространстве, стал Роскомнадзор (полностью — Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций) (http://roskomnadzor.ru/). Роскомнадзор может (или утверждает, что может) блокировать опасные для общества и нежелательные сайты, выдавая предписания российским компаниям, предоставляющим доступ в Интернет. Для этого был создан специальный список адресов заблокированных сайтов, ведением которого занимается Роскомнадзор (https://eais.rkn.gov.ru/faq/).

Конечно, действия федеральной службы иногда становились поводом для шуток. Не все у Роскомнадзора получалось так, как он хотел. Например, во время знаменитой блокировки мессенджера Telegram были заблокированы многие не связанные с ним сайты и телекоммуникационные каналы. Известные российские компании испытывали проблемы с осуществлением электронных платежей. Пострадали даже сайты государственных органов и государственных компаний.

Не работали терминалы платежей и многое другое. А цель по блокировке мессенджера так и не была выполнена. Борьба федеральной службы с Telegram стала популярным сюжетом сетевого фольклора. Несмотря на некоторые неудачи, обычно Роскомнадзор справляется с блокировкой сайтов, к которым надо ограничить доступ с территории России.

Идея блокировать содержимое сети не была абсолютно новой, поскольку многие государства раньше России начали блокировать и фильтровать контент, передаваемый в сети «Интернет». Например, в Китае действует «Великий китайский файрвол» (англ. «Great firewall of China») по аналогии с Великой Китайской стеной (англ. — «Great Wall of China»). Великая китайская интернет-стена блокирует доступ ко многим иностранным сайтам и замедляет трансграничный интернет-трафик. Также технология ограничивает доступ к иностранным интернет-издательствам и блокирует популярные иностранные интернет-сервисы (например, Google Search, Facebook, Twitter, Wikipedia и многие другие). Также в Китае не работают либо замедляются многие мобильные приложения и мессенджеры, если иностранные компании не выполняют требования китайских нормативных актов.

Получается, что борьба с хакерами спровоцировала государства усилить меры по безопасности цифрового пространства в целом. В киберпространстве стало менее удобно осуществлять свою деятельность наркоторговцам, распространителям детской порнографии, мошенникам и другим преступникам. Нельзя сказать, что киберпространство стало совсем безопасно, но теперь оно выглядит значительно более предсказуемым и регулируемым. Похоже, что эра полной свободы и беззакония в сети «Интернет» закончилась. Закручивание гаек в глобальной сети было логичным ответом мирового сообщества на рост киберпреступности. Оптимистичным мечтам разработчиков главной среды коммуникаций не суждено было сбыться. Стремление создать свободное пространство для обмена научными идеями, межкультурного взаимодействия, безопасного творчества привело к катастрофе.

Глобальная сеть постепенно превратилась в пристанище преступников всех мастей, канал распространения асоциальных и античеловечных идей, место сбыта незаконных товаров. В Интернет также переместились военные действия между отдельными государствами.

# ЗОЛОТОЙ ВЕК ХАКЕРОВ

В наше время хакер воспринимается как однозначное зло, но в эпоху возникновения киберпреступности для многих это было неочевидно. Хакеры на заре своей истории стали настоящими суперзвездами. Они были безоговорочными лидерами мнений, у них брали интервью, на них хотела быть похожей молодежь. Фильмы, в основе которых была биография реальных киберпреступников, били рекорды по кассовым сборам в кинотеатрах. Хакеры основывали многомиллионные компании и задавали глобальные экономические тренды. В чем же причина такого феноменального успеха, и почему он сошел на нет?

Необходимо понимать, что само слово «хакер» появилось не для обозначения киберпреступников. Согласно самой распространенной версии словом «хак» (англ. — hack) стали обозначать свои ежегодные розыгрыши на «день дурака» (1 апреля) в легендарном Массачусетском институте технологий (МИТ)[27]. Эти розыгрыши зачастую требовали серьезных научных знаний и нетривиальных инженерных решений. Так, во время одного из розыгрышей студенты за ночь разместили копию полицейского автомобиля на крыше главного учебного здания университета[28]. В другой раз на вершине большого купола одного из зданий учебного заведения появилась корова

[27] A brief history of hacking, https://www.bbc.com/news/technology-13686141
[28] CP Car on the Great Dome, http://hacks.mit.edu/Hacks/by_year/1994/cp_car/