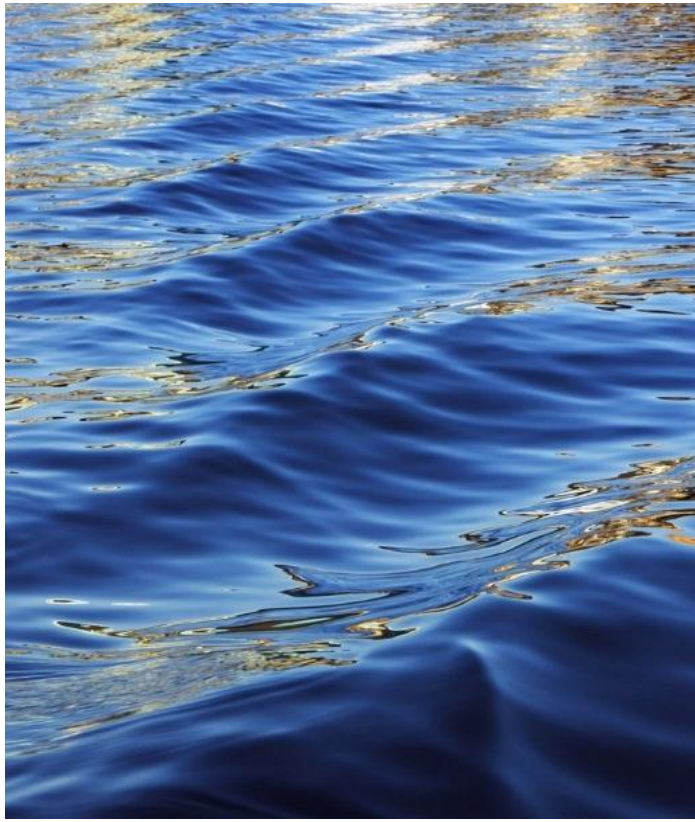
Вирусы и средства борьбы с ними

Информатика для СПО



Понятие вируса

Основная отличительная характеристика компьютерного вируса — способность к самораспространению. Подобно биологическому вирусу для жизни и размножения он активно использует внешнюю среду - память компьютера, операционную систему.

Увеличение скорости передачи информации, объемов и значимости обрабатываемых в вычислительных сетях данных открывает перед вирусописателями все более широкие возможности - распространение по всему миру написанных программ занимает считанные дни или даже часы. Сотни мегабайт оперативной памяти позволяют выполнять практически любые действия незаметно от пользователя. Спектр возможных целей, таких как пароли, карточные счета, ресурсы удаленных компьютеров представляет огромное поле для деятельности. Усложнение операционных систем ведет к появлению все новых дыр, которые могут быть использованы для проникновения на удаленный компьютер.

Понятие вируса

Однако изначально компьютерные вирусы были придуманы с совершенно иной целью.

История начинается в 1983 году, когда американский ученый Фред Коэн (Fred Cohen) в своей диссертационной работе), посвященной исследованию самовоспроизводящихся компьютерных программ впервые ввел термин компьютерный вирус. Известна даже точная дата - 3 ноября 1983 года, когда на еженедельном семинаре по компьютерной безопасности в Университете Южной Калифорнии (США) был предложен проект по созданию самораспространяющейся программы, которую тут же окрестили вирусом. Для ее отладки потребовалось 8 часов компьютерного времени на машине VAX 11/750 под управлением операционной системы Unix и ровно через неделю, 10 ноября состоялась первая демонстрация. Фредом Коэном по результатам этих исследований была опубликована работа "Computer Viruses: theory and experiments"2) с подробным описанием проблемы.

Понятие вируса

Теоретические же основы самораспространяющихся программ были заложены в 40-х годах прошлого столетия в трудах по изучению самовоспроизводящихся математических автоматов американского ученого Джона фон Неймана (John von Neumann), который также известен как автор базовых принципов работы современного компьютера. В 1951 году фон Нейманом был разработан метод, который демонстрировал возможность создания таких автоматов, а в 1959 журнал "Scientific American" опубликовал статью Л. С. Пенроуза (L. S. Penrose) "Self-Reproducing Machines", посвященную самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее, по следам этой статьи другой ученый Ф. Ж. Шталь (F. G. Stahl) реализовал модель на практике с помощью машинного кода на IBM 650.

Понятие вируса

Первые самораспространяющиеся программы не были вредоносными в понимаемом ныне смысле. Это были скорее программы-шутки либо последствия ошибок в программном коде, написанном в исследовательских целях. Сложно представить, что они были созданы с какой-то конкретной вредоносной целью.

Первые вирусы

Pervading Animal (конец 60-х - начало 70-х) — так назывался первый известный вирус-игра для машины Univac 1108. С помощью наводящих вопросов программа пыталась определить имя животного, задуманного играющим. Благодаря наличию функции добавления новых вопросов, когда модифицированная игра записывалась поверх старой версии плюс копировалась в другие директории, через некоторое время диск становился переполненным.

Первый сетевой вирус Creeper появился в начале 70-х в военной компьютерной сети Arpanet3), прототипе Интернет. Программа была в состоянии самостоятельно выйти в сеть через модем и сохранить свою копию на удаленной машине. На зараженных системах вирус обнаруживал себя сообщением: "I'M THE CREEPER : CATCH ME IF YOU CAN". Для удаления назойливого, но в целом безобидного вируса неизвестным была создана программа Reaper. По сути это был вирус, выполнявший некоторые функции, свойственные антивирусу: он распространялся по вычислительной сети и в случае обнаружения тела вируса Creeper уничтожал его.

Первые вирусные эпидемии

Возможности первых вирусов были сильно ограничены малой функциональностью существующих на тот момент вычислительных машин. Только в конце семидесятых, вслед за выпуском нового поколения персональных компьютеров Apple (Apple II) и впоследствии IBM Personal Computer (1981 год), стали возможны вирусные эпидемии. Появление BBS (Bulletin Board System) обеспечило быстрый обмен информацией между даже самыми отдаленными точками планеты.

Elk Cloner (1981 год) изначально использовал для распространения пиратских копий компьютерных игр.

Первые вирусные эпидемии

Поскольку жестких дисков тогда еще не было, он записывался в загрузочные сектора дискет и проявлял себя переворачиванием изображения на экране и выводом текста:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

IT WILL INFILTRATE YOUR CHIPS

YES, IT'S CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!

Первые вирусные эпидемии

Brain (1986 год) — первый вирус для IBM-совместимых компьютеров, вызвавший глобальную эпидемию. Он был написан двумя братьями-программистами Баситом Фарук и Амжадом Алви (Basit Farooq Alvi и Amjad Alvi) из Пакистана с целью определения уровня пиратства у себя в стране: вирус заражал загрузочные сектора, менял метку диска на "(c) Brain" и оставлял сообщение с именами, адресом и телефоном авторов. Отличительной чертой его была функция подмены в момент обращения к нему зараженного сектора незараженным оригиналом. Это дает право назвать Brain первым известным стелс-вирусом. В течение нескольких месяцев программа вышла за пределы Пакистана и к лету 1987 года эпидемия достигла глобальных масштабов. Ничего деструктивного вирус не делал.

Первые вирусные эпидемии

В этом же году произошло еще одно знаменательное событие. Немецкий программист Ральф Бюргер (Ralf Burger) открыл возможность создания программой своих копий путем добавления своего кода к выполняемым DOS-файлам формата COM. Опытный образец программы, получившей название Virdem, был продемонстрирован на форуме компьютерного андеграунда - Chaos Computer Club (декабрь 1986 года, Гамбург, ФРГ). По результатами исследований Бюргер выпустил книгу "Computer Viruses. The Disease of High Technologies", послужившую толчком к написанию тысяч компьютерных вирусов, частично или полностью использовавших описанные автором идеи.

Первые вирусные эпидемии

Lehigh (1987 год) — первый по-настоящему вредоносный вирус, вызвавший эпидемию в Лехайском университете (США), где в то время работал Фред Коэн. Он заражал только системные файлы COMMAND.COM и был запрограммирован на удаление всей информации на текущем диске. В течение нескольких дней было уничтожено содержимое сотен дискет из библиотеки университета и личных дискет студентов. Всего за время эпидемии было заражено около четырех тысяч компьютеров. Однако за пределы университета Lehigh не вышел.

Семейство резидентных файловых вирусов Suriv (1987 год) — творение неизвестного программиста из Израиля. Самая известная модификация, Jerusalem, стала причиной глобальной вирусной эпидемии, первой настоящей пандемией, вызванной MS-DOS-вирусом.

Первые вирусные эпидемии

Действие вирусов Suriv сводилось к загрузке кода в память компьютера, перехватывании файловых операций и заражении запускаемых пользователем COM- и/или EXE-файлов. Это обстоятельство обеспечивало практически мгновенное распространение вируса по мобильным носителям. Jerusalem отличался от своих предшественников дополнительной деструктивной функцией - уничтожением всех запускаемых программ в пятницу, 13. Такой черной датой стало 13 мая 1988 года, когда в одночасье перестали работать компьютеры многих коммерческих фирм, государственных организаций и учебных заведений, в первую очередь Америки, Европы и Ближнего Востока.

Первые вирусные эпидемии

Примечательно, что в том же 1988 году известный программист Питер Нортон (Peter Norton) высказался резко против существования вирусов. Он официально объявил их несуществующим мифом и сравнил со сказками о крокодилах, живущих в канализации Нью-Йорка. Это показывает сколь низка была культура антивирусной безопасности в то время.

Mike RoChenle — псевдоним автора первой известной вирусной мистификации. В октябре 1988 года он разослал на станции BBS большое количество сообщений о вирусе, который передается от модема к модему со скоростью 2400 бит/с. В качестве панацеи предлагалось перейти на использование модемов со скоростью 1200 бит/с. Как это ни смешно, многие пользователи действительно последовали этому совету.

Первые вирусные эпидемии

Червь Морриса (ноябрь 1988) — с ним связана первая эпидемия, вызванная сетевым червем. 60000-байтная программа, написанная 23-летним студентом Корнельского университета (США) Робертом Моррисом, использовала ошибки в системе безопасности операционной системы Unix для платформ VAX и Sun Microsystems. С целью незаметного проникновения в вычислительные системы, связанные с сетью Arpanet, использовался подбор паролей (из списка, содержащего 481 вариант). Это позволяло маскироваться под задачу легальных пользователей системы. Однако из-за ошибок в коде безвредная по замыслу программа неограниченно рассылала свои копии по другим компьютерам сети, запускала их на выполнение и таким образом забирала под себя все сетевые ресурсы.

Первые вирусные эпидемии

Червь Морриса заразил по разным оценкам от 6000 до 9000 компьютеров в США (включая Исследовательский центр NASA) и практически парализовал их работу на срок до пяти суток. Общие убытки были оценены в минимум 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 96 миллионов долларов. Ущерб был бы гораздо больше, если бы червь изначально создавался с разрушительными целями.

4 мая 1990 года впервые в истории состоялся суд над автором компьютерного вируса, который приговорил Роберта Морриса к 3 годам условно, 400 часам общественных работ и штрафу в 10 тысяч долларов США.

Первые вирусные эпидемии

Эпидемия червя Морриса стала причиной создания организации CERT (Computer Emergency Response Team), в функции которой входит оказание содействия пользователям в предотвращении и расследовании компьютерных инцидентов, имеющих отношение к информационным ресурсам. На сайте этой организации (http://www.cert.org) оперативно публикуются самые последние сведения о новых вредоносных программах, обнаруженных уязвимостях в ПО, методах защиты корпоративных сетей, аналитические статьи, а также результаты различных исследований в области компьютерной безопасности.

Первые вирусные эпидемии

Datacrime (1989) — вирус, который несмотря на сравнительно небольшое распространение, вызвал повальную истерию в мировых средствах массовой информации. Он отличался тем, что с 13 октября по 31 декабря инициировал низкоуровневое форматирование нулевого цилиндра жесткого диска, что приводило к уничтожению таблицы размещения файлов (FAT) и безвозвратной потере данных.

В ответ корпорация IBM выпустила (4 октября 1989 года) коммерческий антивирус Virscan для MS-DOS, позволяющий искать характерные для ряда известных вирусов строки в файловой системе. Стоимость программы составила всего 35 долларов США.

Первые вирусные эпидемии

Aids Information Diskette (декабрь 1989) — первая эпидемия троянской программы. Ее автор разослал около 20000 дискет с вирусом по адресам в Европе, Африке и Австралии, похищенным из баз данных Организации всемирного здравоохранения и журнала PC Business World. После запуска вредоносная программа автоматически внедрялась в систему, создавала свои собственные скрытые файлы и директории и модифицировала системные файлы. Через 90 загрузок операционной системы все файлы на диске становились недоступными, кроме одного - с сообщением, предлагавшим прислать $189 на указанный адрес. Автор троянца, Джозеф Попп (Joseph Popp), признанный позднее невменяемым, был задержан в момент обналичивания чека и осужден за вымогательство. Фактически, Aids Information Diskette - это первый и единственный вирус, для массовой рассылки использовавший настоящую почту.

Первые вирусные эпидемии

Cascade (1989) — резидентный зашифрованный вирус, вызывающий характерный видеоэффект - осыпание букв на экране. Примечателен тем, что послужил толчком для профессиональной переориентации Евгения Касперского на создание программ-антивирусов, будучи обнаруженным на его рабочем компьютере. Уже через месяц второй инцидент (вирус Vacsina) был закрыт при помощи первой версии антивируса — V, который несколькими годами позже был переименован в AVP — AntiViral Toolkit Pro

Первые вирусные эпидемии

Eddie (также известен как Dark Avenger, 1989 год) — первый вирус, противодействующий антивирусному программному обеспечению: он заражает новые файлы, пока антивирус проверяет жесткий диск компьютера. Это достигалось применением особой технологии, позволяющей заражать не только COM/EXE- программы в момент их запуска, но и любые файлы при попытке прочтения.

Первые антивирусные утилиты

Первые антивирусные утилиты (1984 год) были написаны Анди Хопкинсом (Andy Hopkins). Программы CHK4BOMB и BOMBSQAD позволяли производить анализ загрузочного модуля с помощью контекстного поиска и перехватывать операции записи и форматирования, выполняемые через BIOS. На то время они были очень эффективны и быстро завоевали популярность.

Первые антивирусные утилиты

Dr. Solomon's Anti-Virus Toolkit (1988) — первая широко известная антивирусная программа. Созданная английским программистом Аланом Соломоном (Alan Solomon), она завоевала огромную популярность и просуществовала до 1998 года, когда компания Dr. Solomon была поглощена другим производителем антивирусов - американской Network Associates (NAI).

Первые антивирусные утилиты

Кроме официального переименования Arpanet в Интернет, следующий год ознаменовался выходом в свет первого номера Virus Bulletin (июль 1989) — самого популярного на сегодняшний день издания, содержащего последние новости в сфере вирусных и антивирусных технологий: подробную информацию о новых вредоносных программах, методах защиты от вирусов и устранения последствий заражения. Основателями журнала выступили руководители английской антивирусной компании Sophos Ян Храске (Jan Hruska), Питер Лэммер (Peter Lammer) и Эд Уайлдинг (Ed Wilding). Впоследствии редакция Virus Bulletin (1991) начала проводить ежегодные конференции для антивирусных экспертов, где корпоративные заказчики имеют возможность напрямую общаться с ведущими специалистами в этой области. В январе 1998 года была учреждена награда VB 100%, присуждаемая антивирусным программам по результатам проводимого редакцией Virus Bulletin тестирования. Количество наград VB 100%, полученных в результате тестирования сегодня зачастую является одним из основных критериев в выборе средств антивирусной защиты.

Первые антивирусные утилиты

В качестве ответа через пару месяцев Dr. Solomon's запустила свой собственный издательский проект - Virus Fax International, впоследствии переименованный в Secure Computing. Сегодня этот журнал является одним из наиболее популярных изданий в области защиты информации, специализируясь на анализе не только антивирусных программ, но также всего спектра программных и аппаратных средств, применяемых для обеспечения компьютерной безопасности.

1990 — 1998

Начиная с 1990 года проблема вирусов окончательно утрачивает связь с научными кругами и становится достоянием рядовых программистов, преследующих личные цели.

В Болгарии открывается первая BBS (VX BBS), ориентированная на обмен вирусами и информацией для вирусописателей. Чуть позже начинают появляться конференции Usenet по вопросам написания вирусов.

Chameleon (начало 1990 года) — первый полиморфный вирус. Его автор, Марк Уошбурн (Mark Washburn) за основу для написания программы взял сведения о вирусе Vienna из книги Ральфа Бюргера "Computer Viruses. The Disease of High Technologies" и добавил к ним усовершенствованные принципы самошифрации вируса Cascade - свойство изменять внешний вид как тела вируса, так и самого расшифровщика. Только в 1992 году был изобретен достаточно эффективный способ нейтрализации полиморфных вирусов - эмулятор процессора для дешифрации кодов. Эта технология является неотъемлемым атрибутом каждого современного антивирусного продукта.

DiskKiller (январь 1989 года — июль 1990 года) — этим вирусом была заражена дискета бесплатного приложения к английскому компьютерному журналу PC Today. В июле 1990 года подписчикам разошлось около 50000 экземпляров. Действие DiskKiller сводилось к уничтожению всей информации на жестком диске.

В это же время впервые были обнаружены и первые российские вирусы — Peterburg, Voronezh и ростовский LoveChild.

1990 — 1998

EICAR (European Institute for Computer Anti-virus Research) — в декабре 1990 года в Гамбурге (Германия) был основан Европейский институт компьютерных антивирусных исследований. Заплатив организационный взнос, его членом может стать любой человек, государственная или частная структура и в течение срока подписки получать оперативную информацию о ситуации в области антивирусной защиты и компьютерной безопасности в целом, а также консультации известных специалистов. Широкому кругу пользователей эта организация известна по созданному ею файлу **eicar.com**, который детектируется всеми известными антивирусными программами как вирус - например, с именем EICAR-Test-File. Однако никакого вреда он не приносит и служит лишь как средство проверки работоспособности антивируса. Загрузить eicar.com можно с eicar.org или же написать лично, следуя рекомендациям, размещенным на этом сайте. Несмотря на громкое заявление Питера Нортона, прозвучавшее двумя годами ранее и где он авторитетно заявлял о надуманности проблемы вирусов, в конце 1990 года вышла первая версия антивирусной программы Norton AntiVirus.

Dir_II (лето 1991 года) — вирус, использовавший принципиально новый способ заражения — link-технологию. На сегодняшний день он остается единственным представителем этого класса, который был обнаружен в диком виде.

MtE (MuTation Engine, 1991 год) — первый известный полиморфик-генератор. Его главное предназначение — возможность интеграции в другие вирусы для обеспечения их полиморфизма. MtE поставлялся в виде готового объектного модуля и сопровождался подробной документацией.

Годом позднее, в июле 1992 года появился первый **конструктор вирусов VCL** (Virus Creation Laboratory), представляющий собой графическую среду для разработки вирусов и различных троянских программ для MS DOS. Начиная с этого момента, любой человек мог легко сформировать и написать вирус.

1990 — 1998

Win.Vir (конец 1992 года) — первый вирус, поражающий исполняемые файлы Microsoft Windows 3.1. Эпидемии не вызвал и его появление осталось практически незаметным. Однако именно Win.Vir положил начало эпохи вирусов для Windows.

Далее события начинают развиваться с невероятной скоростью.

Shifter (январь 1994) — первый вирус, заражающий объектные модули (OBJ-файлы).

SrcVir (апрель 1994) — семейство вирусов, заражающих исходные тексты программ (C и Pascal).

1990 — 1998

OneHalf (июнь 1994) — очень сложный резидентный файлово-загрузочный полиморфный вирус, вызвавший глобальную эпидемию во всем мире, в том числе в России. OneHalf заражал загрузочные сектора дисков и COM/EXE-файлы, увеличивая их размер на 3544, 3577 или 3518 байта, в зависимости от модификации. При каждой перезагрузке зараженного компьютера зашифровывались два последних незашифрованных ранее цилиндра жесткого диска. Это продолжалось до тех пор, пока весь винчестер не оказывался зашифрованным. Встроенная стелс-процедура позволяла вирусу при запросе зашифрованной информации производить расшифровку на лету - следовательно, пользователь долгое время пребывал в неведении. Единственным визуальным проявлением вируса было сообщение "Dis is one half. Press any key to continue...", выводившееся в момент достижения количеством зашифрованных цилиндров диска половины от их общего числа. Однако при первой же попытке лечения, после вылечивания загрузочных секторов диска, вся информация на винчестере становилась недоступной, без возможности восстановления. Популярности этого вируса в России поспособствовала компания Доктор Веб, которая выпустила новую версию своего антивируса, анонсировав его как средство от OneHalf. Однако на практике после лечения загрузочных секторов от этого вируса, Dr.Web забывал расшифровать информацию на диске и восстановить ее было уже невозможно.

1990 — 1998

Следующий год запомнился инцидентом в корпорации Microsoft. В феврале 1995 года, в преддверии выпуска новой операционной системы Windows 95 была разослана демонстрационная дискета, зараженная загрузочным вирусом Form. Копии этого диска получили 160 бета-тестеров, один из которых не поленился провести антивирусную проверку.

Вслед за Microsoft отличились журналы PC Magazine (английская редакция) и Computer Life, которые разослали своим подписчикам дискеты, зараженные загрузочными вирусами Sampo и Parity_Boot соответственно.

1990 — 1998

Concept (август 1995) — первый макровирус, поражавший документы Microsoft Word.

Green Stripe (1995) — первый вирус для AmiPro, популярного в то время текстового редактора. Исходный код Green Stripe был бесплатным приложением к полуподпольному изданию Марка Людвига (Mark Ludwig) "Underground Technology Review".

15 ноября 1995 года Кристофер Пайл (Christopher Pile), известный под псевдонимом Black Baron, автор вирусов Queeg и Pathogen и полиморфик-генератора SMEG был приговорен к 18 месяцам тюремного заключения.

1990 — 1998

Boza (январь 1996) — первый вирус для операционной системы Microsoft Windows 95.

Win.Tentacle (март 1996) — вызвал первую эпидемию среди пользователей Microsoft Windows 3.x.

Wazzu — вирус, ставший причиной очередного вирусного инцидента в Microsoft. Он был обнаружен в одном из документов Word на веб-сайте корпорации. Позднее Wazzu был найден также на компакт-дисках, распространенных Microsoft на выставке компьютерных технологий Orbit (г. Базель, Швейцария), а в сентябре - на компакт-дисках Microsoft Solution Provider.

1990 — 1998

Win95.Punch (декабрь 1996) — первый резидентный вирус для Windows 95. Он загружался в систему как VxD-драйвер, перехватывал обращения к файлам и заражал их.

Linux.Bliss (февраль 1997) — первый вирус для операционной системы Linux.

ShareFun (март 1997) — первый макро-вирус для MS Word 6/7, использующий для своего распространения возможности электронной почты, в частности, почтовую программу MS Mail.

Homer (апрель 1997) — первый сетевой вирус-червь, использующий протокол передачи данных File Transfer Protocol (FTP).

В декабре 1997 года, вскоре после разработки технологии IRC (Internet Relay Chat), образовался новый класс вредоносных программ — IRC-черви.

1990 — 1998

Win95.HPS и Win95.Marburg (февраль 1998) — первые полиморфные Windows32-вирусы. Marburg известен также тем, что им были заражены компакт-диски, сопровождавшие английскую, словенскую, шведскую и итальянскую редакции журнала PC Gamer.

В июне 1998 года был обнаружен вирус тайваньского происхождения Win95.CIH, содержащий логическую бомбу на уничтожение всей информации на жестких дисках и порчу содержимого BIOS на некоторых материнских платах. Дата срабатывания программы (26 апреля) совпадала с датой аварии на Чернобыльской атомной электростанции, вследствие чего вирус получил второе имя — Чернобыль (Chernobyl). Масштабность эпидемии выяснилась 26 апреля 1999 года, когда по различным оценкам пострадало около полумиллиона компьютеров по всему миру, а общий ущерб составил сотни миллионов долларов США. Центром эпидемии стала Южная Корея, где было заражено более 300 тысяч компьютеров. В России Win95.CIH поразил не менее 100 тысяч машин.

1990 — 1998

BackOrifice, Backdoor.BO (август 1998) — первая известная утилита скрытого администрирования удаленных компьютеров. Единственное отличие этого трояна от обычных программ для удаленного управления - несанкционированная установка и запуск. Действие утилиты сводилось к скрытому слежению за системой: ссылка на троянца отсутствовала в списке активных приложений, но при этом зараженный компьютер был открыт для удаленного доступа. Фактически, открывался свободный вход на зараженные компьютеры для других вредоносных программ - впоследствии возник целый класс червей, размножение которых базировалось на оставленных BackOrifice дырах.

Во второй половине 1998 года вирусы активно начинают осваивать новые технологии: Java.StangeBrew — первый вирус, который заражал выполняемые модули Java, VBScript.Rabbit — скрипты Visual Basic (VBS-файлы), HTML.Internal — первый HTML-вирус.

1999 — 2000

Следующий период вирусной истории прошел под знаменем массовых рассылок по электронной почте.

Happy99 (также известный как Ska, январь 1999 года) — первый интернет-червь, использовавший для своего распространения программу MS Outlook.

26 марта 1999 года началась глобальная эпидемия вируса Melissa — первого макро-вируса для MS Word, сочетавшего в себе также и функциональность интернет-червя. Сразу же после заражения системы он считывал адресную книгу почтовой программы MS Outlook и рассылал по первым 50 найденным адресам свои копии. Подобно Happy99 вирус Melissa делал это абсолютно незаметно для пользователя и, что самое страшное, от его имени. Microsoft, Intel, Lockheed Martin были вынуждены временно отключить свои корпоративные службы электронной почты. По разным оценкам совокупный ущерб от вируса варьировался от нескольких миллионов до десятков миллионов долларов США.

Через некоторое время был обнаружен и арестован автор вируса Melissa, Дэвид Л. Смит (David L. Smith). 9 декабря он был признан виновным и осужден на 10 лет тюремного заключения и к штрафу в размере 400000 долларов США.

1999 — 2000

ZippedFiles (также известный как ExploreZip, июнь 1999 года) — первый упакованный интернет-червь. Его тело было упаковано утилитой сжатия Neolite, обращаться с которой в то время антивирусные продукты не умели, что привело к эпидемии.

Bubbleboy (ноябрь 1999) — первый вирус из поколения червей-невидимок, распространявшихся по электронной почте без использования вложенных файлов и проникавших на компьютеры сразу же после прочтения зараженного письма. Все вирусы этого типа используют различные уязвимости в системе безопасности Internet Explorer.

Babylonia (декабрь 1999) — первый вирус-червь, который имел функции удаленного самообновления: он ежеминутно пытался соединиться с сервером, находящемся в Японии и загрузить оттуда список вирусных модулей.

LoveLetter — скрипт-вирус, 5 мая 2000 года побивший рекорд вируса Melissa по скорости распространения. Всего в течение нескольких часов были поражены миллионы компьютеров - LoveLetter попал в Книгу Рекордов Гиннеса. Успех гарантировали методы социальной инженерии: электронное сообщение имело тему "I love you" и интригующий текст, призывающий открыть вложенный файл с вирусом.

1999 — 2000

Liberty (август 2000) — первая вредоносная программа класса троянский конь для операционной системы PalmOS карманных компьютеров Palm Pilot.

Stream (сентябрь 2000) — первый известный вирус, способный манипулировать дополнительными потоками (ADS) файловой системы NTFS.

Pirus (октябрь 2000) — первый вирус, написанный на скрипт-языке PHP.

Fable (октябрь 2000) — первый вирус, скрывающийся в информационных файлах PIF.

Hybris (ноябрь 2000) — опасный и технологически совершенный вирус, главным нововведением которого было использование как веб-сайтов, так и электронных конференций (в частности alt.comp.virus) для загрузки новых модулей вируса на зараженные компьютеры. Кроме того, для идентификации настоящих вирусных модулей, т. е. действительно выпущенных автором, Hybris использовал 128-битный электронный ключ RSA для их шифрования

2001 — 2005

Самые известные вирусы этой эпохи, такие как CodeRed или Nimda, продемонстрировали сочетание способности к практически мгновенному распространению и существенно усложненную, многоуровневую структуру. Фактически, можно выделить такие тенденции: расширение спектра путей и методов проникновения, использование новых платформ и технологий, обновление вирусных кодов через Интернет, новые вредоносные функции и активное противодействие антивирусным программам.

Ramen (январь 2001) — вирус, за считанные дни поразивший большое количество крупных корпоративных систем на базе операционной системы Linux.

Sadmind (май 2001) — первый известный интернет-червь, заражающий компьютеры Sun Sparc с операционной системой Solaris/SunOS. Для размножения использовалась брешь в службе системного администрирования /usr/sbin/sadmind. Червь также атаковал HTTP-серверы с установленным Microsoft Internet Information Server (IIS).

2001 — 2005

CodeRed (12 июля 2001 года) — представитель нового типа вредоносных кодов, способных активно распространяться и работать на зараженных компьютерах без использования файлов. В процессе работы такие программы существуют исключительно в системной памяти, а при передаче на другие компьютеры - в виде специальных пакетов данных. Для проникновения на удаленные компьютеры CodeRed использовал брешь в системе безопасности IIS, которая позволяет злоумышленникам запускать на удаленных серверах посторонний программный код. 18 июня 2001 года Microsoft выпустила соответствующую заплатку, однако подавляющее большинство пользователей не успело вовремя обновить свое программное обеспечение.

CodeRed вызвал эпидемию, заразив около 12000 (по другим данным - до 200000) серверов по всему миру и провел крупномасштабную DDoS1) атаку на веб-сервер Белого дома, вызвав нарушение его нормальной работы.

Через неделю, 19 июля появилась новая модификация CodeRed, показавшая чудеса распространения - более 350000 машин за 14 часов (до 2000 компьютеров в минуту). Однако по замыслу автора 20 июля вирус прекратил свое распространение.

2001 — 2005

Следующая версия, CodeRed.c (CodeRed II) была обнаружена 4 августа 2001 года. После заражения (использовалась все та же брешь в системе безопасности IIS) вирус ничем не выдавал свое присутствие один-два дня, после чего перезагружал компьютер и начинал активные попытки распространения, продолжавшиеся 24 часа (или 48, в случае использования китайской раскладки). Червь также устанавливал троянскую программу explorer.exe и использовал встроенную бекдор-процедуру (Backdoor).

В это же время был обнаружен почтовый червь Sircam (12 июля 2001 года). Этот вирус отличала необычная процедура выбора имени зараженного вложения. Для этого случайным образом на диске выбирался документ, к имени которого добавлялось расширение .pif, .lnk, .bat или .com. Полученная конструкция вида mydiary.doc.com служила темой рассылаемых писем и именем новой копии программы: к отобранному файлу и дописывался код червя - таким образом Sircam мог привести к утечке конфиденциальной информации. При рассылке использовался собственный SMTP-клиент, в поле От указывался один из адресов, найденных на зараженном компьютере, а сообщение содержало текст вида "Hi! How are you? I send you this file in order to have your advice. See you later. Thanks." Кроме этого, в определенный момент времени (в зависимости от системного времени и модификации вируса) на зараженном компьютере удалялись все файлы на системном диске.

2001 — 2005

Nimda (18 сентября 2001 года) — вирус-червь, в течение 12 часов поразивший до 450000 компьютеров. Для распространения были задействованы пять методов: электронная почта (брешь в системе безопасности Internet Explorer, позволяющая автоматически выполнять вложенный исполняемый файл), по локальной сети, внедрение на IIS-серверы, заражение браузеров через javascript, а также с помощью бекдор-процедур, оставленных CodeRed.c и Sadmind. После заражения Nimda добавлял в группу Администраторы пользователя под именем Guest и открывал локальные диски на полный доступ для всех желающих.

Klez (октябрь 2001) — почтовый червь, модификации которого на протяжении следующих нескольких лет занимали первые строки в рейтингах популярности. Программа проникала на компьютер по сети или через электронную почту, используя брешь в защите IFrame браузера Internet Explorer, которая допускала автоматический запуск вложенного файла. Также вирус имел встроенную функцию поиска и подавления антивирусного программного обеспечения. Klez дописывал свой код к одному из документов на зараженной машине и начинал массовую рассылку. В поле От подставлялся любой адрес, найденный на компьютере или же случайно сгенерированный. При этом список всех обнаруженных на зараженном компьютере адресов электронной почты также присоединялся к вложению. Кроме рассылки своих копий, червь обнаруживал себя по 13-м числам четных месяцев или шестым нечетных, в зависимости от модификации: в такой день все файлы на зараженных компьютерах заполнялись случайным содержимым.

2001 — 2005

Tanatos/Bugbear (октябрь 2001) — почтовый червь, устанавливающий бекдор-процедуру (Backdoor) и троян — клавиатурный шпион. Процедура распространения практически списана с Klez - копирование по сети, массовая рассылка с зараженным документом во вложении, использование уязвимости IFrame в Internet Explorer, подавление антивирусных программ. Кроме увеличения трафика, вирус проявлял себя спонтанной печатью разнообразного мусора на сетевых принтерах.

В январе 2003 года грянула эпидемия интернет-червя Slammer, заражающего сервера под управлением Microsoft SQL Server 2000. Вирус использовал брешь в системе безопасности SQL Server, заплата к которой вышла в июле 2002. После проникновения червь начинает в бесконечном цикле посылать свой код на случайно выбранные адреса в сети - только за первые 10 минут было поражено около 90% (120 000 единиц) всех уязвимых серверов, при этом пять из тринадцати главных DNS-серверов сети Интернет вышли из строя.

2001 — 2005

Slammer имел крайне небольшой размер - всего 376 байт (CodeRed - 4 КБ, Nimda - 60 КБ) и присутствовал только в памяти зараженных компьютеров. Более того, при работе червя никакие файлы не создавались, и червь никак не проявлял себя (помимо сетевой активности зараженного компьютера). Это означает, что лечение заключается только в перезагрузке сервера, а антивирусы в данной ситуации бессильны.

В августе 2003 года около 8 миллионов компьютеров во всем мире оказались заражены интернет-червем Lovesan/Blaster. Для размножения использовалась очередная брешь - на этот раз в службе DCOM RPC Microsoft Windows. Кроме того, вирус включал в себя функцию DDoS-атаки на сервер с обновлениями для Windows.

Неделей позже новый вирус, Sobig.f, установил новый рекорд по скорости - доля зараженных им писем доходила до 10 % от всей корреспонденции. Это достигалось использованием спамерских технологий. Sobig.f также инициировал цепную реакцию: каждый новый вариант червя создавал сеть инфицированных компьютеров, которая позднее использовалась в качестве платформы для новой эпидемии. Однако конец эпидемии запрограммировал сам автор - 10 сентября 2003 года Sobig.f прекратил размножение.

2001 — 2005

Swen (также известный как Gibe, сентябрь 2003) — яркий пример удачного использования методов социальной инженерии. Этот вирус-червь распространялся по электронной почте в виде письма якобы от Microsoft Corporation Security Center и с темой "Internet Security Update". Во вложении находился файл с именем q216309.exe, а в самом сообщении говорилось о необходимости срочной установки вложенной заплатки.

Следующий год принес популярность новой технологии распространения вредоносных программ - путем рассылки, по электронной почте или с помощью интернет-пейджера, сообщения со ссылкой, ведущей на сайт с трояном.

2001 — 2005

Mitglieder (январь 2004 года) — троянский proxy-сервер, ссылка на зараженный этой программой сайт была разослана злоумышленником на тысячи адресов ICQ. Mitglieder проникал на компьютер через уязвимость в Microsoft Internet Explorer, позволявшую установить и запустить proxy-сервер на зараженной машине без ведома пользователя. После заражения открывался порт, используемый для рассылки спама. Таким образом, зараженные машины образовывали сеть машин-зомби (ботнет), которыми можно удаленно управлять, чем вскоре и воспользовались авторы новых вредоносных программ.

2001 — 2005

Буквально через месяц, в феврале 2004 года появился Bizex (также известный как Exploit) — первый ICQ-червь. Для распространения использовалась массовая несанкционированная рассылка по ICQ сообщения "http://www.jokeworld.biz/index.html :)) LOL". Получив от знакомого человека такую ссылку, ничего не подозревающая жертва открывала указанную страницу и в случае, если использовался браузер Internet Explorer с незакрытой уязвимостью, на компьютер загружались файлы червя и в некоторых случаях сопутствующего трояна. После установки в систему, Bizex закрывал запущенный ICQ-клиент и подключившись к серверу ICQ с данными зараженного пользователя начинал рассылку по найденным на компьютере спискам контактов. Одновременно происходила кража конфиденциальной информации - банковские данные, различные логины и пароли.

2001 — 2005

В этом же 2004 году разразилась так называемая война вирусописателей. Несколько преступных группировок, известных по вирусам Bagle, Mydoom и Netsky выпускали новые модификации своих программ буквально каждый час. Каждая новая программа несла в себе очередное послание к противостоящей группировке, изобилующее нецензурными выражениями, а Netsky даже удалял любые обнаруженные экземпляры вирусов Mydoom и Bagle.

Почтовый червь Bagle впервые был обнаружен 18 января 2004 года. Для распространения он использовал собственный SMTP-клиент, код вируса пересылался во вложении с произвольным именем и расширением .exe. Рассылка производилась на адреса, найденные на зараженном компьютере. Также Bagle содержал встроенную backdoor-процедуру, открывающую порт 6777 на запуск команд и загрузку любых файлов. Следующие модификации содержали процедуры распространения через P2P-сети, методы социальной инженерии, активно противодействовали антивирусному программному обеспечению.

2001 — 2005

Mydoom известен прежде всего массированной 12-дневной DDoS-атакой на веб-сайт компании SCO, начавшейся 1 февраля 2004 года. За пару часов работа сервера была полностью парализована и вернуться в нормальный режим www.sco.com смог только 5 марта. В ответ руководители SCO объявили награду в размере 250 тысяч долларов США за информацию об авторе червя.

Для распространения Mydoom использовал почтовую рассылку через собственный SMTP-клиент, а также P2P-сети (Kazaa).

Первая модификация почтового червя NetSky (также известен как Moodown) была обнаружена 16 февраля. Кроме электронной почты, для распространения были задействованы P2P и локальные сети. Вторая модификация NetSky отличилась тем, что в силу человеческого фактора ею были заражены тысячи писем, отправленных известным финским производителем антивирусного ПО - компанией F-Secure своим клиентам.

2001 — 2005

Sasser (май 2004) — поразил более 8 млн. компьютеров, убытки от этого червя оцениваются в 979 млн. долларов США. Для проникновения Sasser использовал уязвимость в службе LSASS Microsoft Windows.

Cabir (июнь 2004) — первый сетевой червь, распространяющийся через протокол Bluetooth и заражающий мобильные телефоны, работающие под управлением OS Symbian. При каждом включении зараженного телефона вирус получал управление и начинал сканировать список активных Bluetooth-соединений. Затем выбирал первое доступное соединение и пытался передать туда свой основной файл caribe.sis. Ничего деструктивного Cabir не делал - только снижал стабильность работы телефона за счет постоянных попыток сканирования активных Bluetooth-устройств.

2001 — 2005

Вскоре (август 2004) появились и вирусы для PocketPC — классический вирус Duts и троянская программа Brador.

Однако вредоносные программы — это не только вирусы и трояны. К этому классу в полной мере можно отнести и adware — программы, которые отображают на экране рекламу без ведома и согласия пользователя, и pornware — программы, самостоятельно инициирующие соединения с платными порнографическими сайтами. Начиная с 2004 отмечается широкое распространение использования вирусных технологий для установки adware/pornware на целевые компьютеры.

Этот год также запомнился масштабными арестами вирусописателей - было осуждено около 100 хакеров, причем трое из них находились в двадцатке самых разыскиваемых ФБР преступников.

2005 — ...

В 2005 году наметился некоторый спад активности почтовых червей. Фактически, после Mydoom, NetSky и Bagle до середины лета 2005 года не наблюдалось ни одной сколько-нибудь значительной эпидемии. Это может свидетельствовать об успешности новых технологий распространения вредоносных программ на фоне значительных достижений антивирусных компаний.

Поэтому пальму первенства перехватили сетевые черви и программы, использующие для распространения различные интернет-пейджеры (прежде всего MSN Messenger). Первые активно используют бреши в операционных системах Microsoft Windows - чаще всего это уязвимости в службах RPC DCOM и LSASS, а также дыры, оставленные прошедшими ранее эпидемиями: это позволяет создавать ботнеты, включающий тысячи компьютеров-зомби. Вторые - пользуются некомпетентностью и отсутствием опыта создателей программ обмена сообщениями в упреждении вирусных инцидентов.

2005 — ...

Однако, глобальных эпидемий в первой половине 2005 зафиксировано не было. Это не означает уменьшение числа вирусов - наоборот, с каждым днем их появляется все больше. Но при этом можно отметить увеличение избирательности вредоносных программ - становятся популярны черви, главной целью которых является похищение определенной информации. Кроме уже ставших привычными краж номеров кредитных карт, участились случаи воровства персональных данных игроков различных онлайновых игр - Ultima Online, Legend of Mir, Lineage, Gamania. В России также зафиксированы случаи с игрой "Бойцовский клуб", где реальная стоимость некоторых предметов на аукционах достигает тысяч долларов США.

Развитие получили и вирусные технологии для мобильных устройств. Созданы вирусы всех трех типов - классические вирусы, черви и троянские программы. В качестве пути проникновения используются не только Bluetooth-устройства, но и обычные MMS-сообщения (червь ComWar).

Заключение

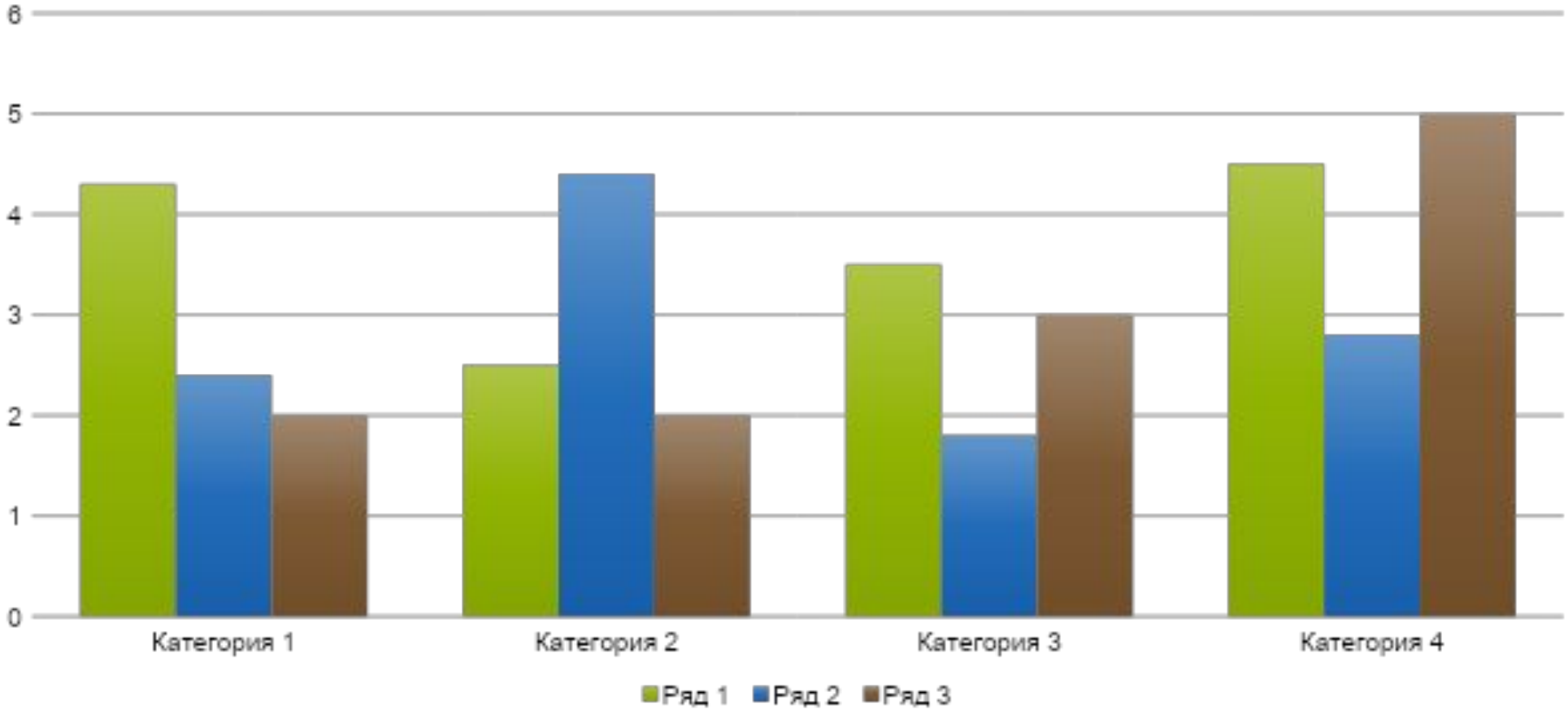
Отличие ученого от вирусописателя состоит в целях, которые преследует автор программы. Вирусы могут не только воровать кредитные карты и рассылать от чужого имени спам. С помощью самораспространяющих программ возможно моделирование в компьютерных системах искусственной жизни, воспроизведение поведения взаимодействующих друг с другом и эволюционирующих живых организмов.

Придуманный Фредом Коэном термин вирус изначально не нес негативной нагрузки. Однако с появлением первых вредоносных программ сформировалось общественное мнение, что вирус - значит плохо. Это практически поставило крест на исследованиях, посвященных разработке таких вирусов, которые вместо вреда приносили бы некоторую пользу - в этом случае получив некоторую выгоду, пользователь предоставлял бы возможность программе свободно развиваться и эволюционировать. Но по состоянию на сегодняшний день, можно уверенно констатировать: встречающиеся в живом виде вирусы несут угрозу нормальному функционированию компьютерных систем.

Заключение

Подтверждением этому может служить статистика - в современном Интернет в среднем каждое тридцатое письмо заражено почтовым червем, около 70% всей корреспонденции - нежелательна. С ростом сети Интернет увеличивается количество потенциальных жертв вирусописателей, выход новых систем и платформ влечет за собой расширение спектра возможных путей проникновения в систему и вариантов возможной вредоносной нагрузки для вирусов. Современный пользователь компьютера не может чувствовать себя в безопасности перед угрозой стать объектом чей-то злой шутки - например, уничтожения информации на винчестере - результатов долгой и кропотливой работы, или кражи пароля на почтовую систему. Точно так же неприятно обнаружить себя жертвой массовой рассылки конфиденциальных файлов или ссылки на порно-сайт. Поэтому при выявлении антивирусным комплексом вируса можно однозначно сказать, что это - вредоносная программа.

Макет заголовка и объектов с диаграммой



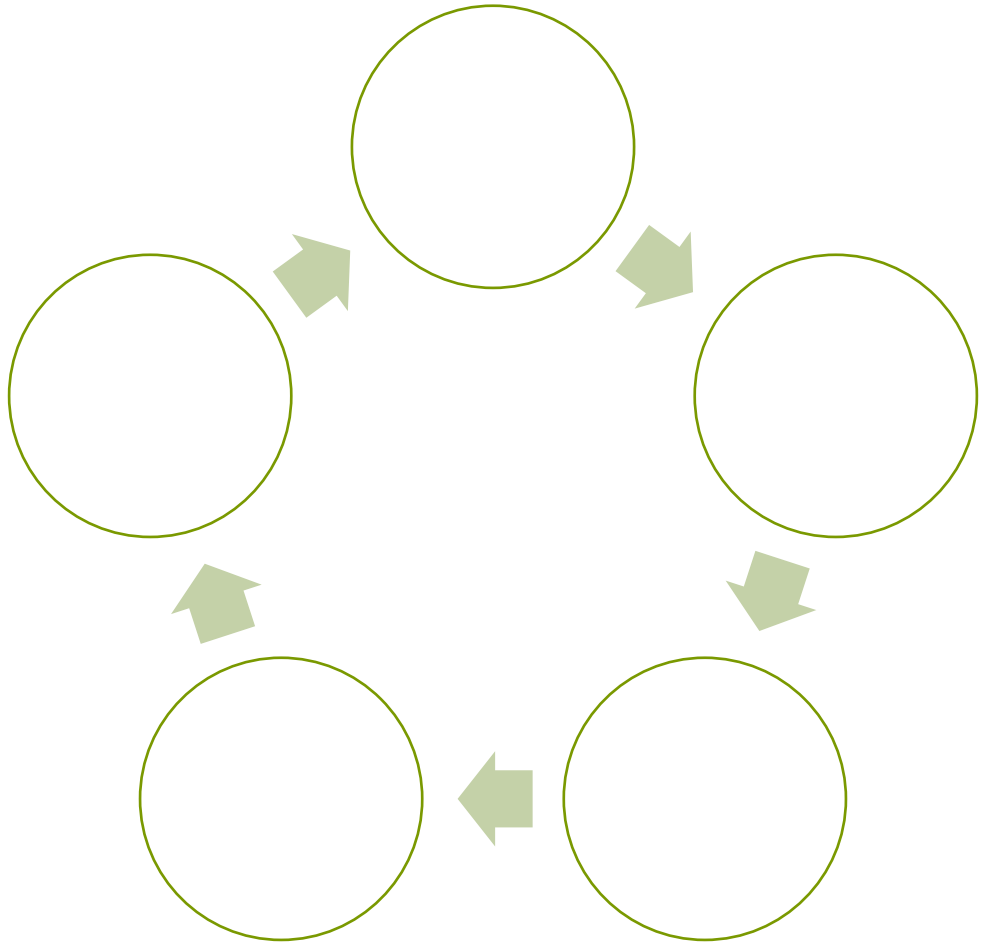
Макет двух объектов с таблицей

- Первый пункт списка
- Второй пункт списка
- Третий пункт списка

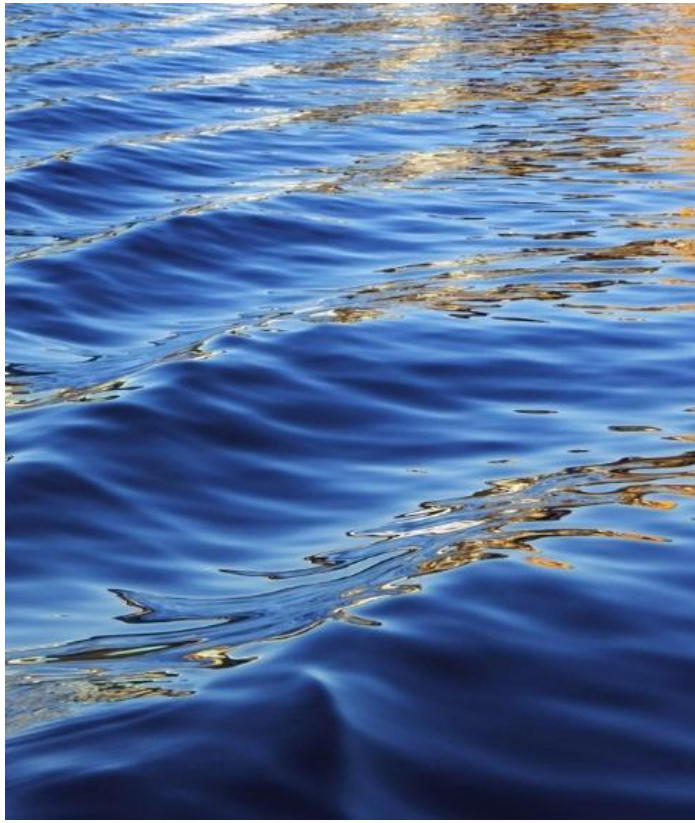
Предмет	Группа А	Группа Б
Предмет 1	82	95
Предмет 2	76	88
Предмет 3	84	90

Макет двух объектов со SmartArt

- Первый пункт списка
- Второй пункт списка
- Третий пункт списка



Добавить заголовок слайда — 1



Добавить заголовок слайда — 2

Добавить заголовок слайда — 3

Добавить заголовок слайда — 4

Добавить заголовок слайда — 5