ГЛАВА 2

КОНЦЕПЦИИ, МЕТОДЫ И СРЕДСТВА ПРИМЕНЕНИЯ КИБЕРОРУЖИЯ

Детально рассмотрены концепции, средства, методы и примеры применения кибероружия, приведены научные обоснования, определения (термины) и классификация кибероружия и видов его воздействия на атакуемые объекты.

Кибервоздействия классифицированы по следующим категориям: по виду (одиночные и групповые), по типу (пассивные и активные), по характеру поражающих свойств (высокочастотные и комплексные), по цели использования (атакующие, оборонительные и обеспечивающие), по способу реализации (алгоритмические, программные, аппаратные, физические).

Рассмотрены и особенности многочисленных разновидностей каждого из вышеуказанных типов. Например, анализируются такие типы атакующих кибервоздействий, как «нарушение конфиденциальности информации», «нарушение целостности информации», «нарушение доступности информации», психологические воздействия. Из оборонительных разновидностей кибервоздействий рассматриваются «выявляющие», «противодействующие», «отвлекающие на ложные информационные ресурсы» и т.д.

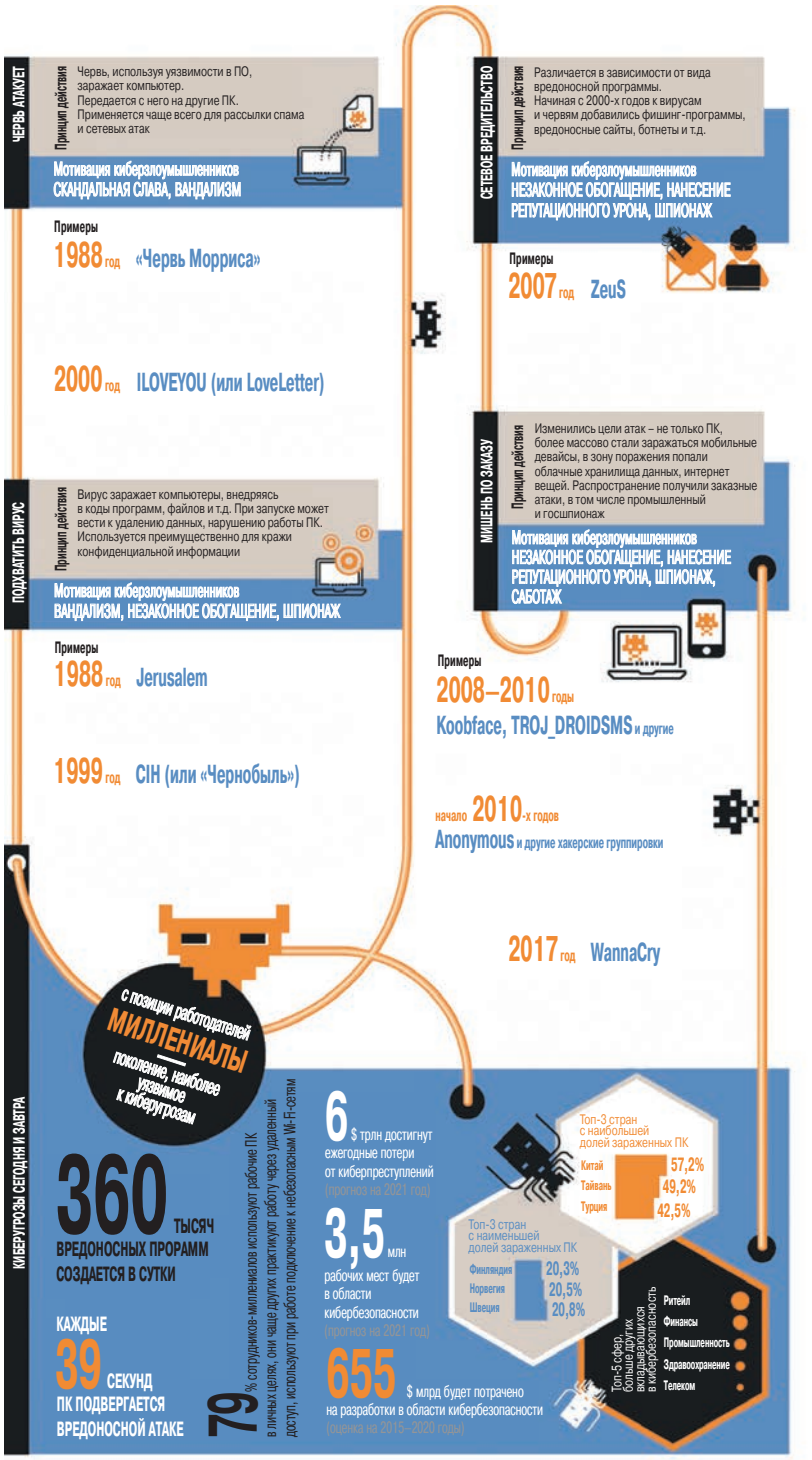
2.1. Краткая история развития кибероружия

2.1.1. Основные эпизоды из предыстории развития кибероружия

Об истории создания и развития кибероружия и его компонентов сегодня написано достаточно много статей и книг, в том числе наша «русскоязычная» двухтомная техническая энциклопедия по программным и аппаратным троянам [1] и «англоязычная» техническая энциклопедия-Handbook [2], эта тема постоянно и активно обсуждается в СМИ, поэтому здесь мы очень кратко перечислим только основные эпизоды хронологического пути развития этого «многоцелевого» и опасного оружия.

Если первые хакеры, разрабатывая свои экспериментальные программки, часто попросту желали бесплатно общаться по телефону или более детально разобраться с нюансами функционирования компьютерных сетей, то со временем цели и задачи компьютерных «взломщиков» становились все более опасными. В наши дни они могут реально угрожать безопасности людей и даже целых государств.

Прежде всего, следует отметить, что в жаргоне студентов Массачусетсского технологического института (МТИ) в конце 60-х годов словом «хакер» называли того, кто мог решить какую-либо сложную техническую задачу необычным, но эффективным способом. Считается, что термин происходит от английского глагола «to hack», ближайший аналог которого в русском языке – «справляться».



Источник: **Trend Micro, Accenture, Cisco, Cybersecurity Ventures, Microsoft, PwC, Symantec и др.**

Рис. 2.1. Цифровые твари и где они обитают [2]

И хотя до появления Интернета было еще далеко, это слово прижилось и сохранилось в лексиконе современных специалистов в области информационной безопасности.

На рис. 2.1 представлен в иллюстративном виде ход эволюции «цифровых тварей», как их часто называют журналисты.

В период 1970–1979 гг. наблюдалась настоящая эпидемия ***телефонного мошенничества***. Хакеры «докомпьютерной эры» называли себя «фрикерами» (каламбур от слов «phreak» и «phone»). Фрикеры взламывали телефонные сети в основном только для того, чтобы звонить бесплатно. Самым известным из фрикеров стал американец Джон Дрейпер по прозвищу «Капитан Кранч», который научился имитировать сигнал телефонной линии с помощью обычного игрушечного свистка.

Начало следующего десятилетия (1980–1989 гг.) характеризуется появлением первых ***компьютерных хакеров***. Так, 17-летний Кевин Митник из Лос-Анджелеса в 1980 году одним из первых «взломал» компьютерную сеть. Для начала он взломал локальную сеть в своей школе, а затем неоднократно проникал в сети различных телефонных компаний, чтобы получать конфиденциальную информацию о технологиях связи и совершенствовать свое мастерство. Вскоре Митника разоблачили, он несколько раз приговаривался к разным срокам заключения, но не оставил своего увлечения, хотя ему и было официально запрещено пользоваться не только компьютером, но и телефоном – это ограничение было снято только в 2003 году.

Считается, ***первым хакером в СССР*** был Мурат Уртембаев – программист, работавший на Волжском автозаводе. Взломав в 1983 г. систему подачи деталей на конвейер, он изменил ее настройки, что должно было дезорганизовать работу предприятия. Уртембаев планировал сразу же после фиксации факта сбоя самостоятельно его и устранить, чтобы получить за это премию. Но сбой произошел раньше, пока его создатель был в отпуске. В итоге после длительного расследования первому советскому хакеру дали условный срок «за хулиганство», обязали его возместить материальный ущерб и разжаловали в слесари. Хотя времена меняются, но даже сегодня одним из самых слабых звеньев в безопасности компании может стать сотрудник. Для того чтобы избежать возможных угроз, существуют специальные программы, например, Kaspersky Endpoint Security для бизнеса.

Появление термина ***«компьютерный вирус»*** относится к 1984 году, когда Фред Коэн, студент Университета Южной Калифорнии, написал программу, которая могла захватывать управление компьютером и создавать копии себя, заражая другие компьютеры в сети. Работу такой программы-вируса Коэн успешно продемонстрировал во время защиты своей докторской диссертации. Впоследствии Фред Коэн являлся одним из крупнейших специалистов по защите от компьютерных вирусов. Вопрос же о том, какую программу можно считать первым компьютерным вирусом, является спорным.

Первый ***сетевой червь*** был зафиксирован в 1988 году, когда аспирант Корнелльского университета (США) Роберт Моррис создал вредоносную программу, которая распространялась в сети Arpanet (прототип интернета). Червь поразил около шести тысяч компьютерных узлов, вызвав настоящую эпидемию. Попав на компьютер, программа многократно воспроизводила себя, что полностью парализовывало его работу. Любопытно, что это было всего лишь результатом ошибки – сам Моррис

такого эффекта не планировал. Ущерб в итоге составил около 96 миллионов долларов. Моррис был приговорен к трем годам условно, 10 тысячам долларов штрафа и 400 часам общественных работ.

Первый ***крупнейший взлом военных компьютеров*** был осуществлен в 1997 г. шотландцем Гэрри Маккинноном, который взломал военные компьютеры США, а несколькими годами позже – компьютеры NASA. Причиной взлома сам хакер назвал поиск спрятанной от гражданского общества информации об НЛО. Американцы добивались выдачи гражданина Великобритании в течение многих лет, однако в 2012 году получили окончательный отказ. В Штатах Гэрри грозило бы до 70 лет лишения свободы.

Первый ***вирус, повреждающий комплектующие компьютера***, был зафиксирован в 1999 г. Вирус CIH, также известный как «Чернобыль», был создан тайваньским студентом Чэнь Инхао. Вирус активизировался только в годовщину взрыва на Чернобыльской АЭС и поразил около полумиллиона компьютеров, удаляя данные, а часто еще и стирая содержимое флэш-памяти BIOS. Из-за этого зараженные компьютеры попросту переставали включаться. Раньше считалось, что вирусы на такое не способны.

Одна из первых зафиксированных крупных ***DoS-атак*** датируется 2000 г. Аббревиатура DoS происходит от английского denial of service – «отказ в обслуживании». Серверы, подвергающиеся атаке, получают одновременно множество запросов от компьютеров, зараженных злоумышленниками и, не выдерживая нагрузки, становятся недоступными для пользователей. В 2000 году одна из первых DoS-атак была совершена на сайты некоторых интернет-магазинов и веб-сервисов. Как выяснилось позже, атака была организована канадским подростком, известным как Mafiaboy. Злоумышленника приговорили к восьми месяцам тюрьмы. Ущерб от атаки составил, по разным оценкам, от 500 миллионов до 6 миллиардов долларов.

Первая серьезная ***атака на корневые DNS-сервера*** отмечена в октябре 2002 г., когда хакеры с помощью мощной DDoS-атаки попытались заблокировать все 13 корневых доменных серверов – в результате мог «сломаться» весь Интернет. Кто стоял за атакой, до сих пор осталось неизвестным.

Первый ***троянец для банкоматов*** был обнаружен в 2009 г. Тогда «Лаборатория Касперского» обнаруживает первую в истории троянскую программу, нацеленную на банкоматы, – Backdoor.Win32.Skimmer. Она ворует данные попадающих в устройство кредитных карт и умеет несанкционированно выдавать деньги.

Первое применение кибероружия, как считает большинство западных экспертов, относится к 2010 г., когда белорусским программистом Сергеем Усенем, к которому обратились за консультацией иранские эксперты по кибербезопасности, был обнаружен вирус Stuxnet. Уникальность этого вируса заключалась в том, что он был способен поражать и физически разрушать компоненты автоматизированных систем управления производственным оборудованием. Stuxnet был создан США и Израилем для заражения и разрушения компьютерной системы ядерной программы Ирана. Вирусу удалось нарушить работу более тысячи устройств для обогащения уранового топлива и сорвать ядерную программу Ирана. Более подробно особенности этой кибероперации, которая получила название «Олимпийские игры», мы рассмотрим в главе, посвященной вирусам и троянам.

Появление вируса Stuxent показало всему миру, что на смену «любителям», пишущим вирусы разных направлений, а потом и киберпреступникам, вымогающим или крадущим деньги, пришли «профессионалы», воспринимающие информационные системы исключительно как «поле боя».

В 2013 году были зафиксированы первые случаи атаки ***червя Carbanak***. В течение нескольких лет с его помощью было украдено около 1 миллиарда долларов. Жертвами стало около 100 финансовых организаций по всему миру, в том числе в СНГ. Одним из способов получения хакерами денег был удаленный контроль банкоматов. Сообщники подходили к ним в определенное время, а те просто выдавали наличные. В 2015 году в ходе совместного расследования «Лаборатория Касперского», Европол и Интерпол раскрыли беспрецедентную киберпреступную операцию. Ограбления продолжались два года и затронули около 100 финансовых организаций по всему миру. Лидера группировки задержали только в 2016 году.

В 2016 были зафиксированы и первые атаки на Интернет Вещей. Интернетом Вещей называют совокупность связанных между собой устройств, управляемых через Сеть, – самой различной домашней или офисной техники, которую в просторечии называют «умной». Хакеры атакуют и такие устройства, что может приводить к крайне неприятным последствиям: например, в 2016 году в Финляндии были взломаны «умные дома» – в результате в них отключили отопление. В том же году были зафиксированы атаки ботнета Mirai, образованного из сотен тысяч взломанных «умных» устройств. В результате одной из его атак «обрушился» целый сегмент Интернета, к примеру, были недоступны Twitter, Github, Soundcloud, Spotify и другие сервисы. Стоит ли говорить, какую опасность может повлечь взлом медицинской техники или «умных» кардиостимуляторов.

С появлением *биткоина* в 2017 году была зафиксирована ***эпидемия WannaCry***. Массовое распространение одного из самых известных червей началось в мае 2017. Считается, что за год с небольшим он заразил около полумиллиона компьютеров по всему миру. Используя уязвимость в операционной системе, WannaCry зашифровывает важные файлы пользователей и требует за них выкуп в биткоинах. Если оплата не поступает в течение 3 дней, сумма выкупа удваивается. А через неделю доступ к файлам пропадает навсегда. Экономический ущерб от эпидемии оценивается в 4 миллиарда долларов.

Особую угрозу действия «киберсолдат» представляют для инфраструктур современного *топливо-энергетического комплекса* – нефтяных и газовых транспортных систем, электростанций (особенно – для атомных станций).

Так, в 2015 г. «неизвестные злоумышленники» с использованием программы «Black Energy» перехватили управление украинскими энергосетями, отключив несколько областей. Информационно-управляющие системы операторов украинских энергосетей при этом были просто заблокированы: они наблюдали как зрители процесс отключения, но никак не могли ему помешать.

В апреле 2015 года в информационно-управляющей сети немецкой АЭС «Gundremmingen» были обнаружены вредоносные программы W32.Romanit и Conficker.

Надо отметить, что использование различного рода вредоносных программ сегодня становится все более простой задачей: «каркас» любой такой программы-вируса можно легко найти в Интернете и затем «начинять» его любым содержанием,

тем более что в Интернете полно подобных «криминальных сервисов», включая широкий спектр средств разработки вредоносных программ.

Так, в той же Германии в 2014 г. пятнадцатилетний подросток-школьник со своего домашнего компьютера подключился к микроконтроллерам центра управления тепловой электростанции, вызвав ее аварийную остановку.

Предприятия нефтяной и газовой индустрии также являются потенциальными объектами кибероружия. Так, в 2012 г. работа национальной нефтяной компании Саудовской Аравии Saudi Aramco была заблокирована на три недели вследствие атаки программы Shamoon, в 2016 году атаки были повторены.

За период с 2017 по 2019 г. как минимум семь «нефтепроводных» компаний («Energy Transter Partnes LP», «TransCanada Corp» и др.) официально объявляли о попытках повреждения (перехвата управления) как минимум трети своих информационно-коммуникационных сетей. Как сообщали в октябре 2019 г. российские СМИ, и «Газпром» не является здесь исключением из общего правила, – часть газоперекачивающих станций газотранспортной сети одновременно на некоторое время просто «отключились».

Надо понимать, что далеко не все подобные «киберинциденты» становятся известны широкой общественности – крупные компании не заинтересованы в разглашении фактов своей уязвимости в области обеспечения кибербезопасности.

Создателей подобных вирусов можно условно разделить на три большие группы.

Первые «зарабатывают» тем, что воруют деньги с банковских счетов, вымогают или крадут и продают аккаунты.

Вторые специализируются на целевых атаках и пишут особые вредоносные программы, позволяющие незаметно проникать в конкретную защищенную систему.

Третью группу представляют так называемые киберсолдаты, которые в основном финансируются государственными структурами.

С появлением *криптовалют*, соответственно, появились и новые вредоносные программы и вирусы. Их можно разделить на две большие группы:

Программы-майнеры (криптомайнеры), которые заставляют атакуемый компьютер производить (зарабатывать) для злоумышленников криптовалюту, и ***программы цифровальщики***, несанкционированно кодирующие информацию на атакуемом компьютере и затем вымогающие криптовалюту (биткоины) за ее расшифровку (Petya, WannaCry и Bad Rabbit).

Напомним, что *майнинг – это процесс добычи криптовалюты посредством организации сложных вычислений, которые выполняются непосредственно на вашем (или чужом) компьютере*. На сегодня известны две разновидности «зловредного майнинга». В первом случае программа-майнер скрытно от вас устанавливается на ваш компьютер и начинает постоянно использовать его вычислительные мощности – процессор и видеокарту. Во втором случае майнинг выполняется только тогда, когда вы заходите на «зараженный» сайт (браузер-майнинг).

Первый случай для злоумышленника предпочтительнее, но и более сложный, ведь компьютер надо как-то «заразить». Второй – проще, здесь нужную мощность ресурсов злоумышленник «добирает» за счет большого количества пользователей заходящих на эти сайты.

2.1.2. Изменение видов киберугроз за период с 1980 по 2010 г.

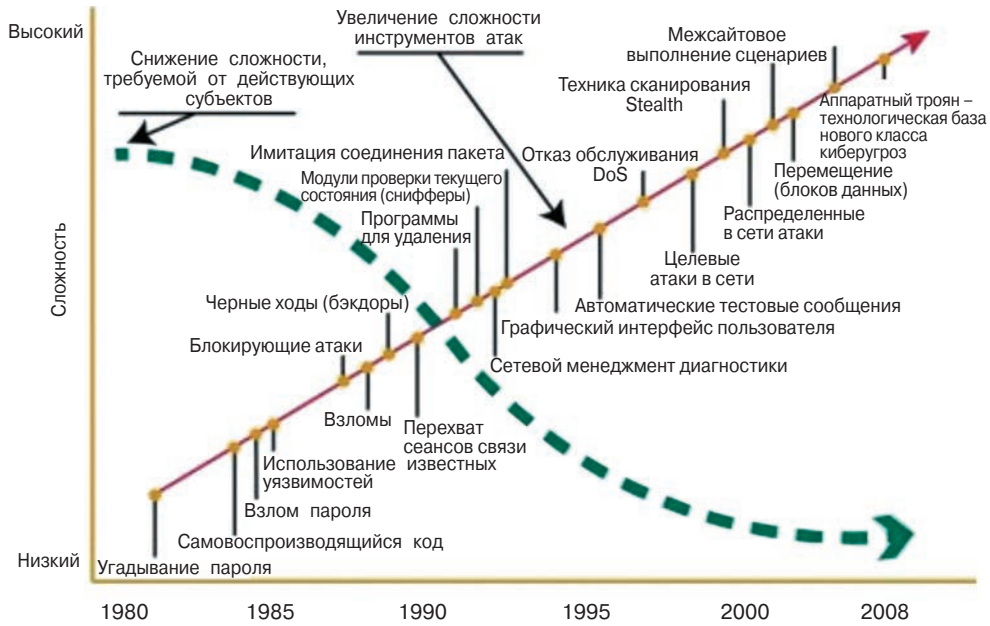


Рис. 2.2. Динамика роста угрозы кибератак в период с 1980 по 2010 г.

На этом рисунке представлены основные тенденции развития всякого рода угроз для современного так называемого информационного общества и «цифровой экономики». Здесь анализируемый автором [3] период времени относится к 2000–2010 гг. Поскольку этот рисунок имеет в основном не технический, а демонстративно-иллюстративный характер, по вертикальной оси «Y» «рост угроз» показан рост с течением времени уровня сложности и относительной частоты наблюдений различного рода атак на существующие сетевые и локальные системы управления банков, системы управления промышленными производствами, каналы передачи данных, социальных сетей и т.д.

Конечно, подобная *визуализация* этого процесса носит весьма условный характер. На этом достаточно примитивном рисунке аналитик попытался представить графическое решение задачи определения взаимосвязи между уровнем безопасности современных информационных и телекоммуникационных устройств и перечнем различного вида изощренных атак, предпринимаемыми различными злоумышленниками почти за тридцатилетний период наблюдения, точнее – за период с 1980 по 2010 г.

Если в начале этой криминальной эпохи простейшие атаки хакеров начинались с простого «угадывания» паролей, затем «взлома паролей», то буквально через пару лет они перешли к вообще немыслимому в то время процессу – «перехват сеансов связи», внедрения в сетевой менеджмент стандартной (как считалось пользователями) диагностики, затем появилась генерация злоумышленных автоматических текстовых сообщений, а потом – целевые и распределенные атаки в социальных сетях и т.п.