Коми Республикаса йӧзӧс велӧдан да том йӧз политика министерство
Министерство образования и молодежной политики Республики Коми
Государственное профессиональное образовательное учреждение
«Сыктывкарский целлюлозно-бумажный техникум»

III Внутритехникумовская студенческая научно-практическая конференция «Студенческая наука», посвященная 95-летию Республики Коми.

ВИРУСЫ

Секция
Знание – сила

Выполнили:
Можегов Олег Вадимович, Шахтаров Владислав Михайлович, студенты группы СЗ-11
Специальность
08.02.01 Строительство и эксплуатация зданий и сооружений
Научный руководитель:
Аверьянова А.Г., преподаватель

Сыктывкар 2016

Содержание проекта.

1. Обоснование выбора темы проекта.
2. Аннотация к проекту.
3. Основополагающий вопрос.
4. Проблемный вопрос.
5. Гипотеза.
6. Задачи.
7. Оборудование, необходимое для реализации проекта.
8. Этапы исследования.
9. Выводы.
10. Заключение.
11. Список использованных ресурсов.

1. Обоснование выбора темы проекта.

Технические и биологические науки долгое время развивались параллельными путями и подчинялись собственной логике развития. Однако в последнее время ученые находят все больше сходства между предметами информатики и биологии.

В сложных искусственных системах начинают работать законы живого мира. Термин «технический прогресс» пора менять на термин «эволюция». В качестве одного из примеров «переходных» систем американский технологический журнал Wired предлагает рассматривать компьютерные вирусы. Сходство между вирусами компьютерными и биологическими сегодня не вызывает сомнений. Многие ученые относят биологические вирусы к царству вирусы, называя их неклеточными формами жизни.

Сегодня компьютерные вирусы представляют собой одну из самых серьезных проблем в информационной безопасности. Ежедневно сообщают о появлении новых представителей и модификаций старых программ, как на информационном поле, так и в природе.

Этот вопрос и явился основой для разработки данного проекта.

2. Аннотация к проекту.

Проект основывается на сравнительном анализе компьютерных и биологических вирусов.

Цель проекта – проанализировать информационные источники и создать на основе их компьютерную видео - презентацию, которая бы показывала пример сходства биологических и компьютерных вирусов. Проект рассчитан на обучающихся первого курса и может быть использован на лекциях по дисциплинам биологии и валеологии при изучении темы “Вирусы”, на классных часах при рассмотрение темы “Профилактика СПИд и ВИч”, на лекциях информатики при изучении компьютерных вирусов и антивирусных программ, при изучении тем по защите информации. Кроме того, информация, содержащаяся в проекте полезна для расширения области знаний обучающихся в названных предметных областях.

3. Основополагающий вопрос.

Вирусная инфекция – области распространения.

4. Проблемный вопрос.

Сходства и различия компьютерных и биологических вирусов.

5. Гипотеза.

Грань между живой и неживой природой становится всё менее чёткой!

6. Задачи.

1. изучить историю происхождения компьютерных и биологических вирусов.

2. проанализировать вред, наносимый компьютерными и биологическими вирусами и их последствия.

3. изучить классификацию компьютерных и биологических вирусов.

4. установить признаки заражения компьютерными и биологическими вирусами.

5. изучить методы борьбы с компьютерными и биологическими вирусами.

6. подготовить видео презентации “Механизм заражения биологическим вирусом” и “Механизм заражения компьютерным вирусом”

7. подготовить материал к выступлению.

7. Оборудование, необходимое для реализации проекта

1. Компьютерное рабочее место с выходом в Интернет.
2. Сканер.
3. Мультимедийный проектор.
4. Программное обеспечение: офисные приложения Windows, графический редактор для обработки изображений.
5. Программы Cinema4d и SonyVegas 12.

8. Этапы исследования

Рассмотрим этапы исследования:

1. История происхождения компьютерных и биологических вирусов.

Компьютерный вирус – это программа, способная создавать свои копии, внедрять их в различные объекты или ресурсы компьютерных систем, сетей и производить определенные действия без ведома пользователя.

Мнений по поводу рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были. Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г., журнал "Scientific American" опубликовал статью Л.С. Пенроуза, которая также была посвящена 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 - реализовал модель на практике с помощью машинного кода на IBM 650. В 1962 г. инженеры из американской компании Bell Telephone Laboratories - В.А. Высотский, Г.Д. Макилрой и Роберт Моррис - создали игру "Дарвин". Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

Считается, что автором первой программы – вируса является американец Фред Коэн. В 1983, будучи студентом, он в рамках работы над диссертацией написал программу, которую назвал «вирусом» за ее способность к саморазмножению.

Вирусы биологические — неклеточные формы жизни, которые могут развиваться только внутри клеток организмов. Это связанно с тем, что вирусы устроены очень просто и не имеют собственных систем поддержания жизнедеятельности. Вне клеток они не активны, и как бы «спят». Вирус состоит из оболочки и нуклеиновой кислоты (ДНК или РНК), в которой и записан код: «как при помощи внутренних ресурсов клеток-хозяев собирать себе подобных». [Рис.1.]

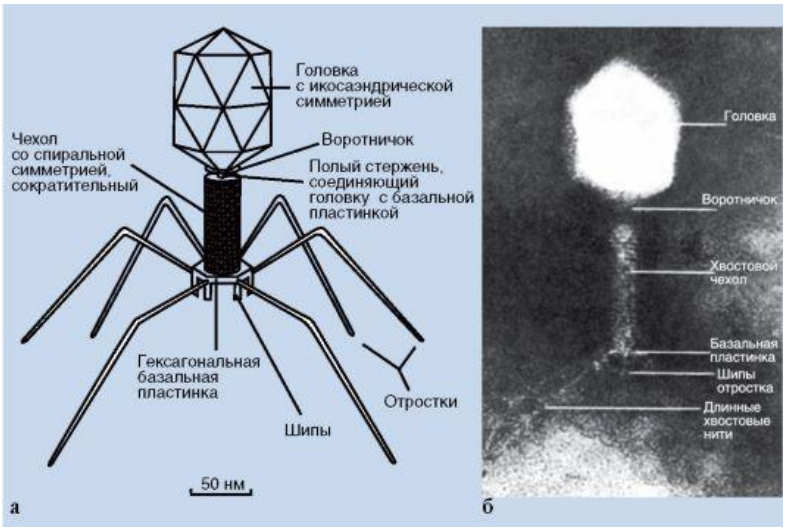

Рис.1. Строение вируса бактериофага.

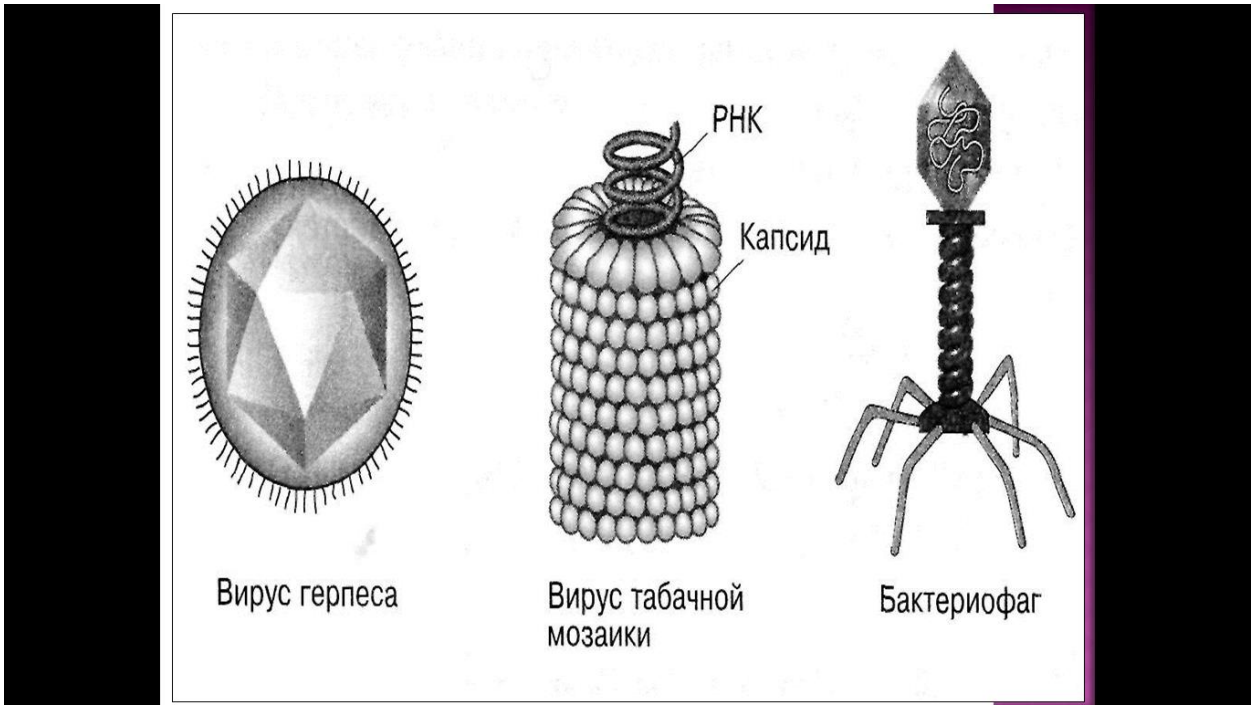

Рис.2. Многообразие вирусов.

Оболочки вирусов имеют различную сложность. [Рис.2.]
Оболочки некоторых представлены лишь белками, но большинство оболочек включают в себя различные соединения, и даже части клеток хозяина. На эти ухищрения вирусы идут для того, чтобы свободно проникать в клетки организма и паразитировать в них. Если сказать проще, то вирус — это «волк в овечьей шкуре». Благодаря этой оболочке вирус свободно проникает в клетку. Внутри оболочка «паразита» растворяется, и вирус начинает заражение клетки.

Одновременно собираются нуклеиновые кислоты и оболочки в вирусы.
Возникшие маленькие вирусы дружным строем покидают одну клетку и ищут другие, в которых они могли бы размножаться. Клетка может, либо погибнуть, либо остаться в живых, но уже в ослабленном состоянии, так как синтез вирусов мешал ее нормальной жизнедеятельности. Стоит отметить так же, что разные вирусы предпочитают свой тип клеток для размножения.

Во второй половине прошлого столетия учеными-микробиологами были открыты бактерии, вызывающих заболевания человека, животных и растений. Микробиологи обратили внимание на ряд инфекционных заболеваний человека и животных (оспа, бешенство, корь, краснуха и др.), а также растений, при которых бактериальные методы выяснения их возбудителей оказались непригодными. Выходом из тупика, в котором очутилась микробиология, послужило открытие, сделанное русским ученым Д. И. Ивановским. В 1887 г. он, будучи еще студентом Петербургского университета, поехал на Украину и в Молдавию, где изучал причины мозаичной болезни табака, которая причиняла большой ущерб табачным плантациям южных районов. Свои исследования он проводил в течение нескольких лет и после окончания университета. В результате тщательного изучения этого заболевания Д. И. Ивановский показал, что оно вызывается специфическим возбудителем, состоящим из мельчайших частиц, или корпускул, которые по своим размерам значительно меньше бактерий. Листья табака, пораженного мозаикой, он растирал в ступке и затем полученную массу фильтровал через специальные бактериальные фильтры, не пропускающие бактерий. Полученная после фильтрации прозрачная жидкость не содержала видимых в обычном микроскопе частиц. Но при нанесении ее на царапины, сделанные на поверхности здоровых листьев табака, растение заболевало мозаичной болезнью. Этот прием можно было повторять много раз.

Результаты исследований Д. И. Ивановского были опубликованы в 1892 г. в книге «О двух болезнях табака». В этой работе впервые в истории микробиологии было показано, что в природе существует особый мир мельчайших возбудителей инфекционных заболеваний. Эти возбудители проходят через бактериальные фильтры, невидимы в обычном микроскопе, не растут на тех средах, которые применяются для выращивания бактерий, и способны размножаться только в организме человека, животных и растений. Эти мельчайшие организмы получили название вирусов. Блестящее открытие Д. И. Ивановского ознаменовало новую эпоху в развитии микробиологии и заложило основы новой науки — вирусологии. Открытие первого вируса — возбудителя мозаики табака — было толчком к проведению широких исследований в области вирусологии.

Пользуясь предложенным Д. И. Ивановским методом, ученые стали открывать один за другим вирусы, вызывающие различные заболевания человека, животных и растений. В конце XIX — начале XX в. стало известно, что в природе существуют также вирусы, которые поражают бактерии и при этом вызывают распад (лизис) их клеток. Эти вирусы получили название бактериофагов — «пожирателей бактерий».

2. Вред, наносимый компьютерными и биологическими вирусами и их последствия.

Программа, внутри которой находится компьютерный вирус, называется зараженной программой.

Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы, а также выполняет запланированные деструктивные действия. Для маскировки своих действий вирус активизируется не всегда, а лишь при выполнении определенных условий (истечение некоторого времени, выполнение определенного числа операций, наступления некоторой даты или дня недели и т.д.).

После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится. Внешне зараженная программа может работать так же, как и обычна программа. Подобно настоящим вирусам компьютерные вирусы прячутся, размножаются и ищут возможность перейти на другие ПК.

Таким образом, вирусы должны инфицировать ПК достаточно незаметно, а активизироваться лишь через определенное время (время инкубации). Это необходимо для того, чтобы скрыть источник заражения.

Вирус не может распространяться в полной изоляции от других программ. Очевидно, что пользователь не будет специально запускать одинокую программу-вирус. Поэтому вирусы прикрепляются к телу других полезных программ.

Несмотря на широкую распространенность антивирусных программ, предназначенных для борьбы с вирусами, вирусы продолжают плодиться. В среднем в месяц появляется около 300 новых разновидностей. Естественно, что вирусы появляются не самостоятельно, а их создают кракеры – вандалы.

Различные вирусы выполняют различные действия:

- Выводят на экран мешающие текстовые сообщения (поздравления, политические лозунги, фразы с претензией на юмор, высказывания обиды от неразделенной любви, нецензурные выражения, рекламу, прославление любимых певцов, названия городов);
- Создают звуковые эффекты (проигрывают гимны, гамму или популярную мелодию);
- Создают видеоэффекты (переворачивают или сдвигают экран, имитируют землетрясение, вызывают падение букв в тексте или симулируют снегопад, имитируют скачущий шарик, прыгающую точку, выводят на экран рисунки и картинки);
- Замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивает износ оборудования (например, головок дисководов);
- Вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- Имитируют повторяющиеся ошибки работы операционной системы (например, с целью заключения договора на гарантированное обслуживание ЭВМ);
- Уничтожают FAT – таблицу, форматируют жесткий диск, стирают BIOS, стирают или изменяют установки CMOS, стирают секторы на диске, уничтожают или искажают данные, стирают антивирусные программы;
- Осуществляют научный, технический, промышленный и финансовый шпионаж;
- Выводят из строя системы защиты информации, дают злоумышленникам тайный доступ к вычислительной машине;
- Делают незаконные отчисления с каждой финансовой операции и т.д.;

Главная опасность самовоспроизводящихся кодов заключается в том, что программы – вирусы начинают жить собственной жизнью, практически не зависящей от разработчика программы. Так же, как в цепной реакции в ядерном реакторе, запущенный процесс трудно остановить.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Ви́рус биологический (от лат. *virus* — яд) — микроскопическая частица, способная инфицировать клетки живых организмов. Вирусы являются облигатными паразитами — они не способны размножаться вне клетки.

Одно из свойств биологических вирусов — их вездесущность. Они поражают человека, домашних и диких животных, сельскохозяйственные и дикие растения, простейших, бактерии, грибы и даже микроплазмы. И эти элементы далеко не всегда нейтральны по отношению к человеку и объектам его хозяйственной деятельности.

Попадая в клетку, биологический вирус может встраиваться в ДНК, которая содержится в ядре, или начинает синтезировать вещества, информация о которых содержится в его собственной ДНК, с помощью внутриклеточных механизмов.

3. Классификация (виды) компьютерных и биологических вирусов.

Существует большое число различных классификаций вирусов.

По **среде обитания** они делятся на сетевые, файловые, загрузочные и файлово – загрузочные вирусы.

По **способу заражения** – на резидентные и нерезидентные вирусы.

По **степени опасности** – на неопасные, опасные и очень опасные вирусы.

По **особенностям алгоритма** – на вирусы-компаньоны, паразитические вирусы, репликаторы (черви), невидимки (стелс), мутанты (призраки, полиморфные вирусы, полиморфики), макро-вирусы, троянские программы.

По **целостности** – на монолитные и распределенные вирусы.

Сетевые вирусы распространяются по различным компьютерным сетям.

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot – сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record – MBR). Некоторые вирусы записывают свое тело в свободные сектора диска, помечая их в FAT – таблице как “плохие” (Bad cluster).

Файловые вирусы инфицируют исполняемые файла компьютера, имеющие расширения com и exe. К этому же классу относятся и макровирусы, написанные помощью макрокоманд. Они заражают неисполняемые файлы (например, в текстовом редакторе MS Word или в электронных таблицах MS Excel).

Загрузочно – файловые вирусы способны заражать и загрузочные секторы и файлы.

Резидентные вирусы оставляют в оперативной памяти компьютера свою резидентную часть, которая затем перехватывает обращения неинфицированных программ к операционной системе, и внедряются в них. Свои деструктивные действия и заражение других файлов, резидентные вирусы могут выполнять многократно.

Нерезидентные вирусы не заражают оперативную память компьютера и проявляют свою активность лишь однократно при запуске инфицированной программы.

Действия вирусов могут быть не опасными, например, на экране появляется сообщение: “Хочу чучу”. Если с клавиатуры набрать слово “чуча”, то вирус временно “успокаивается”.

Значительно опаснее последствия действия вируса, который уничтожает часть файлов на диске.

Очень опасные вирусы самостоятельно форматируют жесткий диск и этим уничтожают всю имеющуюся информацию. Примером очень опасного вируса может служить вирус CIN (Чернобыль), активизирующийся 26 числа каждого месяца и способный уничтожать данные на жестком диске и в BIOS.

Компаньон-вирусы (companion) – это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE – файлов новые файлы-спутники (дубликаты), имеющие то же самое имя, но с расширением COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM – файл и никак не изменяет одноименный EXE – файл. При запуске такого файла DOS первым обнаружит и выполнит COM – файл, т.е. вирус, который затем запустит и EXE – файл.

Паразитические вирусы при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. В эту группу относятся все вирусы, которые не являются “червями” или “компаньонами”.

Вирусы – **черви** (worm) – распространяются в компьютерной сети и, так же как и компаньон – вирусы, не изменяют файлы или секторы на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов.

Репликаторы могут размножаться без внедрения в другие программы и иметь “начинку” из компьютерных вирусов.

Вирусы – невидимки (стелс – Stealth) используют некоторый набор средств для маскировки своего присутствия в ЭВМ. Название вируса аналогично названию американского самолета – невидимки.

Стелс – вирусы трудно обнаружить, так как они перехватывают обращения операционной системы к пораженным файлам или секторам дисков и “подставляют” незараженные участки файлов.

Вирусы, которые шифруют собственное тело различными способами, называются полиморфными. Полиморфные вирусы (или вирусы – призраки, вирусы – мутанты, полиморфики) достаточно трудно обнаружить, так как их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление.

Макро – вирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы и электронные таблицы). В настоящее время широко распространяются макро – вирусы, заражающие документ Word и Excel.

Троянская программа маскируется под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT-таблицу) или собирает на компьютере информацию, не подлежащую разглашению. В отличии от вирусов троянские программы не обладают свойством самовоспроизводства.

Троянская программа маскируется, как правило, под коммерческий продукт. Ее другое название “троянский конь”.

Программа монолитного вируса представляет собой единый блок, который можно обнаружить после инфицирования.

Программа распределенного вируса разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус. Таким образом, вирус почти все время находится в распределенном состоянии, и лишь на короткое время собирается в единое целое.

Фактом является то, что компьютерные вирусы можно разбить на группы и на виды, чего нельзя сделать с их биологическими «сородичами». Нет никаких разделений, перегородок между ними, биологические вирусы просто вызывают какое-либо забо-

левания. Почти каждый день мы встречаемся с ними, даже не подозревая этого. Однако с медицинской точки зрения классификация биологических вирусов существует.

В таксономии живой природы вирусы выделяются в отдельный таксон *Vira*, образующий в классификации Systema Naturae 2000 вместе с доменами *Bacteria*, *Archaea* и *Eukaryota* корневой таксон *Biota*. В течение XX века в систематике выдвигались предложения о создании выделенного таксона для неклеточных форм жизни (*Aphanobionta* Novak, 1930; надцарство Acytota Jeffrey, 1971; *Acellularia*), однако такие предложения не были кодифицированы. Систематику и таксономию вирусов кодифицирует и поддерживает Международный Комитет по Таксономии Вирусов (International Committee on Taxonomy of Viruses, ICTV), поддерживающий также и таксономическую базу The Universal Virus Database ICTVdB.

Форма представления генетической информации лежит в основе современной классификации вирусов. В настоящее время вирусы разделяют на следующие сборные группы:

- Вирусы, содержащие двуцепочечную ДНК и не имеющие РНК-стадии (например, герпесвирусы, поксвирусы, мимивирус).
- Вирусы, содержащие двуцепочечную РНК (например, ротавирусы).
- Вирусы, содержащие одноцепочечную молекулу ДНК (например, парвовирусы).
- Вирусы, содержащие одноцепочечную молекулу РНК положительной полярности (например, пикорнавирусы, флавивирусы).
- Вирусы, содержащие одноцепочечную молекулу РНК негативной или двойной полярности (например, ортомиксовирусы, филовирусы).
- Вирусы, содержащие одноцепочечную молекулу РНК и имеющие в своем жизненном цикле стадию синтеза ДНК на матрице РНК, ретровирусы (например, ВИЧ).
- Вирусы, содержащие двуцепочечную ДНК и имеющие в своем жизненном цикле стадию синтеза ДНК на матрице РНК, ретроидные вирусы (например, вирус гепатита В).
- Вироид-подобные вирусы, названные в честь первого открытого представителя, вируса гепатита Дельта - дельтавирусы.

Дальнейшее деление производится на основе таких признаков как структура генома (наличие сегментов, кольцевая или линейная молекула), генетическое сходство с другими вирусами, наличие липидной оболочки, таксономическая принадлежность организма-хозяина и так далее.

4. Признаки заражения компьютерными и биологическими вирусами.

Признаки заражения (симптомы) компьютерным и биологическим вирусом можно представить в виде таблицы, из которой четко просматривается их аналогия.

Компьютерные	**Биологические**

Увеличение размера файлов	Воспаления, поражения органов, проявляющиеся в их увеличении
Появление не существовавших ранее «странных» файлов	Проявление симптомов, не присущих здоровому человеку
Уменьшение объёма доступной оперативной памяти	Нарушение функций головного мозга (в частности – функций памяти) Вирус ZIKA
Внезапно возникающие эффекты (звуковые, видео и т.д.)	Побочные явления, возникающие следствие резкого ухудшения состояния организма (галлюцинации, бред и т.д.)
Появление сбоев в работе операционной системы	Замедленная реакция, несогласованность функционирования различных систем организма
Замедление, прекращение или неправильная работа ранее нормально функционирующих программ	Снижение или потеря трудоспособности, нарушения функционирования, как отдельных органов, так и организма в целом

5. Методы борьбы с компьютерными и биологическими вирусами.

В общих чертах методы борьбы с вирусами:

1. **Компьютерные:**
   Создание антивирусных программ.
   Сканирование информации для выявления вируса.
2. **Биологические:**
   Профилактика заболевания.
   Создание вакцины.

Из выше изложенного можно сделать вывод, методы борьбы идентичные.

Для борьбы с компьютерными вирусами разрабатываются антивирусные программы. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку “здоровым” программам.

Различают следующие виды антивирусных программ:

- Программы – детекторы (сканеры);
- Программы – доктора (или фаги, дезинфекторы);
- Программы – ревизоры;
- Программы – фильтры (сторожа, мониторы);
- Программы – иммунизаторы.

Программы – детекторы рассчитаны на обнаружение конкретных вирусов и основаны на сравнении характерной (спецификой) последовательности байтов (сигнатур или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Программы – детекторы нужно регулярно обновлять, так как они быстро устаревают и не могут выявлять новые виды вирусов.

Следует подчеркнуть, что программы – детекторы могут обнаружить только те вирусы, которые ей “известны”, то есть, есть сигнатуры этих вирусов заранее помещены в библиотеку антивирусных программ.

Таким образом, если проверяемая программа не опознается детектором как зараженная, то еще не следует считать, что она “здорова”. Она может быть инфицирована новым вирусом, который не занесен в базу данных детектора.

Для устранения этого недостатка программы – детекторы стали снабжаться блоками эвристического анализа программ. В этом режиме делается попытка обнаружить новые

или неизвестные вирусы по характерным для всех вирусов кодовым последовательностям. Наиболее развитые эвристические механизмы позволяют с вероятностью около 80% обнаружить новый вирус.

Программы – доктора не только находят файлы, зараженные вирусами, но и лечат их, удаляя из файла тело программы – вируса. Программы – доктора, которые позволяет лечить большое число вирусов, называют полифагами.

В России получили широкое распространение программы – детекторы, одновременно выполняющие и функции программ – докторов. Наиболее известные представители этого класса – AVP (Antiviral Toolkit Pro, автор – Е. Касперский), Aidstest (автор – Д. Лозинский) и Doctor Web (авторы – И. Данилов, В. Лутовин, Д. Белоусов).

Ревизоры – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. При этом проверяется состояние BOOT – сектора, FAT – таблицы, а также длина файлов, их время создания, атрибуты, контрольные суммы.

Контрольная сумма является интегральной оценкой всего файла (его слепком). Получается контрольная сумма путем суммирования по модулю для всех байтов файла. Практически всякое изменение кода программы приводит к изменению контрольной суммы файла.

Антивирусы – фильтры – это резидентные программы (сторожа), которые оповещают пользователя обо всех попытках какой – либо программы выполнить подозрительные действия. Фильтры контролируют следующие операции:

- Обновление программных файлов и системной области диска;
- Форматирование диска;
- Резидентное размещение программ в ОЗУ.

Обнаружив попытку выполнения таких действий, сторож (монитор) сообщает об этом пользователю, который окончательное решение по выполнению данной операции. Заметим, что она не способна обезвредить даже известные вирусы. Для “лечения” обнаруженных фильтром вирусов нужно использовать программы – доктора.

К последней группе относятся наименее эффективные антивирусы – вакцинаторы (иммунизаторы). Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование. Этот вид антивирусных программ морально устарел.

Рассмотрим основные меры по защите ЭВМ от заражения вирусами.

- Необходимо оснастить ЭВМ современными антивирусными программами и постоянно обновлять их версии.
- При работе в глобальной сети обязательно должна быть установлена программа – фильтр (сторож, монитор).
- Перед считыванием с дискет информации, записанной на других ЭВМ, следует всегда проверять эти дискеты на наличие вирусов.
- При переносе на свой компьютер файлов в архивированном виде необходимо их проверять сразу же после разархивации.
- При работе при работе на других компьютерах необходимо всегда защищать свои дискеты от записи.
- Целесообразно делать архивные копии ценной информации на других носителях информации.
- Не следует оставлять дискету в дисководе при включении или перезагрузке ЭВМ, так как это может привести к заражению загрузочными вирусами.
- Антивирусную проверку желательно проводить в “чистой” операционной системе, то есть после ее загрузки с отдельной системной дискеты.
- Следует иметь ввиду, что невозможно заразиться вирусом, просто подключившись к Internet. Чтобы вирус активизировался программа, полученная с сервера из сети, должна быть запущена на клиенте.

- ❖ Получив электронное письмо, к которому приложен исполняемый файл, не следует запускать этот файл без предварительной проверки. По электронной почте часто распространяются “троянские кони”.
- ❖ Целесообразно иметь под рукой аварийную загрузочную дискету, с которой можно будет загрузиться, если система откажется сделать это обычным образом.
- ❖ При установке большого программного продукта необходимо вначале проверить все дистрибутивные файлы, а после инсталляции продукта повторно произвести контроль наличия вирусов.

6. Создание видео - презентации “Механизм заражения биологическим вирусом” и “Механизм заражения компьютерным вирусом”

На основе проанализированного материала мы создали две видео-презентации и про анализировали механизм заражения вирусами. Он оказался идентичным. Для примера взяли вирус ВИЧ и Conficker.

Червь использует уязвимости Windows, связанные с переполнением буфера и при помощи обманного RPC-запроса выполняет код. Первым делом он отключает ряд служб - автоматическое обновление Windows, Windows Security Center, Windows Defender и Windows Error Reporting, а также блокирует доступ к сайтам ряда производителей антивирусов.

Периодически червь случайным образом генерирует список сайтов (около 50 тыс. доменных имён в сутки), к которым обращается для получения исполняемого кода. При получении с сайта исполняемого файла червь сверяет электронно-цифровую подпись, и если она совпала - исполняет файл. Кроме того, червь реализует P2P-механизм обмена обновлениями, что позволяет ему рассылать обновления удалённым Conficker [Рис.4.] (также известен как Downup,Downadup и Kido) — компьютерный червь, эпидемия которого началась 21 ноября2008. Вредоносная программа была написана на Microsoft Visual C++ и впервые появилась в сети 21 ноября 2008. Заражает операционные системы семейства Microsoft Windows (Windows XPи Windows Server 2008 R2). На январь 2009 вирус поразил 12 миллионов компьютеров во всём мире. 12 февраля 2009 Microsoft обещал 250 000 долларов за информацию о создателях вируса.

Отключены и/или не включаются службы:Windows Update ServiceBackground Intelligent Transfer ServiceWindows DefenderWindows Error Reporting ServicesБлокируется доступ компьютера к сайтам производителей антивирусов. При наличии заражённых компьютеров в локальной сети повышается объём сетевого трафика, поскольку с этих компьютеров начинается сетевая атака. Антивирусные приложения с активным сетевым экраном сообщают об атаке Intrusion.Win.NETAPI.buffer-overflow.exploit. Компьютер начинает очень медленно реагировать на действия пользователя, при этом Диспетчер Задач сообщает о 100%-ом использовании ресурсов ЦП процессом svchost.exe. Блокируется служба IPSec. Как следствие нарушение работы сети.

Биологические вирусы не размножаются клеточным делением, поскольку не имеют клеточного строения. Вместо этого они используют ресурсы клетки-хозяина для образования множественных копий самих себя, и их сборка происходит внутри клетки.

Жизненный цикл биологического вируса проходит в 6 этапов [Рис.3.]:

- **Прикрепление** представляет собой образование специфичной связи между белками вирусного капсида и рецепторами на поверхности клетки-хозяина. Это специфичное связывание определяет круг хозяев вируса. Например, ВИЧ поражает только определённый тип человеческих лейкоцитов. Этот механизм обеспечивает инфицирование вирусом только тех клеток, которые способны осуществить его репликацию. Слияние вирусной и клеточной мембран и проникновению вируса в клетку.

- **Проникновение в клетку.** На следующем этапе вирусу необходимо доставить внутрь клетки свой генетический материал. Некоторые вирусы также переносят внутрь клетки собственные белки, необходимые для её реализации (особенно это характерно для вирусов, содержащих негативные РНК). Различные вирусы для проникновения в клетку используют разные стратегии: например, пикорнавирусы впрыскивают свою РНК через плазматическую мембрану, а вирионы ортомиксовирусов захватываются клеткой в ходе эндоцитоза и попадают в кислую средулизосом, где происходит депротеинизация вирусной частицы, после чего РНК в комплексе с вирусными белками преодолевает лизосомальную мембрану и попадает в цитоплазму. Вирусы также различают по тому, где происходит их репликация: часть вирусов (например, те же пикорнавирусы) размножается в цитоплазме клетки, а часть (например, ортомиксовирусы) в её ядре. Процесс инфицирования вирусами клеток грибов и растений отличается от инфицирования клеток животных. Растения имеют прочную клеточную стенку, состоящую изцеллюлозы, а грибы — из хитина, так что большинство вирусов могут проникнуть в них только после повреждения клеточной стенки. Однако почти все вирусы растений (включая вирус табачной мозаики) могут перемещаться из клетки в клетку в форме одноцепочечных нуклеопротеиновых комплексов через плазмодесмы. Бактерии, как и растения, имеют крепкую клеточную стенку, которую вирусу, чтобы попасть внутрь, приходится повредить. Но в связи с тем, что клеточная стенка бактерий намного тоньше таковой у растений, некоторые вирусы выработали механизм впрыскивания генома в бактериальную клетку через толщу клеточной стенки, при котором капсид остаётся снаружи.
- **Лишение оболочек** представляет собой процесс потери капсида. Это достигается при помощи вирусных ферментов или ферментов клетки-хозяина, а может быть и результатом простой диссоциации. В конечном счёте вирусная геномная нуклеиновая кислота освобождается.
- **Репликация** вирусов подразумевает, прежде всего, репликацию генома. Репликация вируса включает синтез мРНК ранних генов вируса (с исключениями для вирусов, содержащих положительную РНК), синтез вирусных белков, возможно, сборку сложных белков и репликацию вирусного генома, которая запускается после активации ранних или регуляторных генов. Вслед за этим может последовать (у комплексных вирусов с крупными геномами) ещё один или несколько кругов дополнительного синтеза мРНК: «поздняя» экспрессия генов приводит к синтезу структурных или вирионных белков.
- Вслед за этим происходит **сборка** вирусных частиц, позже происходят некоторые модификации белков. У вирусов, таких как ВИЧ, такая модификация (иногда называемая созреванием) происходит после выхода вируса из клетки-хозяина.
- **Выход из клетки.** Вирусы могут покинуть клетку после лизиса, процесса, в ходе которого клетка погибает из-за разрыва мембраны и клеточной стенки, если такая есть. Эта особенность есть у многих бактериальных и некоторых животных вирусов. Некоторые вирусы подвергаются лизогенному циклу, где вирусный геном включается путём генетической рекомбинации в специальное место хромосомы клетки-хозяйки. Тогда вирусный геном называется *провирусом*, или, в случае бактериофага, *профагом*. Когда клетка делится, вирусный геном также удваивается. В пределах клетки вирус в основном не проявляет себя; однако в некоторый момент провирус или профаг может вызвать активацию вируса, который может вызвать лизис клеток-хозяев.

Активно размножающийся вирус не всегда убивает клетку-хозяина. Оболочечные вирусы, в том числе ВИЧ, обычно отделяются от клетки путём отпочковывания. В ходе этого процесса вирус обзаводится своей оболочкой, которая представляет собой модифицированный фрагмент клеточной мембраны хозяина или другой внутренней мембраны. Таким образом, клетка может продолжать жить и продуцировать вирус.

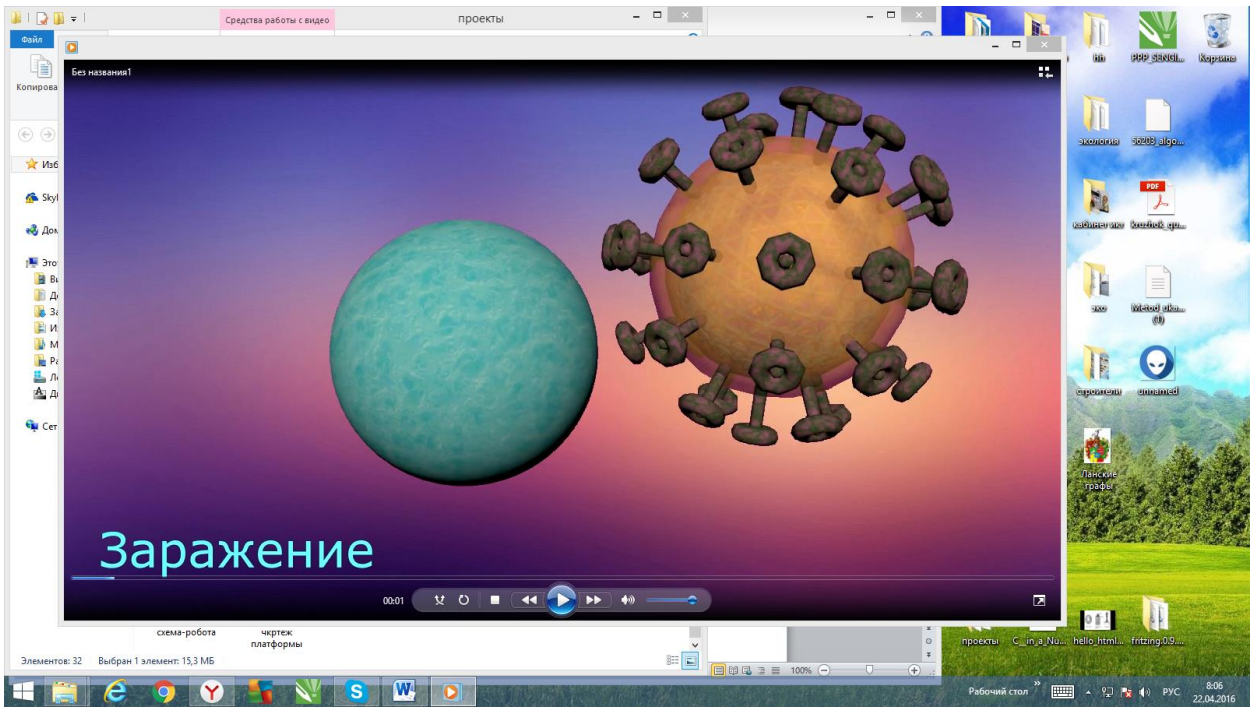

Рис.3. Механизм заражения биологическим вирусом

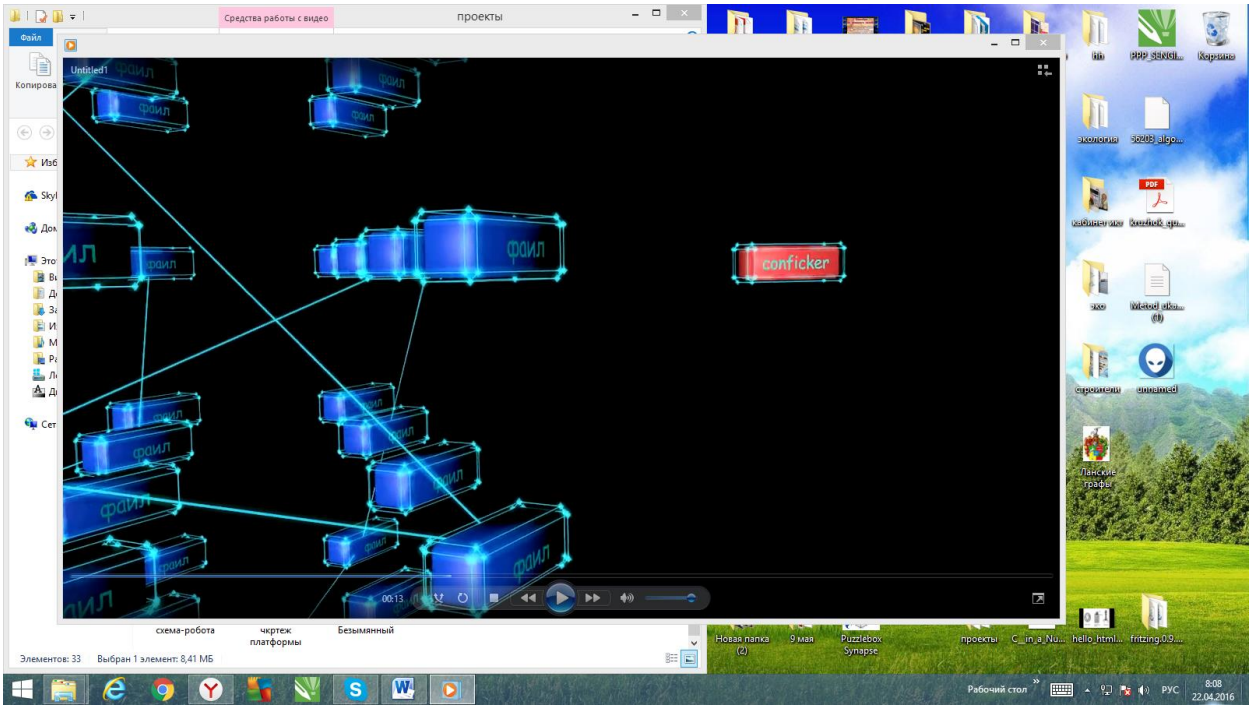

Рис.4. Механизм заражения компьютерным вирусом.

9. Выводы.

Итак, можно подвести итоги. Определим сходства и различия компьютерных и биологических вирусов с точки зрения биологии и валеологии.

Сходства	**Различия**
• Существует определенный набор симптомов – признаков поражения вирусом. • Существуют меры профилактики против вирусов. • Существуют методы борьбы и вирусами.	• В отличие от организма человека, компьютер контролирует вторжение вируса. • В отличие от компьютерных вирусов, биологические оставляют серьезные последствия в виде осложнений. • В отличие от компьютерных вирусов изучение биологических длится дольше, иногда средство бывает не найдено.

С точки зрения компьютерных технологий также сделаем определенные выводы:

1. Компьютерные вирусы появились (а точнее - были изобретены) значительно позже открытия биологических вирусов. Но то, что компьютерные вирусы названы вирусами из-за сходства с биологическими – факт!
2. И те и другие способны к саморазмножению. Однако, компьютерные вирусы в отличие от биологических не способны мутировать.
3. Методы борьбы с вирусами в определенной мере идентичны. Однако их различие в том, что последствия заражения биологическим вирусом является следствием более тяжелых осложнений. Заражение компьютерным вирусом, как правило, имеет менее тяжкие последствия.
4. Сделали видео - презентацию по механизмам заражения.
5. Презентовали проект.

10. Заключение.

Мысль о том, что граница между живой и неживой природой не так уж отчетлива, начинает получать все больше подтверждений в современном мире. Неживой мир жив, и мы с каждым днем будем все больше в этом убеждаться.

11. Список использованных Интернет-ресурсов.

1. Вирусы фото.
URl:http://images.google.ru/images?hl=ru&q=%D0%B2%D0%B8%D1%80%D1%83%D1%81%D1%8B&btnG=%D0%9F%D0%BE%D0%B8%D1%81%D0%BA+%D0%BA%D0%B0%D1%80%D1%82%D0%B8%D0%BD%D0%BE%D0%BA&gbv=2

2. Вирусы энциклопедия
URL:http://images.google.ru/imgres?imgurl=http://03.com.ua/images/b/b2/HIV_virion.jpg&imgrefurl=http://03.com.ua/index.php/%25D0%2592%25D0%25B8%25D1%2580%25D1%2583%25D1%2581%25D1%258B&h=327&w=350&sz=64&hl=ru&start=11&tbnid=fCP0PY5FFsMRmM:&tbnh=112&tbnw=120&prev=/images%3Fq%3D%25D0%25B2%25D0%25B8%25D1%2580%25D1%2583%25D1%2581%25D1%258B%26gbv%3D2%26hl%3Dru%26newwindow%3D1%26sa%3DG

3. Сравнительный анализ антивирусов. Журнал “Хакер” 2005 №1
URL: http://www.xakep.ru/post/26299/?page=1