

Московский Государственный Технический Университет

имени Н.Э. Баумана

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет "Биомедицинская техника"

Кафедра "Медико-технические информационные технологии"

Домашнее задание

На тему:

Сравнение эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов.

по дисциплине  
«Управление в биомедицинской инженерии»

Студентка группы БМТ 2-31М \_\_\_\_\_\_\_\_\_\_ Дьяченкова С.И. *подпись*

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_ Котин В.В. *подпись*

Москва 2020

Оглавление

[ВВЕДЕНИЕ 2](#_Toc52737228)

[1 Источники возникновения эпидемий 3](#_Toc52737229)

[1.1 Классификация компьютерных и биологических вирусов 3](#_Toc52737230)

[2 Модели распространения эпидемий 6](#_Toc52737231)

[2.1 Подходы к моделированию эпидемий в обществе 6](#_Toc52737232)

[2.1 Подходы к моделированию эпидемий компьютерных вирусов 7](#_Toc52737233)

[3 Методы борьбы с угрозами 7](#_Toc52737234)

[4 Сравнение эпидемий в обществе и эпидемий компьютерных вирусов. Обобщенная таблица 7](#_Toc52737235)

[5 Заключение 7](#_Toc52737236)

[Список использованной литературы 8](#_Toc52737237)

# ВВЕДЕНИЕ

На протяжении всей истории человечества эпидемии влияли не только на численность населения и продолжительность жизни, но и на развитие общественного уклада и науки. На сегодняшний день эпидемии по праву считаются одним из самых губительных для человека природных явлений, согласно статистическим данным, инфекционные заболевания унесли больше жизней, чем войны. Развитие биологических вирусов, несмотря на успехи в борьбе с ними, становится причинами пандемий, несущих помимо всего прочего тяжелые последствия для мировой экономики.

Но не стоит забывать, что в XXI веке существуют и информационные угрозы, экономические последствия которых могут быть сравнимы с последствиями инфекционных пандемий.

Еще в 1966 году вышла монография Джона фон Неймана «Теория самовоспроизводящихся автоматов», в которой рассматривалась возможность существования некоего «механического» организма, компьютерного кода, который бы повреждал машины, создавая собственные копии и заражая новые машины, аналогично тому, как это делает биологический вирус. [1] Сейчас можно сказать, что мысленный эксперимент Неймана стал реальностью, и, начиная с 1971 года, компьютерное пространство перенесло десятки эпидемий разных масштабов, и сам компьютерный вирус претерпел множества модификаций.

Целью данной работы является проведение сравнительного анализа эпидемий в обществе и эпидемий компьютерных вирусов.

# 1 Источники возникновения эпидемий

Источниками эпидемий в обществе являются биологические вирусы - неклеточные формы жизни, обладающие собственным геномом и способные к воспроизведению лишь в клетках более высокоорганизованных существ. Для Вирусов в целом характерны две формы существования: внеклеточная, или покоящаяся, и внутриклеточная, размножающаяся (репродуцирующаяся), или вегетативная. [2]

Компьютерный вирус – это нематериальный, неживой объект, - программа, характерной особенностью которой является заражение других программ, создание своих собственных копий. [3]

Существует обширная классификация биологических вирусов, однако, исходя из поставленной задачи, в рамках данной работы рассмотрим классификацию биологических вирусов по параметрам, присущим компьютерным вирусам. [4]

## 1.1 Классификация компьютерных и биологических вирусов

- По среде обитания компьютерные вирусы делятся на:

Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя в загрузочный сектор диска или в сектор системного загрузчика жесткого диска. Начинают работу при загрузке компьютера и обычно становятся резидентными.

Макровирусы заражают файлы широко используемых пакетов обработки данных. Эти вирусы представляют собой программы, написанные на встроенных в эти пакеты языках программирования.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

Кроме того, существуют разнообразные сочетания вирусов — например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные секторы дисков, или сетевые макровирусы, которые заражают редактируемые документы и рассылают свои копии по электронной почте.

Средой обитания биологических вирусов являются живые клетки-бактерии (это вирусы бактерий или бактериофаги), клетки растений, животных и человека.

- По способам заражения

По способам заражения компьютерные вирусы бывают резидентные и нерезидентные.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными лишь ограниченное время.

А что касается биологических вирусов, то существует два способа передачи вирусов от клетки к клетке это горизонтальный - путем выхода вирусной частицы из одной клетки и внедренные в другую (путь передачи инфекционного агента с половыми клетками, в хромосомы которых встраивается наследственный материал вируса). Вертикальный – из поколения в поколение в результате встраивания в хромосому клетки хозяина (процесс взаимодействия вируса и организма хозяина, включающий внедрение паразита, его размножение и выделение в окружающую среду)

Попадание биологического вируса в организм человека может осуществляться: воздушно-капельным, гематогенным, алиментарным и половым путем.

- По особенности алгоритма

И компьютерные, и биологические вирусы имеют схожее устройство: они состоят из большого числа простых блоков, объединенных в последовательности, то есть в цепочки ДНК или строки программы.

Биологические вирусы имеют уникальный геном. Различают ДНК-содержащие и РНК-содержащие вирусы.

По особенностям алгоритма среди компьютерных вирусов выделяют резидентные вирусы, стелс-вирусы, полиморфные и др. Резидентные вирусы способны оставлять свои копии в ОП, перехватывать обработку событий (например, обращение к файлам или дискам) и вызывать при этом процедуры заражения объектов (файлов или секторов). Эти вирусы активны в памяти не только в момент работы зараженной программы, но и после. Резидентные копии таких вирусов жизнеспособны до перезагрузки ОС, даже если на диске уничтожены все зараженные файлы. Если резидентный вирус является также загрузочным и активизируется при загрузке ОС, то даже форматирование диска при наличии в памяти этого вируса его не удаляет.

К разновидности резидентных вирусов следует отнести также макровирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора.

Стелс-алгоритмы позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации. Частично к стелс-вирусам относят небольшую группу макровирусов, хранящих свой основной код не в макросах, а в других областях документа — в его переменных или в Auto-text.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы — это трудно выявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного и того же вируса не имеют совпадений. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

- По деструктивным возможностям вирусы разделяются на:

- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, замедлением работы компьютера, графическим и звуковыми эффектами;

- опасные, которые потенциально могут привести к нарушениям в структуре файлов и сбоям в работе компьютера;

- очень опасные, в алгоритм которых специально заложены процедуры уничтожения данных и возможность обеспечивать быстрый износ движущихся частей механизмов путем ввода в резонанс и разрушения головок чтения/записи некоторых НЖМД.

в случае с биологическими вирусами мы не можем говорить о безопасных вирусах, т.к. таковые не существует. У человека, животных и растений нет безвредных вирусов. Биологические вирусы оставляют серьезные последствия в виде осложнений. Поэтому в зависимости от характера инфекционного процесса, проявления симптомов и выделения вируса в окружающую среду мы рассмотрим хронические, латентные и медленные вирусные инфекции.

Хроническая вирусная инфекция проявляется в форме рецидивов заболевания, развития тяжелых поражений центральной нервной системы, внутренних органов, подавления иммунных функций организма.

Длительную бессимптомную вирусную инфекцию, не сопровождающуюся выделением вируса инфицированным организмом, обозначают термином «латентная вирусная инфекция».

Медленные вирусные инфекции характеризуются длительным (иногда многолетним) инкубационным периодом и медленным развитием основных симптомов болезни (куру, болезнь Крейтцфельдта — Якоба и др.).

# 2 Модели распространения эпидемий

## 2.1 Подходы к моделированию эпидемий инфекционных заболеваний

Для сравнения эпидемий в обществе и эпидемий компьютерных вирусов было принято решение рассмотреть основные подходы к моделированию с целью изучения распространения исследуемых эпидемий. В работе [] была изучена тенденция развития эпидемиологического моделирования и разных подходов к нему. Был выполнен систематический поиск литературы в базе данных Web of Science. Полученные данные были разбиты на 4 кластера:

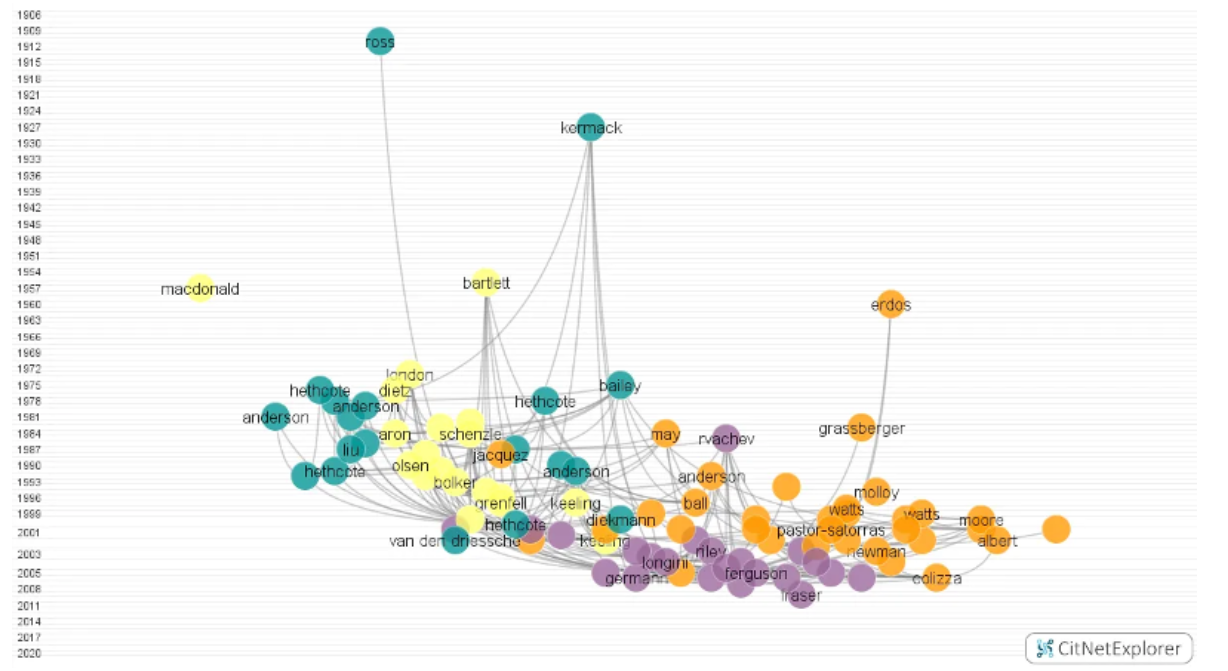


Рисунок 1- Граф, представляющий собой карту прямого цитирования публикаций про эпидемиологические модели; - жёлтый: как распространяется корь, - цвета морской волны: модели на обычных дифференциальных уравнениях и стохастические модели, - оранжевый: моделирование на сетях, - фиолетовый: модели новых эпидемий. [5]

В желтом кластере (модели распространения кори) зародилась гипотезу, что ход эпидемии зависит от числа заражённых и числа уязвимых людей — по аналогии с открытым незадолго до этого законом действующих масс в химии, где скорость реакции зависит от концентрации реагентов. Эта идея стала базовой для компартментальных моделей. Начинается развитие стохастических моделей и последующее их усложнение путем ввода дополнительных параметров, например фактор сезонности или пространственный компонент.

Кластер цвета морской волны показывает динамику исследовательских подходов от обычных дифференциальных уравнений к моделям, включающим вероятности и нелинейные закономерности распространения вируса.

Оранжевый кластер посвящён сетевому подходу к моделированию эпидемий. Население представлено как сеть, где узлы сети — люди, а связи между ними — контакты. От заражённого индивида вирус передаётся тем, кто с ним контактирует, а от них — дальше по сети. В этом кластере часто ссылаются на теорию случайных графов. Более современные работы тоже пользуются случайными графами, при этом считают началом эпидемии не появление первого заражённого, а первую передачу вируса.

Фиолетовый кластер объединяет работы, в которых сложные сетевые модели используются для симуляции эпидемий, в том числе пандемий гриппа в эпоху глобализации, когда из-за дальних путешествий инфекции быстро распространяются по миру.[5]

Таким образом, для моделирования биологических эпидемий характерна тенденция перехода от простых детерменированных SIR моделей, достоинством которых является простой математический аппарат, а недостатком – невозможность учитывать неоднородность популяции и нетривиальные пути передачи инфекции, к стохастическим имитационным, а затем и к сетевому подходу, используя теорию случайных графов, что значительно усложнило математический аппарат, однако позволило учитывать большее количество переменных при моделировании, что дает более реалистичные результаты. [6-8]

## 2.2 Подходы к моделированию эпидемий компьютерных вирусов

Проведенный анализ литературы [9-11] показал, что для моделирования эпидемий компьютерных вирусов довольно часто применяется биологический подход математического моделирования. Рассмотренные работы выявили ряд характерных особенностей распространения компьютерных вирусов в сети и получить математическую оценку скорости заражения отдельных объектов в различных режимах функционирования, исходя из этого, было выявлено, что модели SI, SIR, PSIDR наиболее адекватно описывают процесс распространения компьютерных вирусов. Однако данные математические модели не учитывают связанность и топологических особенностей компьютерных сетей, что является их существенным недостатком. [12]

Для моделирования активного распространения компьютерных червей в интернете используют AAWP (Analytical Active Worm Propagation) отличается от других моделей тем, что основана на дискретном времени (что повышает точность моделирования быстрых червей), учитывает возможность устранения уязвимости, используемой вирусом, учитывает время, требуемое для заражения компьютера и возможность одновременной атаки с различных узлов (что повышает точность моделирования массовых эпидемий). В работе [13] AAWP модель сравнивается с симулятором Уивера, имитационной моделью требующей в отличие от аналитических гораздо больше вычислительных ресурсов, но позволяет с высокой точностью оценивать и сравнивать скорости аспространения вирусов, использующих различные технологии сканирования (случайное сканирование, сканирование заранее составленного списка, сканирование локальных подсетей и перестановочное сканирование). В результате сравнения авторами выяснено, что модернизированная AAWP модель показывает не меньшую эффективность, чем модель Уивера, при этом имея более простой математический аппарат.

Рассмотренные выше модели предполагают, что структура сети не оказывает влияние на динамику распространения эпидемии. При этом вероятность контакта для всех узлов в разные моменты времени является одинаковой. Что не соответствует реальности.

Таким образом, современные подходы к моделированию распространения компьютерных вирусов предполагают учет топологии сетей, поэтому наиболее перспективными с точки зрения разработки механизмов защиты являются модели, основанные на графе сети.

В публикациях последних лет обсуждается разработка интеллектуальных моделей развития и описания вирусных эпидемий в компьютерных сетях, например, подходы, сходные с теорией клеточных автоматов. Так, в [14] рассматривается модель развития вирусной эпидемии не с произвольным порядком распространения вирусов, а с учетом погрешности результатов атак вследствие воздействия вирусов на уже зараженные узлы в сети. С этой целью авторы представляют сеть в виде направленного вероятностного графа (без петель), узлы которого описываются переменными, задающими вероятности их состояния (зараженный, иммунизированный, восприимчивый), а дуги задают взаимодействие между переменными модели. Вирусное распространение определяется характеристиками сети и аналогично действию клеточного автомата. Вирусы могут блуждать в произвольном порядке по пространству графа, иметь различные позиции и скорость. Их перемещение по узлам описывается набором правил. Восприимчивый узел заражается, когда на него попадает вирус; узел, который является носителем болезни, не может быть заражен второй болезнью (т. е. активная болезнь блокирует вторичную инфекцию); иммунизированный узел не может быть заражен повторно и т. д.

Кроме того, очень активно развиваются модели на основе цепей Маркова. В частности, предлагается модель описания развития вирусных эпидемий на основе стохастических моделей интерактивных цепей Маркова [15], в которых состояние узлов сети на каждом следующем шаге развития эпидемии зависит от его состояния и состояния соседей на предыдущем шаге, а сама сеть представляется в виде ненаправленного графа. Использование цепей Маркова, по мнению авторов, позволяет оценить защищенность сетей с различной топологией от компьютерных вирусов и выбирать наиболее безопасные сетевые структуры уже на раннем этапе проектирования.

# 3 Методы борьбы с угрозами

Очевидно, что создание моделей распространения как компьютерных, так и вирусов инфекционных заболеваний осуществляется, прежде всего, с целью последующей разработки механизмов защиты.

В отношении инфекционных заболеваний были разработан комплекс противоэпидемиологических мероприятий, который включает в себя: санитарно-эпидемиологическую разведку и наблюдение; организацию режимно-ограничительных мероприятий; экстренную и специфическую профилактику; использование инди­видуальных и коллективных средств защиты; лечебно-эвакуационные мероприятия; обеззараживание (дезинфекцию, дезинсекцию, дератизацию) и санитарную обработ­ку лиц, находившихся в эпидемическом очаге.

Данные меры включают в себя непрерывное и свое­временное получении достоверных сведений о санитарно-эпидемическом состоянии территории и уровня заболеваемости среди населения, установление источника распространения инфекции, ее возбудитель и условия его распространения.

Важной особенностью противоэпидемических мероприятий при угрозе распро­странения инфекционных заболеваний является организация системы режимно-ограничительных мер.

После выявления заболевших в эпидемическом очаге для всего населения уста­навливается режим обсервации. Под обсервацией понимается система изоляцион­но-ограничительных и лечебно-профилактических мероприятий, направленных на предупреждение распространения инфекционных заболеваний. В случае обнаружения факта появления особо опасных инфекций, а также при проявлении других массовых контагиозных заболеваний об­сервацию заменяют карантином. Карантин - это система медико-санитарных и ад­министративных мероприятий, направленных на полную изоляцию эпидемического очага и ликвидацию в ном инфекционной заболеваемости. Важнейшей задачей при карантине является воспрещение распространения ин­фекций как внутри очага, так и за его пределы. При карантине ранее проводимые обсервационные мероприятия усиливаются дополнительными режимными меропри­ятиями.

Экстренная профилактика инфекционных заболеваний и другие мероприятия по специфической защите обеспечивают необходимую степень защиты лишь в комплек­се с неспецифическими мерами защиты - индивидуальными и коллективными.

Таким образом, рассмотренный выше комплекс противоэпидемиологических мер содержит последовательные шаги для обеспечения ликвидации эпидемиологического очага в кратчайшее время. Описанный подход заключается в локализации очага инфекции и применения профилактических гигиенических мер. [16]

Одним из наиболее значимых методов профилактики инфекционных заболеваний является вакцинация. Вакционопрофилактика является фактором уменьшения заболеваемости, ослабления тяжести клинического течения и снижение смертности заболевших, уменьшение числа осложнений у перенесших инфекционные заболевания. Такие крупнейшие достижения медицины, как ликвидация оспы в мире, значительное сокращение заболеваемости полиомиелитом (которое позволило поставить вопрос о его ликвидации), дифтерией, корью стали возможными только благодаря тому, что были созданы эффективные вакцинные препараты против возбудителей этих инфекций. Их применение в широких масштабах позволило защитить людей от заражения, создавать невосприимчивость организма человека к инфекционному агенту.

В случае с компьютерными вирусами выделяют следующие методы борьбы с ними:

Профилактика вирусного заражения и уменьшение предполагаемого ущерба от такого заражения, которая включает в себя резервное копирование значимой информации прочие методы компьютерной гигиеной, для которых можно провести аналогию с мерами гигиены и индивидуальной защиты при эпидемии инфекционных заболеваний.

Использование антивирусных программ.

Антивирусные программы -это компьютерные программы, которые могут сканировать компьютерные системы для обнаружения вредоносных программ, встроенных в память компьютера, и зараженных компьютерных файлов. Затем вредоносные программы могут быть удалены из памяти или зараженных файлов, зараженные файлы могут быть помещены в карантин или зараженный файл может быть удален из компьютерной системы.

Данные программы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры - это резидентные программы, которые оповещают пользователя о всех попытках какой-либо программы записаться на диск, и отформатировать его, а также о других подозрительных действиях.

Данный тип программ может основываться на эвристическом и сигнатурном подходе. Эвристический подход является более действенным для обнаружения новых вирусов, не успевших попасть в базы данных, в то время как сигнатурный подход позволяет выявить лишь известные вирусы.

Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ (сигнатурное сканирование).

Ревизоры - программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохранённой ранее в одном из файлов данных ревизора. Анализируя сообщения программы-ревизора, пользователь может решить, чем вызваны изменения: вирусом или нет.

К последней группе относятся антивирусы - вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной.

Все эти программы универсальные и перспективные, сочетающие функции антивирусного сканера, резидентного сторожа и доктора.

В качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. [17-20]

# 

# 4 Сравнение эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов. Обобщенная таблица сходств и различий

Таблица 1 – Сравнение эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов

|  |  |
| --- | --- |
| Сравнение возбудителей | |
| Сходство | Различие |
| Схожее устройство – состоят из большого числа простых блоков, объединенных в последовательности. (ДНК/РНК, строки кода) [2,3] | Происхождение – антропогенное и природное |
| Характерно как существование вирусов, проявляющих себя сразу, так и ретровирусов [17] | Частота, с которой появляются и мутируют компьютерные вирусы гораздо больше, чем у биологических [9] |
| Способность мутировать [2,3] | Существуют неопасные компьютерные вирусы. Вирусы инфекционных заболеваний всегда наносят ущерб организму, а также могут вызвать осложнения [9] |
| Активное распространение вирусных эпидемий тем выше, чем выше уровень развития сетей сообщения, транспортных, для инфекционных заболеваний, сети интернет, для компьютерных вирусов | Компьютерные вирусы способны к саморепликации в сети, в то время как вирусы инфекционных заболеваний размножаются только в организме носителя [2,9] |
| Сравнение подходов к моделированию эпидемий | |
| Сходство | Различие |
| Моделирование инфекционных заболеваний и эпидемий компьютерных вирусов имеет схожий путь развития от простых детерминированных SIR моделей, к стохастическим имитационным, а затем и к сетевому подходу, используя теорию случайных графов. Во многом это сходство обусловлено тем, что Компьютерные вирусы начали активно изучаться в 1950-х годах, когда уже существовали основные детерминированные модели, поэтому, исходя из сходств возбудителей, эти модели начали применяться и для моделирования эпидемий компьютерных вирусов [5-15] |  |
| Сравнение методов защиты [16-20] | |
| Можно провести аналогию между мерами профилактики компьютерных угроз и инфекционных заболеваний. | Компьютер не способен самостоятельно выработать иммунитет. |
| Антивирусная техника не может предсказать тенденцию эволюции вирусов. | Для компьютерных вирусов, так же как и для вирусов инфекционных заболеваний, применяется понятие вакцинация, однако суть метода другая. |
| Понятие карантина применяется, как для локализации очага инфекционных заболеваний, так и при лечении компьютерных вирусов. |  |
| Прочее | |
| Оба вида эпидемий способны нанести серьезный экономический ущерб | Применение в медицине бактериофагов [21] |

# 5 Заключение

В ходе данной работы был проведен сравнительный анализ эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов. В первой части была дана классификация компьютерных вирусов, исходя из которой, были выделены их сходства и различия с вирусами инфекционных заболеваний. Можно сказать, что рассматриваемые вирусы имеют множество структурных и поведенческих сходств. Существенным различием является способность к саморепликации компьютерных вирусов вне организма-носителя и частота появления мутаций и новых компьютерных вирусов, а также скорость их распространения.

Исходя из первой части работы, можно сделать вывод о том, что не смотря на существующие различия, вирусы инфекционных заболеваний и компьютерные вирусы похожи. Отсюда вытекает тенденция применения биологических подходов в моделировании эпидемий компьютерных вирусов. Во второй части работы были изучены подходы к моделированию эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов и определено, что они прошли похожий путь развития от применения простых детерминированных подходов до применения теорий сложных сетей.

Поскольку создание моделей распространения как компьютерных, так и вирусов инфекционных заболеваний осуществляется, прежде всего, с целью последующей разработки механизмов защиты. Были рассмотрены существующие методы борьбы с компьютерными угрозами и комплекс противоэпидемиологических мероприятий. В обоих случаях используемые меры включают в себя меры по обнаружению и выявлению угрозы, ее локализации и устранения очага инфекции. Однако существуют существенные различия, поскольку для компьютеров невозможно применить такое понятие как иммунитет. С постоянным появлением новых вариантов существующих вирусов, а также новых типов вирусных штаммов, борьба, ведущаяся человеком против вирусов, обречена быть бесконечной, трудной и коварной; действительно, разработка новых типов антивирусных программ всегда отстает от появления новых типов вирусов. Таким образом, антивирусная техника не может предсказать тенденцию эволюции вирусов и, следовательно, не может дать глобальных рекомендаций по их предотвращению и контролю.

Также нельзя обойти тот факт, что оба вида эпидемии способны нанести большой урон мировой экономике.

В заключение своей работы я попытаюсь ответить на вопрос: «Какое значение для медико-биологического применения играет экскурс в область компьютерных вирусов?»

В ходе работы были выявлены многочисленные сходства эпидемий инфекционных заболеваний и эпидемий компьютерных вирусов. Однако в то время как новые виды биологических вирусов появляются раз в несколько лет, компьютерные вирусы развиваются и мутируют куда более стремительно, соответственно эпидемии в сети интернет происходят чаще. Таким образом, появляется большое количество релевантной информации, которая может быть использована для применения новых методов моделирования, которые впоследствии могут стать эффективными для прогнозирования эпидемий инфекционных заболеваний.

# Список использованной литературы

1. Бёркс А. и др. Теория самовоспроизводящихся автоматов. – 2009.
2. Общая и частная вирусология, под ред. В.М. Жданова и С.Я. Гайдамович, т. 1—2, М., 1982; Тихоненко Т.И. и др. Вирусы, БМЭ, 3-е изд., т. 4, с. 232, М., 1976.
3. Безруков Н.Н. Компьютерные вирусы. - М.: Наука - 1991.
4. Новиков С.В. Модель распространения вирусных атак в Сетях передачи данных общего пользования на основе расчета длины Гамильтонова пути/ Автореферат. СПб.: - 2007.
5. Электронный ресурс: <https://polit.ru/> [А. Лосева, Л. Панкравтова,   
   Моделирование эпидемий: история развития, 2020]
6. Sharkey K. J. Deterministic epidemiological models at the individual level //Journal of Mathematical Biology. – 2008. – Т. 57. – №. 3. – С. 311-331.
7. Lahrouz A., Omari L., Kiouach D. Global analysis of a deterministic and stochastic nonlinear SIRS epidemic model //Nonlinear Analysis: Modelling and Control. – 2011. – Т. 16. – №. 1. – С. 59-76.
8. Allen L. J. S., Lahodny Jr G. E. Extinction thresholds in deterministic and stochastic epidemic models //Journal of Biological Dynamics. – 2012. – Т. 6. – №. 2. – С. 590-611.
9. Williamson M. M. Biologically inspired approaches to computer security [Электронный ресурс] / HP Labs Technical Report HPL-2002-131, HP Labs Bristol, UK. 10 p. // (по состоянию на 12.03.2007).
10. Kephart J. O., White S. R. Directed-graph epidemiological models of computer viruses // Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, California, 1991. P. 343–359.
11. Rohloff K. R., Basar T. Stochastic behavior of random constant scanning worms //Proceedings. 14th International Conference on Computer Communications and Networks, 2005. ICCCN 2005. – IEEE, 2005. – С. 339-344.
12. Давыдов В. В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом //Системи обробки інформації. – 2012. – №. 3 (2). – С. 147-151.
13. Chen Z., Gao L., Kwiat K. Modeling the spread of active worms //IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428). – IEEE, 2003. – Т. 3. – С. 1890-1900.
14. Vălean H., Pop A., Avram C. Intelligent model for virus spreading // Proceed. of the Int. Symp. on System Theory, Automation, Robotics, Computers, Informatics, Electronics and Instrumentation. SINTES 13. 18-20 October 2007, Craiova, Romania. P. 117–122.
15. Далингер Я.М., Бабанин Д.В., Бурков С.М. Математические модели распространения вирусов в компьютерных сетях различной структуры // Моделирование систем. 2011. № 4(30). С. 3–11.
16. Хизгияев В. И. Санитарно-противоэпидемические (профилактические) мероприятия //Российское предпринимательство. – 2002. – №. 8.
17. Singh J. et al. A fractional epidemiological model for computer viruses pertaining to a new fractional derivative //Applied Mathematics and Computation. – 2018. – Т. 316. – С. 504-515.
18. Williamson M. M. Biologically inspired approaches to computer security //Information Infrastructure Laboratory, HP Laboratories Bristol. – 2002.
19. Pham K. et al. System and method for protecting computer users from web sites hosting computer viruses : заяв. пат. 09988606 США. – 2003.
20. Hill R. K. Protecting computers and people from viruses. – 2020.
21. Асланов Б. И., Любимова А. В., Зуева Л. П. Бактериофаги как эффективные противоэпидемические средства для купирования вспышек внутрибольничных инфекций //Журнал инфектологии. – 2019. – Т. 11. – №. 1. – С. 65-70.