СОДЕРЖАНИЕ

Введение

В постановлении Президента Республики Узбекистан «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий» от 21 марта 2012 год, № ПП-1730 [1] особое внимание уделено вопросам «Совершенствования системы регулирования в сфере информационно-коммуникационных технологий с учетом состояния развития информационных ресурсов технологий и систем...».

Вряд ли стоит напоминать, что компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации. Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность. Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Достаточно вспомнить появление «первой ласточки», наделавшей много шума - вируса WinWord. Concept, поражающего документы в формате текстового процессора Microsoft Word for Windows. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера

знаний о природе вирусов, способах заражения вирусами и защиты от них.

В литературе весьма настойчиво пропагандируется, что избавиться от вирусов можно лишь при помощи сложных (и дорогостоящих) антивирусных программ, и якобы только под их защитой вы можете чувствовать себя в полной безопасности. Это не совсем так - знакомство с особенностями строения и способами внедрения компьютерных вирусов поможет вовремя их обнаружить и локализовать, даже если под рукой не окажется подходящей антивирусной программы.

Все вышеперечисленные факторы и обусловили актуальность нашего исследования.

Целью данной выпускной квалификационной работы является исследование методов обнаружения вредоносных программ и компьютерных вирусов в инфокоммуникационных системах.

ВКР состоит из введения, трех глав, заключения и списка использованной литературы.

Во введении обосновывается актуальность избранной темы.

В теоретическом разделе отражаются типы компьютерных вирусов, анализируются каналы распространения вирусов и вредоносных программ, выполняющей сканирование файлов для поиска известных вирусов и обнаружение подозрительного поведения любой из программ. Описываются эвристического и сигнатурного методов анализа компьютерных вирусов и методики обнаружения вредоносных программ без использования специальных средств. Кроме того рассматриваются принципы реализации единой технической политики при обосновании выбора антивирусных продуктов и охвата системой антивирусной защиты всей локальной сети организации.

В основном разделе рассматриваются методы защиты от вирусов. Во-первых, это межсетевые экраны, препятствующие проникновению вредоносных программ, а во-вторых, антивирусные программы, обнаруживающие «вирусы» и уничтожающие их. Исследуется алгоритм на

основе методом Монте-Карло, позволяющий изменить выбранный случайным образом элемент матрицы и вычислить время заражения и модели распространения компьютерных вирусов на основе цепей Маркова, определяющей вероятности изменения состояния и заражения компьютера. Описывается методика комплексной оценки антивирусных программ на основе нечетких математических моделей, выполняющая тестировать антивирусов по различным критериям. Предлагается алгоритм защиты компьютера от вредоносных воздействий, позволяющий представить комплексный подход к определению целостности данных в программно-аппаратные средств защиты информации.

Третий раздел включает в себя безопасность жизнедеятельности.

В заключении приводятся основные результаты и выводы, полученные автором в ходе выполнения работы.

1. Теоретическая часть. Особенности вредоносных программ и компьютерных вирусов в инфокоммуникационных системах

1.1. Определение и типы компьютерных вирусов

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а, скажем, при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается резидентно, т.е. до перезагрузки DOS, в памяти компьютера и время от времени заражает программы и выполняет вредные действия на компьютере[2].

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющих в компьютере дисках. Но некоторые виды файлов вирус может «заразить». Это означает, что вирус может «внедриться» в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Следует заметить, что тексты программ и документов, информационные файлы без данных, таблицы табличных процессоров и

другие аналогичные файлы не могут быть заражены вирусом, он может их только испортить.

Типы компьютерных вирусов

Бытовые вирусы сектора начальной загрузки. Программы, записывающиеся в хвост программы начальной загрузки диска С: либо замещающие её, выполняя с момента заражения и её, и свои функции. Эти вирусы попадают на машину при загрузке с инфицированной дискеты. Когда считывается и запускается программа начальной загрузки, вирус загружается в память и инфицирует всё, для чего он “предназначен”.

Бутовые вирусы главной загрузочной записи. Инфицируют главную загрузочную запись системы (Master Boot Record) на жестких дисках и сектор начальной загрузки на дискетах. Этот тип вируса берет контроль над системой на самом низком уровне, перехватывая инструкции между аппаратными средствами компьютера и операционной системой.

1. Макровирусы: в некоторых компьютерных программах используются макроязыки, которые позволяют автоматизировать часто выполняемые процедуры. Поскольку компьютеры стали более мощными, решаемые задачи усложняются. Некоторые макроязыки дают возможность записывать файлы форматов, отличных от оригинального документа. Эта особенность может использоваться авторами вирусов для создания макрокоманд, которые инфицируют документы. Макровирусы обычно распространяются через файлы Microsoft Word и Excel.

2. Комбинированные вирусы: вирусы, проявляющие комбинацию перечисленных выше свойств. Они могут инфицировать и файлы, и сектора начальной загрузки, и главные загрузочные записи.

3. Файловые вирусы: рассмотрим теперь схему работы простого файлового вируса. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы совсем не обязательно резидентны. Рассмотрено схему функционирования нерезидентного файлового вируса. Пусть у нас имеется инфицированный исполняемый файл. При запуске

такого файла вирус получает управление, производит некоторые действия и передает управление «хозяину»

Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса. Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла. Заражая исполняемый файл, вирус всегда изменяет его код - следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

- он не обязан менять длину файла;
- неиспользуемые участки кода;
- не обязан менять начало файла.

Наконец, к файловым вирусам часто относят вирусы, которые «имеют некоторое отношение к файлам», но не обязаны внедряться в их код. Таким образом, при запуске любого файла вирус получает управление (операционная система запускает его сама), резидентно устанавливается в память и передает управление вызванному файлу.

1. Загрузочно-файловые вирусы: мы не станем рассматривать модель загрузочно-файлового вируса, ибо никакой новой информации вы при этом не узнаете. Но здесь представляется удобный случай кратко обсудить крайне «популярный» в последнее время загрузочно-файловый вирус One Half, заражающий главный загрузочный сектор (MBR) и исполняемые файлы. Основное разрушительное действие - шифрование секторов винчестера. При каждом запуске вирус шифрует очередную порцию секторов, а, зашифровав половину жесткого диска, радостно сообщает об этом. Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить

вирус из MBR и файлов, надо расшифровать зашифрованную им информацию.

2. Полиморфные вирусы: Большинство вопросов связано с термином «полиморфный вирус». Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Объясним же, что это такое.

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку «по ходу дела», может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Стелс-вирусы: В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или

системную область диска, он на ходу подменяет читаемые данные, как будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

Троянские кони, программные закладки и сетевые черви: Троянский конь - это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы - вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в компьютерных сетях, - взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Компьютерные вирусы распространяются по многим принципам, однако существуют все же наиболее распространенные:

- электронная почта с вложениями. Это просто: можно что-либо прикрепить к отправляемому сообщению. Этим и пользуются распространители вирусов. Нередко люди из любопытства открывают входящее сообщение, после чего начинаются проблемы. Мера предосторожности проста: если вам неизвестно, от кого пришла данная почта, и что может быть во вложении, просто не открывайте его, а сразу удалите. Такие меры могут показаться радикальными, но на самом деле они являются самыми разумными в подобной ситуации.
- просмотр сайтов. Как известно, существуют сайты целевой аудиторией которых являются в основном взрослые. Эти сайты по сути своей являются

ненадежными, а также нередко распространяют компьютерные вирусы. Также к ненадежным сайтам можно отнести игровые и сайты со взломанным программным обеспечением. При их посещении очень легко получить компьютерный вирус[3]. Мошенники специально создают такие сайты для получения доступа к компьютерам пользователей. Однако если вы не хотите попасться, лучше всего изменить настройки антивирусной программы так, чтобы ни одно внешнее соединение не могло быть установлено без вашего участия, а также чтобы ни одна программа не была установлена на ваш ПК без вашего ведома.

Сеть В случае, если компьютер подключен к домашней сети, либо же является частью крупной сети, можно легко получить вирус не по своей вине. Один из участников сети получает вирус и уже через несколько минут является распространителем этого вируса.

Фишинг. Потеря данных в результате фишинга это нередкое явление, но при этом легко заразить компьютер вирусами. При посещении фальшивых сайтов, программы шпионы часто автоматически устанавливают вирусы на компьютеры. В случае возникновения подозрений лучше всего сразу позвонить в банк и проверить, все ли в порядке, а не нажимать сомнительные ссылки.

Программное обеспечение с вирусами схема проста - пользователь скачивает программное обеспечение, которое заражено вирусом. Так он попадает на компьютер. Благодаря тому, что сегодня в сети Интернет можно скачать практически все, вирусы получают очень широкое распространение, так как платить за программное обеспечение никто не хочет.

1.2. Основные каналы распространения вирусов и вредоносных программ

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

- сканирование файлов для поиска известных вирусов, соответствующих

определению в антивирусных базах.

- обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Обычно, все ниже перечисленные методы, вместе редко используются в одной антивирусной программе. Но более тонкая спецификация антивирусов позволяет им более надежно защититься от определенных видов угроз, если ее учитывать.

Рассмотрено возможности, которые предоставляют нам большинство антивирусных программ:

- обнаружение, основанное на сигнатурах. Антивирусная программа, анализируя файл, обращается к антивирусным базам;
- метод обнаружения аномалий. Наблюдаются определённые действия (работа программ/процессов, сетевой трафик, работа пользователя) в поисках необычных событий и тенденций;
- обнаружение, основанное на эмуляции.

Эмулируется исполнение файлов, с целью выявления тех признаков вредоносного кода, которые появляются только во время исполнения программы.

Метод «Белого списка»

Эта технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены как безопасные.

Эвристический анализ

Эвристическое сканирование схоже с сигнатурным, однако, в отличие от него, ищется не точное совпадение с записью в сигнатуре, а допускается расхождение.

HIPS

Система мониторинга всех приложений, работающих в системе, с чётким разделением прав для разных приложений.

Ревизоры изменений

Эта технология защиты основана на том факте, что вирусы могут

создавать новые или внедряться в уже существующие объекты, таким образом оставляя следы в файловой системе, которые затем можно отследить и выявить факт присутствия вредоносной программы.

Монитор доступа к файлам и реестру

Предоставляет ясную картину текущей файловой и реестровой активности и становится отличным подспорьем продвинутым пользователям. Можно наблюдать за любым активным процессом, видеть его расположение и время выполнения, а также отслеживать изменения реестра и, «в случае чего», мгновенно реагировать. Внутренняя защита (самозащита) + защита конфигурации паролем. Делает невозможным выключение антивируса кем-либо, кроме авторизованного пользователя программы. Защищает от попыток выключения антивируса вредоносными программами.

Контроль доступа приложений к сети (сетевой экран)

Осуществляет контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

- Почтовый Антивирус + Антиспам

Проверка почтовых сообщений.

- IM-антивирус

Защищает информацию, поступающую по протоколам интернет-пейджеров.

- Антируткиты

Обнаруживают в системе присутствие руткитов и удаляют их.

- Детектор клавиатурных шпионов

Выявляют кейлогеры.

- Анализатор открытых портов TCP/UDP

Анализатор опирается на обновляемую базу портов известных Trojan/Backdoor программ и известных системных сервисов.

- Анти-фишинг

Веб-адреса проверяются на принадлежность к спискам фишинговых и подозрительных адресов.

- Анти-баннер

Блокирует рекламную информацию.

- Безопасная среда (sandbox)

Позволяет запускать приложения в безопасном для системы окружении.

Недостатки антивирусных программ:

- ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов;
- антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %;
- антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания);
- антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.

Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми, антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Разновидности антивирусных программ

Антивирусные программы развивались параллельно с эволюцией вирусов. По мере того как появлялись новые технологии создания вирусов, усложнялся и математический аппарат, который использовался в разработке антивирусов.

Первые антивирусные алгоритмы строились на основе сравнения с эталоном. Речь идет о программах, в которых вирус определяется

классическим ядром по некоторой маске. Смысл алгоритма заключается в использовании статистических методов. Маска должна быть, с одной стороны, маленькой, чтобы объем файла был приемлемых размеров, а с другой - достаточно большой, чтобы избежать ложных срабатываний (когда "свой" воспринимается как "чужой", и наоборот).

Первые антивирусные программы, построенные по этому принципу (так называемые сканеры-полифаги), знали некоторое количество вирусов и умели их лечить[4]. Создавались эти программы следующим образом: разработчик, получив код вируса (код вируса поначалу был статичен), составлял по этому коду уникальную маску (последовательность 10-15 байт) и вносил ее в базу данных антивирусной программы. Антивирусная программа сканировала файлы и, если находила данную последовательность байтов, делала заключение о том, что файл инфицирован. Описанные подходы использовались большинством антивирусных программ вплоть до середины 90-х годов, когда появились первые полиморфные вирусы, которые изменяли свое тело по непредсказуемым заранее алгоритмам. Тогда сигнатурный метод был дополнен так называемым эмулятором процессора, позволяющим находить шифрующиеся и полиморфные вирусы, не имеющие в явном виде постоянной сигнатуры.

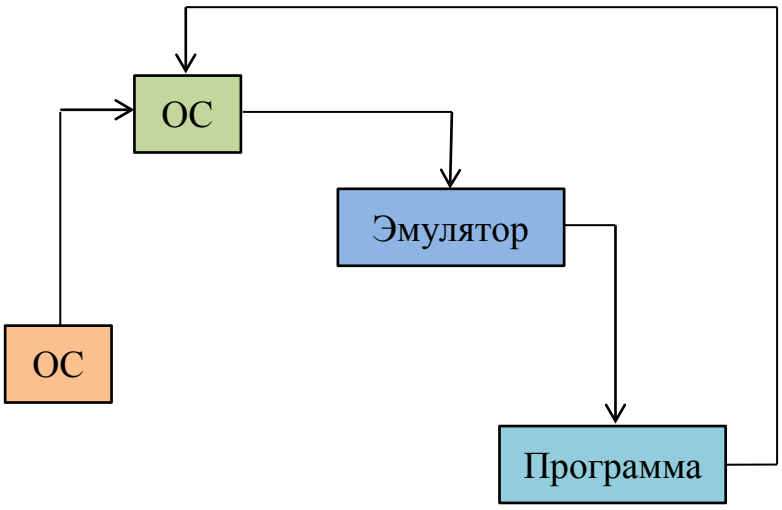


Рис.1.1. Схема работы эмулятора процессора

Принцип эмуляции процессора демонстрируется на рис.1.1. Если

обычно условная цепочка состоит из трех основных элементов: ЦПУ®ОС®Программа, то при эмуляции процессора в такую цепочку добавляется эмулятор. Эмулятор как бы воспроизводит работу программы в некотором виртуальном пространстве и реконструирует ее оригинальное содержимое. Эмулятор всегда способен прервать выполнение программы, контролирует ее действия, не давая ничего испортить, и вызывает антивирусное сканирующее ядро.

Второй механизм, появившийся в середине 90-х годов и использующийся всеми антивирусами, - это эвристический анализ. Дело в том, что аппарат эмуляции процессора, который позволяет получить выжимку действий, совершаемых анализируемой программой, не всегда дает возможность осуществлять поиск по этим действиям, но позволяет произвести некоторый анализ и выдвинуть гипотезу типа "вирус или не вирус?".

В данном случае принятие решения основывается на статистических подходах. А соответствующая программа называется эвристическим анализатором.

Для того чтобы размножаться, вирус должен совершать какие-либо конкретные действия: копирование в память, запись в сектора и т.д. Эвристический анализатор (он является частью антивирусного ядра) содержит список таких действий, просматривает выполняемый код программы, определяет, что она делает, и на основе этого принимает решение, является данная программа вирусом или нет.

При этом процент пропуска вируса, даже неизвестного антивирусной программе, очень мал. Данная технология сейчас широко используется во всех антивирусных программах.

Классификация антивирусных программ

Классифицируются антивирусные программы на чистые антивирусы и антивирусы двойного назначения (рис.1.2).

Рис.1.2. Схема классификации антивирусных программ

Чистые антивирусы отличаются наличием антивирусного ядра, которое выполняет функцию сканирования по образцам. Принципиальным в этом случае является то, что возможно лечение, если известен вирус. Чистые антивирусы, в свою очередь, по типу доступа к файлам подразделяются на две категории: осуществляющие контроль по доступу (on access) или по требованию пользователя (on demand). Обычно on access-продукты называют мониторами, а on demand-продукты - сканерами.

On demand-продукт работает по следующей схеме: пользователь хочет что-либо проверить и выдает запрос (demand), после чего осуществляется проверка. On access-продукт - это резидентная программа, которая

отслеживает доступ и в момент доступа осуществляет проверку.

Кроме того, антивирусные программы, так же как и вирусы, можно разделить в зависимости от платформы, внутри которой данный антивирус работает.

Программы двойного назначения - это программы, используемые как в антивирусах, так и в ПО, которое антивирусом не является. Например, CRC-checker - ревизор изменений на основе контрольных сумм - может использоваться не только для ловли вирусов. Разновидностью программ двойного назначения являются поведенческие блокираторы, которые анализируют поведение других программ и при обнаружении подозрительных действий блокируют их. От классического антивируса с антивирусным ядром, распознающего и лечащего от вирусов, которые анализировались в лаборатории и которым был прописан алгоритм лечения, поведенческие блокираторы отличаются тем, что лечить от вирусов они не умеют, поскольку ничего о них не знают. Данное свойство блокираторов позволяет им работать с любыми вирусами, в том числе и с неизвестными. Это сегодня приобретает особую актуальность, поскольку распространители вирусов и антивирусов используют одни и те же каналы передачи данных, то есть Интернет. При этом антивирусной компании всегда нужно время на то, чтобы получить сам вирус, проанализировать его и написать соответствующие лечебные модули. Программы из группы двойного назначения как раз и позволяют блокировать распространение вируса до того момента, пока компания не напишет лечебный модуль.

1.3. Методы проникновения вредоносных программ

Троянские программы распространяются множеством способов. Рассмотрены некоторые из них:

Наиболее популярным способом распространения троянских программ является передача информации между друзьями, при этом пользователи не

догадываются об опасности программ. Доверять программам, полученным от друзей, можно только в том случае, если пользователь уверен в их сознательном отношении к безопасности своего компьютера.

Сообщения Usenet. Usenet - компьютерная сеть, используемая для общения и публикации файлов. Многие пользователи запустят программу злоумышленника, просто послав сообщение в группу новостей Usenet. Иногда сообщение Usenet содержит ссылку на Web-страницу, с которой можно скачать программу, что даёт злоумышленнику дополнительное преимущество, так как он может видеть IP-адрес любого пользователя, загрузившего троянскую программу, что в дальнейшем позволит быстрее найти взломанный компьютер.

Исправление недостатков существующих программ. Когда в программе, например, на FTP-сервере, обнаруживается ошибка, в различные группы новостей и списки рассылки поступает множество сообщений по данной тематике. Злоумышленники могут сообщить об исправлении недостатка и предложить собственное решение, которое на самом деле не устраняет проблему или даже пробивает в системе новую брешь. Даже эксперты, которые видят, что ошибка не исправлена, могут предположить, что приславший решение злоумышленник, просто недостаточно хороший программист, и не обратить внимание на присутствие негативного эффекта запуска программы.

Реклама по электронной почте. Некоторые злоумышленники отправляют троянские программы большому количеству адресатов, надеясь на то, что хоть кто-нибудь запустит программу. Многие пользователи обычно из тех, которые не задумываясь инсталлируют и запустят или, по крайней мере, протестируют все, что покажется им интересным.

Проверки системы безопасности. Как и в случае ложного исправления недостатков программ, злоумышленники часто рассылают троянские программы, которые, как они заявляют, помогут найти уязвимые места системы по отношению к самым последним обнаруженным

недостаткам. В действительности, предоставленная программа создаёт новую брешь в системе защиты[5]. Нередко, злоумышленник указывает, что для правильной проверки уязвимых мест программа должна быть запущена с правами root.

Программы взлома системы безопасности. После обнаружения нового уязвимого места определённой программы, часто на сайтах можно получить программу атаки, которая позволяет взломать компьютер с помощью обнаруженного недостатка. Эти программы могут применять системные администраторы, чтобы проверить справедливость утверждения, но чаще они используются злоумышленниками-новичками, которые не в состоянии самостоятельно создать собственные программы атаки. Часто злоумышленник дает ссылку на программный код, как бы предназначенный для выполнения удаленной атаки. На самом деле этот код взламывает компьютер, с которого запускается данная программа атаки. На такую уловку обычно попадаются только те пользователи, которые хотят получить несанкционированный доступ к чужим компьютерам.

Обоснование выбора данного типа атак. Некоторые троянские программы просто разрушительны; они предназначены для уничтожения систем или данных. Одним из примеров чисто разрушительной программы-троянца была программа для записи CD-ROM, DVD-ROM доступная в Internet пару лет назад и обещавшая огромные функциональные возможности. Она будто бы конвертировала стандартный читающий привод компакт-дисков (используемых для установки программного обеспечения или проигрывания музыки) в привод.

Согласно файлу README, распространявшемуся с таким, очевидно фантастическим, инструментом, можно было создавать собственные музыкальные компакт-диски или делать резервное копирование системы при помощи всего лишь бесплатного обновления программы. В этой поразительной сделке имелись всего две подозрительные вещи. Во-первых, такое просто физически невозможно сделать в программе. Во-вторых, этот

инструмент был троянским конем, который стирал все содержимое жестких дисков пользователей. Многие люди загрузили его и в результате потеряли все свои данные.

Некоторые троянцы просто разрушают систему, другие позволяют атакующему похищать данные или даже управлять системами дистанционно. Опасность троянских программ заключается в сборе чужих персональных данных (паролей, кодов, номеров счетов и т.п.) и отправке их своему автору, отключении некоторые функции системы безопасности, маскировке под другие процессы. Некоторые троянские программы могут самостоятельно скачивать из Internet дополнительные программы (например, другие троянские программы), использовании для связи с злоумышленником порты, открытые другими приложениями. При обнаружении доступа в Интернет серверная часть трояна сообщает клиентской части IP адрес пораженного компьютера и порт для прослушивания.

Банковские трояны, предназначенные для кражи финансовой информации, стремительно развиваются. Один из последних экземпляров, троян StealAll. A, предназначен для кражи информации, вводимой пользователями в онлайновых формах.

Исходя из этого можно сделать вывод, что троянские программы имеют множество различных модификаций и опасны как для компьютеров обычных пользователей, так и для компьютерных сетей предприятий.

Способы обнаружения троянских программ без использования специальных средств

Троянские программы установлены на огромном количестве компьютеров, причем работающие на них пользователи даже не догадываются об этом. Большинство троянских программ не афиширует своего присутствия на компьютере пользователя, однако предположить, что компьютер заражен, можно по ряду косвенных признаков:

- отказ работы одной либо нескольких программ, особенно антивируса и брандмауэра;

- появление всплывающих окон, содержащих рекламу;
- периодическое появление окна dial-up-соединения с попытками соединиться с провайдером либо вообще с неизвестным номером;
- при отсутствии активности пользователя на подключенном к Интернету компьютере (пользователь ничего не скачивает, программы общений неактивны и т.д.) индикаторы подключения к сети продолжают показывать обмен информацией;
- стартовая страница браузера постоянно меняется, а страница, указанная в роли стартовой, не сохраняется;
- при попытке посетить сайты, куда раньше пользователь легко заходил (например, в поисковые системы), компьютер переадресовывает пользователя на незнакомый сайт, часто содержащий порнографическую либо рекламную информацию.

Если троян не умеет скрывать свой процесс, то он виден через стандартный диспетчер задач.

Чаще всего цель трояна - через сеть переслать какую-либо ценную информацию, поэтому необходимо отслеживать подозрительные сетевые соединения.

Обнаружить троянскую программу можно и с помощью программных и аппаратных средств.

1.4. Комплексная антивирусная защита локальной сети

На сегодняшний день нет необходимости доказывать необходимость построения антивирусной защиты любой информационной системы. По оценкам западных аналитиков общемировой ущерб от проникновения вирусов, червей, троянских и других вредоносных программ составляет от 8 до 12 миллиардов долларов. Достаточно вспомнить последние эпидемии, охватившие весь мир (I-Worm.LoveLetter, I-Worm.Nimda, I-Worm.Klez). При этом вирусная опасность с каждым годом растёт всё больше и больше.

Объясняется это, с одной стороны возрастающим количеством и разнообразием компьютерной инфекции, а с другой - уязвимостью локальных сетей, за счёт проникновения в них вирусов из внешний сетей, в том числе по каналам электронной почты сети Internet.

Но, тем не менее, на практике антивирусной защите не уделяется должного внимания. Даже разработчики комплексных систем информационной безопасности часто ограничиваются рекомендациями по выбору антивирусного пакета, а также оказывают помощь в его настройке.

Опасность заражения вычислительных сетей реальна для любого предприятия, но реальное развитие вирусная эпидемия может получить в локальных сетях крупных хозяйственно-производственных комплексов с территориально-развлетвлённой инфраструктурой. Их вычислительные сети, как правило, создавались поэтапно, с использованием различного аппаратного и программного обеспечения. Очевидно, что для таких предприятий вопрос антивирусной защиты становится весьма сложным, причём не только в техническом, но и в финансовом плане.

Вместе с тем решение этого вопроса достигается путём сочетания организационных мер и программно-технических решений. Данный подход не требует больших технических и немедленных финансовых затрат, и может быть применён для комплексной антивирусной защиты локальной сети любого предприятия.

В основу построения такой системы антивирусной защиты могут быть положены следующие принципы:

- принцип реализации единой технической политики при обосновании выбора антивирусных продуктов для различных сегментов локальной сети;
- принцип полноты охвата системой антивирусной защиты всей локальной сети организации;
- принцип непрерывности контроля локальной сети предприятия, для своевременного обнаружения компьютерной инфекции;
- принцип централизованного управления антивирусной защитой.

Принцип реализации единой технической политики предусматривает использование во всех сегментах локальной сети только антивирусного ПО, рекомендуемого подразделением антивирусной защиты предприятия. Эта политика носит долгосрочный характер, утверждается руководством предприятия и является основой для целевого и долговременного планирования затрат на приобретение антивирусных программных продуктов и их дальнейшее обновление.

Принцип полноты охвата системой антивирусной защиты локальной сети предусматривает постепенной внедрение в сеть программных средств антивирусной защиты до полного насыщения в сочетании с организационно-режимными мерами защиты информации.

Принцип непрерывности контроля за антивирусным состоянием локальной сети подразумевает такую организацию ее защиты, при которой обеспечивается постоянная возможность отслеживания состояния сети для выявления вирусов.

Принцип централизованного управления антивирусной защитой предусматривает управление системой из одной органа с использованием технических и программных средств. Именно этот орган организует централизованный контроль в сети, получает данные контроля или доклады пользователей со своих рабочих мест об обнаружении вирусов и обеспечивает внедрение принятых решений по управлению системой антивирусной защиты.

С учётом этих принципов в комплексной системе информационной безопасности создаётся подразделение антивирусной защиты, которая должна решать следующие задачи:

- приобретение, установка и своевременная замена антивирусных пакетов на серверах и рабочих станциях пользователей;
- контроль правильности применения антивирусного ПО пользователями;

- обнаружение вирусов в локальной сети, их оперативное лечение, удаление зараженных объектов, локализация зараженных участков сети;
- своевременное оповещение пользователей об обнаруженных или возможных вирусах, их признаках и характеристиках.

Для решения этих задач в комплексной системе информационной безопасности кроме администраторов информационной безопасности создаются администраторы антивирусной защиты. Если ЛВС небольшая или достаточно хорошо оснащена антивирусным ПО, то назначение специального администратора антивирусной защиты чаще всего нецелесообразно, так как его функции может выполнять администратор безопасности сети[6].

Для организации функционирования антивирусной защиты необходима разработка внутренних организационно-распорядительных документов. Кроме того, должны быть определены порядки передачи сообщений о вирусах от пользователей и оповещений администраторов о фактах и возможностях вирусных заражений локальной сети.

Эффективность создаваемой подсистемы антивирусной защиты зависит также от выполнения следующих дополнительных условий:

- подключение ПК пользователей в корпоративную сеть должно производиться только по заявке с отметкой администратора антивирусной защиты об установке лицензионного антивирусного ПО (заявка заносится в базу данных с фиксацией сроков действия лицензии);
- передачу ПК от одного пользователя другому необходимо производить с переоформлением подключения к сети;
- обнаруженные вирусы целесообразно исследовать на стенде подразделения защиты информации с целью выработки рекомендаций по их корректному обезвреживанию;
- в удаленных структурных подразделениях следует назначить внештатных сотрудников, ответственных за антивирусную защиту.

Практическая реализация антивирусной защиты информации на серверах и ПК корпоративной сети осуществляется с использованием ряда программно-технических методов, являющихся стандартными, но имеющих свою специфику, определяемую особенностями корпоративной сети. К ним относятся:

- использование антивирусных пакетов;
- архивирование информации;
- резервирование информации;
- ведение базы данных о вирусах и их характеристиках.

Главным методом антивирусной защиты является установка антивирусных пакетов. Выбор антивирусного ПО является одной из важнейших задач антивирусной защиты, от правильности решения которой в дальнейшем будут зависеть антивирусная безопасность системы, а также затраты на ее поддержание. Используемые антивирусные средства должны удовлетворять следующим общим требованиям:

- система должны быть совместима с операционными системами серверов и ПК;
- система антивирусной защиты не должна нарушать логику работы остальных используемых приложений;
- наличие полного набора антивирусных функций, необходимых для обеспечения антивирусного контроля и обезвреживания всех известных вирусов;
- частота обновления антивирусного ПО и гарантии поставщиков (разработчиков) в отношении его своевременности.

В отличие от других подсистем информационной безопасности в рассматриваемой области отсутствуют четко сформулированные показатели защищенности и соответствующие критерии сравнения различных антивирусных средств. Как правило антивирусные комплексы сравниваются по следующим показателям: обнаружение, лечение, блокирование, восстановление, регистрация, обеспечение целостности, обновление базы

данных компьютерных вирусов, защита антивирусных средств от доступа паролем, средства управления, гарантии проектирования, документация.

При комплексной защите локальной сети необходимо уделить внимание всем возможным точкам проникновения вирусов в сеть извне.

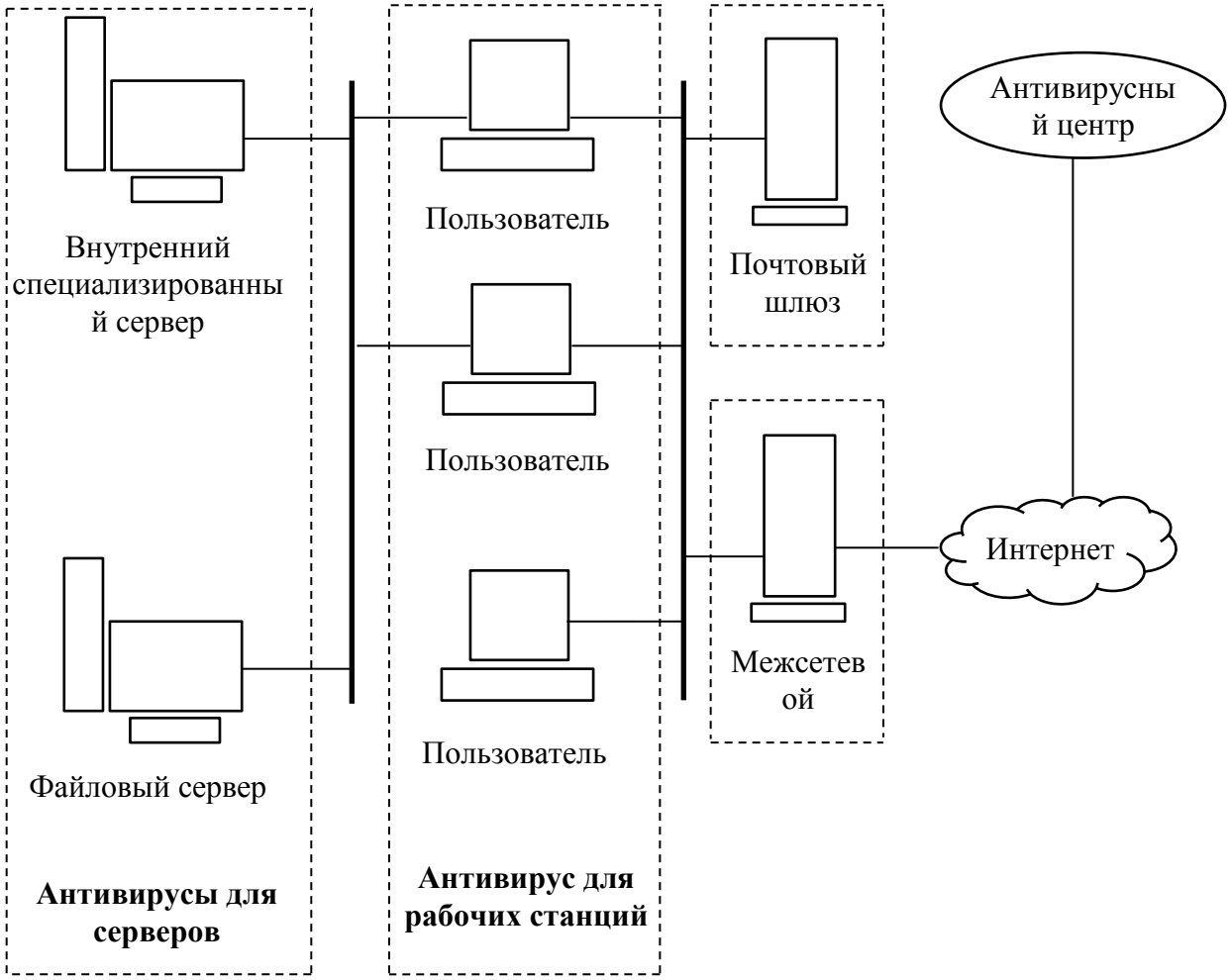


Рис.1.3. Общая структура антивирусной защиты локальной сети

На рис.1.3 приведена общая структура антивирусной защиты локальной сети. На первом уровне защищают подключение в Интернет или сеть поставщика услуг связи - это межсетевой экран и почтовые шлюзы, поскольку по статистике именно оттуда попадает около 80% вирусов. Необходимо отметить, что таким образом будет обнаружено не более 30% вирусов, так как оставшиеся 70% будут обнаружены только в процессе выполнения.

Применение антивирусов для межсетевых экранов на сегодняшний день сводится к осуществлению фильтрации доступа в Интернет при

одновременной проверке на вирусы проходящего трафика. Осуществляемая такими продуктами антивирусная проверка сильно замедляет работу и имеет крайне не высокий уровень обнаружения, по этому в отсутствии необходимости фильтрации посещаемых пользователями веб-узлов применение таких продуктов является не целесообразным.

Антивирусной защите подлежат все компоненты информационной системы, участвующие в транспортировке информации и/или её хранении:

- файл-серверы;
- рабочие станции;
- рабочие станции мобильных пользователей;
- сервера резервного копирования;
- почтовые сервера.

Как правило, использование одного (базового) антивирусного пакета для защиты локальной сети представляется наиболее целесообразным. Однако анализ рынка антивирусных средств показывает, что в случае, когда мы имеем дело с большой корпоративной сетью, это не всегда возможно вследствие разнородности применяемых в сегментах сети операционных платформ.

Следующим после выбора пакетов шагом является их тестирование администратором безопасности на специальном стенде подразделения защиты информации. Эта процедура позволяет выявить ошибки в антивирусном ПО, оценить его совместимость с системным и прикладным ПО, используемым на ПК и серверах сети. Опыт показывает, что такое тестирование оказывается далеко не лишним, поскольку разработчик не способен в полном объеме исследовать процесс функционирования своих антивирусных средств в условиях реальных сетей. Результаты тестирования направляются разработчику пакета, что позволяет тому провести необходимые доработки до начала массовой установки последнего.

Современные антивирусные пакеты содержат в себе следующие основные программные компоненты:

- монитор (резидентно размещается в оперативной памяти компьютера и автоматически проверяет объекты перед их запуском или открытием; при обнаружении вируса программа в зависимости от настроек может: удалить зараженный объект, вылечить его, запретить к нему доступ);
- сканер (осуществляет проверку объектов на наличие вирусов по запросу пользователей);
- сетевой центр управления (позволяет организовать управление АВЗ корпоративной сети: управлять компонентами пакета, задавать расписания запуска сканера, автоматического обновления антивирусных баз и т.д.);
- дополнительные модули, обеспечивающие проверку электронной почты и Web-страниц в момент получения информации.

Установку антивирусных пакетов и их настройку выполняют специалисты подразделения, осуществляющего техническое обслуживание сети. Программы «монитор» и «сканер» устанавливаются как на серверах, так и на ПК, причем первый настраивается на постоянное включение.

При обнаружении вирусов пользователям не рекомендуется заниматься "самолечением", так как это может привести к потере информации. В таких случаях им следует по "горячей линии" обращаться к администраторам антивирусной защиты, которые принимают меры по обезвреживанию вирусов и предотвращению дальнейшего заражения[7].

Следующими по важности методами антивирусной защиты являются архивирование и резервное копирование информации, позволяющие исключить потерю информации в случае вирусного заражения. Архивирование заключается в периодическом копировании системных областей машинных носителей информации на внешние устройства. На серверах с наиболее важной информацией архивирование необходимо проводить с минимальной периодичностью. Резервное копирование информации проводится ежедневно в целях защиты ее от искажения и разрушения.

Антивирусная защита локальной сети крупной организации является сложной проблемой, которая не сводится к простой установке антивирусных продуктов. Как правило, требуется создание отдельной подсистемы. В техническом плане при решении данной проблемы особое внимание следует уделить тестированию всего вновь приобретаемого антивирусного ПО, а также установке антивирусных пакетов на почтовые серверы.

2. Основная часть. Методика разработки математической модели защиты информации от вредоносных программ и компьютерных вирусов в инфокоммуникационных системах

2.1. Нахождение времени заражения локальной сети вредоносных программ и вирусов на основе сети формальных нейронов

Возможность моделирования распространения «вирусных» программ в локальной вычислительной сети вытекает из того, что каждая рабочая станция может находиться только в двух состояниях - «зараженном» и «незараженном». Построено формальную модель вычислительной сети, отражающую процесс распространения «вирусных» программ. Прежде всего сопоставит локальной сети невзвешенный граф, вершины которого представляют собой отдельные рабочие станции. Случай невзвешенного графа соответствует одноранговой сети, для рассмотрения сети с выделенным сервером необходимо ребрам графа сопоставить веса, соответствующие относительной интенсивности информационного обмена между двумя рабочими станциями.

Зараженность $i-$ой рабочей станции в момент времени t будет описывать величиной $S_i(t)$, которая может принимать два значения:

$$S_i(t) = \begin{cases} 1, & \text{если заражен;} \\ 0, & \text{иначе.} \end{cases} \qquad (2.1)$$

Каждую рабочую станцию будет представлять как формальный нейрон. При этом роль синапсов будут играть ребра графов, а величина $S_i(t) -$ характеристика аксона. Как и в других моделях, время в компьютерной сети можно рассматривать как дискретную величину, тогда состояние отдельного нейрона в момент времени t будет определяться сигналами, поступившими в предыдущий момент времени $t — 1$. Сигнал, передаваемый по синапсам, может иметь два значения $- 0$ или 1. Ноль соответствует информации, не содержащей вредоносных программ, а единица - распространению «вируса». Будем считать вирусы активными, то есть «зараженная» рабочая станция передает только «зараженную» информацию.

Наличие межсетевых экранов у рабочих станций будет выражаться величиной r_i, определяющей пороговое значение объема вредоносной информации, выше которого происходит переключение нейрона в единичное значение, что соответствует заражению рабочей станции. Однако это пороговое значение может повышаться или понижаться в результате деятельности пользователя. В результате выполнения задач, решаемых на рабочей станции, уровень защиты может как повышаться, так и понижаться. Кроме того, пользователь может инициировать процессы, которые могут «вылечивать» зараженный компьютер. Этот процесс также носит случайный характер[8]. Чтобы учесть описанные случайные процессы, в модель необходимо ввести случайную величину, воздействующую на уровень защищенности. В дальнейшем межсетевой экран в момент времени t будет записываться в виде $r_i(1-\zeta(i,t))$, где $\zeta(i,t)$ −случайная величина с нормальным распределением.

Важную роль в нейронных сетях играет функция отклика отдельного нейрона $\theta(\upsilon)$, где $\upsilon -$ сигнал, подаваемый на синапсы. Также рассмотрен простейший случай ступенчатой функции отклика:

$$\theta(\upsilon)=\begin{cases}1, & \text{если } \upsilon \geq 0;\\ 0, & \text{если } \upsilon < 0.\end{cases} \quad (2.2)$$

Таким образом, состояние рабочей станции в i −ом узле в момент времени t может быть найдено из соотношения:

$$ot_i = S_i + \sum S_j(t-1) - r_i\big(1-\zeta(i,t_{n-1})\big),$$

$$S_i(t)=\theta\left(ot_i - r_i\big(1-\zeta(i,t-1)\big)\right)=\begin{cases}1, & \text{если } ot \geq r_i\big(1-\zeta(i,t-1)\big);\\ 0, & \text{если } ot < r_i\big(1-\zeta(i,t-1)\big).\end{cases}$$

(2.3)

Здесь $ot_i -$ суммарное воздействие «вирусов» соседних узлов на i −ую рабочую станцию, суммирование производится по ближайшим соседям (индекс j пробегает номера узлов, непосредственно связанных с i −ым).

Рабочая станция переходит в зараженное состояние, если воздействие вирусов превышает порог защиты.

Введем вектор состояния системы в момент времени $V(t)$ в момент времени t в пространстве $\{0,1\}^N$, где $N-$ количество узлов сети. Координатами $V(t)$ будут величины $S_i(t)$:

$$V(t) = \big(S_1(t), S_2(t), \dots, S_N(t)\big). \qquad (2.4)$$

Обозначено через M матрицу связности графа сети, тогда эволюция системы во времени будет описываться уравнением:

$$V(t) = \ominus\,(V(t-1) + M \cdot V(t-1) - R \cdot (1 - Z(t))). \qquad (2.5)$$

Здесь $\ominus -$ ступенчатая вектор-функция, $R = (r_1, r_2, \dots, r_N)$ −вектор пороговых значений уровня защиты рабочих станций, $I -$ единичная матрица, $Z(t) -$ матрица случайных величин.

$$Z(t) = \begin{pmatrix} \zeta_1(t) & 0 \dots \dots & 0 \\ 0 & \zeta_2(t) \dots \dots & 0 \\ 0 & 0 \dots \dots & \zeta_N(t) \end{pmatrix} \qquad (2.6)$$

Для характеристики скорости заражения введем время перехода локальной сети в зараженное состояние T как минимальное время, через которое все рабочие станции оказываются «зараженными» $S_i(T) = 1, i = \overline{1, N}$.

Очевидно, что наибольшим временем заражения обладает линейная цепочка с начальным заражением крайней рабочей станции, так как в каждый момент времени может быть заражена только одна рабочая станция, и каждый узел испытывает воздействие только одного соседнего узла. Обозначено время заражения линейной цепочки через T_0. Для сетей, обладающих другой топологией, введем относительное время заражения:

$$\tau = T/T_0 \quad (7)$$

В начальный момент времени заражена только одна рабочая станция $S_1(0) = 1,\ S_2(0) = 0, \dots, S_N(0) = 0.$

А также были рассмотрены различные топологии локальных вычислительных сетей, для которых уравнение (1) решалось численно. Для

каждой топологии локальной сети время заражения вычислялось 10 раз с дальнейшим усреднением. Так, для широко распространенных топологий «кольцо» и «звезда» были получены значения $T_r = 0.5$ и $T_s = \frac{2}{N}$ при $r_i = 0.5$ для всех $i = \overline{1, N}$.

Далее был осуществлен поиск схем соединения $N = 20$ рабочих станций, обладающих наибольшим относительным временем заражения τ для одинакового порогового значения $r = 0.5$ для всех рабочих станций.

Поиск наиболее устойчивых к заражению топологий сети осуществлялся методом Монте-Карло. В качестве исходной бралась матрица связности, состоящая только из единиц. Затем применялся следующий алгоритм:

1. Изменяется выбранный случайным образом элемент матрицы.
2. Вычисляется время заражения.
3. Если, в результате такого изменения, время заражения увеличивается, то новая топология считается более выгодной и оставляется, иначе происходит возврат к прежней матрице связности.

Алгоритм выполняется до тех пор, пока изменения в матрице связности не приводят к увеличению времени заражения. При реальных расчетах вычисления прерывались, если пятьдесят подряд следующих попыток изменения матрицы отбрасывались. Вычисления показали, что наличие петель и ответвлений в линейной цепочке существенно уменьшает время заражения.

2.2. Модели распространения компьютерных вирусов на основе цепей Маркова

Компьютерные вирусы на сегодняшний день являются постоянной угрозой, представляющей опасность как для отдельных пользователей ПК, так и для предприятий. Актуальной является задача проектирования локальных сетей таким образом, чтобы сеть была максимально защищена от вирусов своей структурой. Для точной оценки защищенности сети от вирусов

необходимо иметь возможность смоделировать развитие вирусной эпидемии на выбранной конфигурации сети.

Существующие модели распространения вирусов в компьютерных сетях $(SI, SIR[1], AAWP[2], PSIDR[3])$ не учитывают структуру сети, основываясь на предположении, что сеть является полносвязным графом.

Рассмотрено локальную сеть, состоящую из N компьютеров. Каждый компьютер может находиться в одном из двух состояний - незараженный или зараженный.

Сеть можно представить в виде графа, узлами которого являются компьютеры, а дугами - каналы связи между ними, по которым могут распространяться вирусы. Вес связи w_{ij} означает вероятность перехода вируса по каналу связи между компьютерами i и j за единицу времени.

Модель на основе цепи Маркова для всей сети

Общее состояние сети является совокупностью состояний всех компьютеров сети, которое можно описать вектором из N элементов, где значение г-го элемента соответствует состоянию $i-$го компьютера: I (infected), если компьютер заражен, и S (suspected), если компьютер не заражен.

Построение матрицы переходов

Переходные вероятности вычисляются по формуле

$$P_{ij} = P\left[f^t = s^j \middle| f^{t-1} = s^i\right] \quad (2.1)$$

Сеть перейдет из состояния s_i в состояние s_j при условии, если каждый компьютер в сети перейдет из состояния s_k^i в состояние s_k^j где $k -$ номер компьютера в сети. Вероятность этого события описывается следующей формулой: $P_{ij} = P\left[f^t = s^j \middle| f^{t-1} = s^i\right] = \prod_{k=1}^{N} P\left[f_k^t = s_k^j \middle| f_k^t = s_k^i\right]$. (2.2)

Определение вероятности изменения состояния компьютера

Вероятность $P\left[f_k^t = s_k^j \middle| f_k^t = s_k^i\right]$ перехода $k-$го компьютера из состояния s_k^i в состояние s_k^j можно вычислить следующим образом.

Необходимо рассмотреть четыре варианта для различных состояний компьютера на предыдущем и следующем шаге: переход из состояния S в состояние I, из S в S, I в S, и I в I.

$S \to I$. Пусть $\mathrm{P_{зар}(k, s^i)}$ – вероятность заражения незараженного k –го компьютера из состояния сети $\mathrm{s^i}$.

$S \to S$. Поскольку событие перехода компьютера в зараженное состояние и событие, при котором незараженный компьютер останется незараженным, образуют полную группу событий, то вероятность $\mathrm{P\left[f_k^t = S \middle| f_k^{t-1} = S\right]}$ будет равна $1 - P_{\text{зар}}(k, s^i)$.

$I \to S$. Так как модель не учитывает излечения компьютера от вирусов, то переход из состояние 1 в состояние 0 невозможен, т.е. имеет нулевую вероятность.

$I \to I$. Так как модель не учитывает излечения компьютера от вирусов, то вероятность перехода из состояния 1 в состояние 1 равна единице. В результате получается следующая формула:

$$\mathrm{P\left[f_k^t = s_k^j \middle| f_k^t = s_k^i\right]} = \begin{cases} \mathrm{P_{зар}(k, s^i)}, & \text{если } \mathrm{s^i = S,\ s^j = I} \\ 0, & \text{если } \mathrm{s^i{}_k = I,\ s^j{}_k = S} \\ 1, & \text{если } \mathrm{s^i{}_k = I,\ s^j{}_k = I} \end{cases} \qquad (2.3)$$

Определение вероятности заражения компьютера

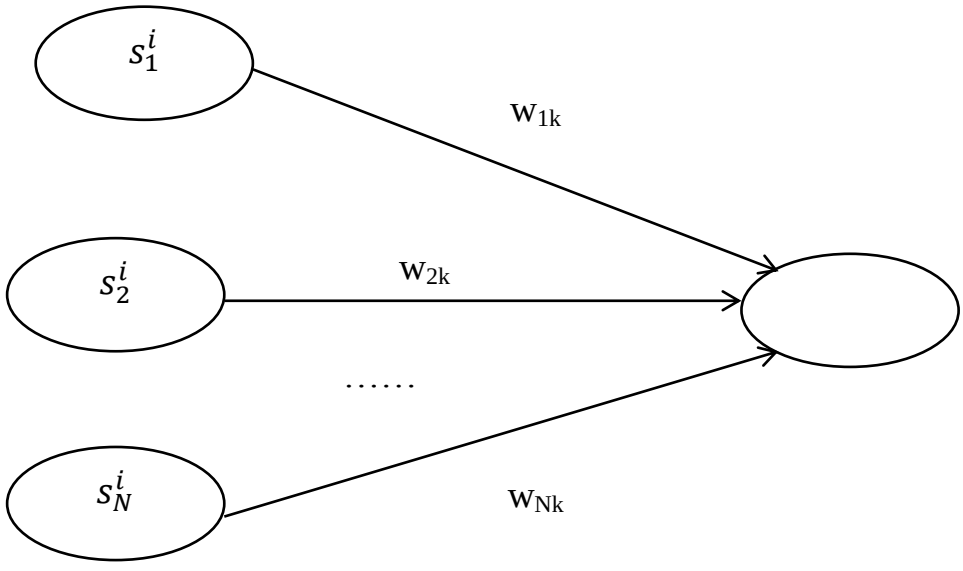


Рис.2.1. Схема заражения узла

Узел k перейдет из незараженного состояния в зараженное за единицу времени в случае, если вирус к нему поступит хотя бы с одного другого узла[9]. Поскольку события заражения k-го компьютера от различных узлов являются независимыми, то вероятность заражения незараженного k-го узла будет равна:

$$P_{зар}(k, s^i) = 1 - \prod_{m-1}^{N}(1 - P_{передачи}(m, k, s_m^i)) \qquad (2.4)$$

Вероятность передачи вируса от узла m узлу k при состоянии сети s_m^i можно вычислить следующим образом:

- если компьютер m заражен, вероятность равна w_{mk};
- если компьютер m не заражен, то вероятность передачи вируса с него равна нулю.

$$P_{передачи}(m, k, s_m^i) = \begin{cases} w_{mk}, & \text{если } s_m^i = 1 \\ 0, & \text{если } s_m^i = S \end{cases} \qquad (2.5)$$

Модель на основе цепи Маркова для отдельных узлов

Если рассматривать в виде Марковской цепи не процесс распространения вируса по всей сети, а строить отдельную Марковскую цепь для каждого узла, можно значительно сократить объем вычислений.

В каждый момент времени каждый компьютер с определенной вероятностью может быть незараженным (S), либо зараженным (I). Вектор состояния в данном случае состоит из двух элементов - вероятности того, что компьютер не заражен и вероятности того, что компьютер заражен: $P_k^t = \{P_k^t(S), P_k^t(I)\}$, где k – номер компьютера, t – номер шага.

Матрица переходных вероятностей для данного узла будет иметь следующий вид:

$$P = \begin{pmatrix} P(f^t=S)|f^{t-1}=S)|P(f^t=I)|f^{t-1}=S)| \\ P(f^t=S)|f^{t-1}=I)|P(f^t=I)|f^{t-1}=I)| \end{pmatrix} \quad (2.6)$$

Поскольку данная модель не учитывает возможность излечения, то переход из состояния *I* в состояние *S* невозможен, а из состояния *I* возможно попасть только обратно в состояние *I*, то

$$P\{(f^t = S)|f^{t-1} = I\} = 0$$

$$\mathrm{P}\{(\mathrm{f}^{\mathrm{t}} = \mathrm{I})|\mathrm{f}^{\mathrm{t}-1} = \mathrm{I}\} = 1$$

Так как сумма элементов строки матрицы переходов всегда равна единице, то

$$P[f^t = S \mid f^{t-1} = S] = 1 - P[f^t = I | f^{t-1} = \mathrm{S}]$$

Обозначим $\mathrm{P}_{\text{зар}}(\mathrm{k}) = \mathrm{P}[\mathrm{f}^{\mathrm{t}} = \mathrm{I}|\mathrm{f}^{\mathrm{t}-1} = \mathrm{S}]$, где k – это номер узла, для которого составляется модель.

Передача вируса от узла m узлу k произойдет при одновременном наступлении следующих событий:

- если компьютер m заражен на предыдущем шаге, вероятность этого события равна $\mathrm{P}_{\mathrm{k}}^{\mathrm{t}-1}(\mathrm{I})$;
- если вирус пройдет по связи $\mathrm{m} - \mathrm{k}$, вероятность этого события равна w_{mk}.

Следовательно, вероятность передачи вируса от узла m узлу k равна произведению вероятности зараженности компьютера m на предыдущем шаге, умноженной на вероятность перехода вируса по связи $m - k$:

$$\mathrm{P}_{\text{передача}}(\mathrm{m}, \mathrm{k}) = \mathrm{P}_{\mathrm{m}}^{\mathrm{t}-1}(\mathrm{I}) \cdot \mathrm{w}_{\mathrm{mk}} \qquad (2.7)$$

Как можно заметить, цепь Маркова для каждого узла является неоднородной.

Использование модели на основе цепи Маркова для всей сети

Для использования модели на основе цепи Маркова необходимо задать начальное распределение π_0 – вектор вероятностей нахождения сети в том или ином состоянии в начальный момент времени. Выбирается единственное начальное состояние сети f_0, для которого вероятность принимается равной единице, для остальных - нулю: $\pi_0 = \{p_j^0\}$, где $p_j^0 = P[\mathrm{f}_0 = s_j] = \begin{cases} 1, & \mathrm{f}_0 = s_j \\ 0, & \mathrm{f}_0 \neq s_j \end{cases}$

Исходя из теории марковских цепей, распределение на шаге t будет равно $\pi_t = \pi_{t-1} P$.

Математическое ожидание среднего числа зараженных компьютеров на шаге n можно вычислить следующим образом:

Для каждого состояния сети s_j легко определить количество зараженных компьютеров: поскольку s_j представляет собой вектор, состоящий из N элементов, то количество зараженных компьютеров для состояния s_j определяется как

$$N_t(s_j) = \sum_{i-1}^{N} \begin{cases} 1, & s_{ij} = I \\ 0, & s_{ij} \neq I \end{cases}$$

Поскольку сумма всех элементов вектора состояния на шаге t всегда равно единице, то математическое ожидание количества зараженных компьютеров будет равно

$$M[N_I^t] = \sum_{j=1}^{2^N} p_j^{(t)} \cdot N_i(s_j)$$

Проводя вычисления для $t = 0 \dots t_{max}$, получено зависимость среднего количества зараженных компьютеров от номера шага t.

Использования модели Марковских цепей для отдельных узлов

Использование модели для отдельных узлов значительно проще[10]. Начальное распределение задается для каждого узла сети: $\pi_j^0 = \{P_j^0(S), P_j^0(I)\}$, где j − номер узла. Удобнее всего выбрать в сети зараженные компьютеры, для которых вероятность нахождения в зараженном состоянии равна 1, т.е. $\pi_j^0 = \{0; 1\}$, а для остальных - наоборот $\pi_j^0 = \{1; 0\}$.

Далее для каждого шага *t* производятся следующие действия:

- для каждого j −го узла по формуле (2.7) строится матрица переходов.
- вектор начального на предыдущем шаге умножается на полученную матрицу переходов, в результате получается вектор распределения для первого шага: $\pi_j^t = \pi_j^{t-1} P$.
- имея множество векторов распределения на шаге t равно $\pi_1^t, \pi_2^t, \dots, \pi_N^t$, а следовательно, зная вероятность нахождения каждого узла в

зараженном состоянии в момент времени $t(P_j^t(I))$, можно вычислить математическое ожидание количества зараженных компьютеров на этом шаге:

$$M\lceil N_I^t \rceil = \sum_{j=1}^{N} P_j^t(I)$$

Проводя вычисления для $t = 0 \ldots t_{max}$, получим зависимость среднего количества зараженных компьютеров от номера шага t. И так были предложены модели, позволяющие рассчитывать распространение компьютерных вирусов в вычислительных сетях различной топологии. Был описан механизм их использования для получения информации о характере распространения вирусной эпидемии в сети. Использование данных моделей позволит оценить защищенность сетей различных топологий от вирусных атак.

2.3. Методика комплексной оценки антивирусных программ на основе нечетких математических моделей

На данный момент для выбора лучшего антивирусного пакета существует множество методик их тестирования. Каждая методика имеет свои плюсы и минусы. Зачастую данные методики ориентированы на конкретный продукт, поэтому остальные антивирусные пакеты остаются в заведомо проигрышном положении[11]. Многие существующие методики остаются достаточно субъективными. Более объективной может дать комплексная оценка, основанная на результатах нескольких тестов (испытаний), оценивающих антивирусные программы по различным критериям: скорость, уровень детектирования вирусов, наличие проактивной защиты и т.д. Также важно, чтобы оценки, которые будут агрегированы в ходе получения комплексной оценки были получены различными компаниями-тестерами, что позволит исключить или, по крайней мере, снизить уровень субъективности полученной комплексной оценки.

Объектом исследования при построении методики были выбраны результаты тестирования антивирусов по различным критериям, которые проводились различными компаниями: anti-malware.ru, AV-Comparatives, NSS Labs, AV-Test и т.д.

В качестве анализируемых тестов были выбраны следующие тесты:

1. Тест самозащиты антивирусов (anti-malware.ru);
2. Тест антивирусов на лечение активного заражения (anti-malware.ru);
3. Тест родительских контролей (anti-malware.ru);
4. Тест антивирусов на уровень распознавания вредоносных кодов (AV Comparatives);
5. Тестирование ложных срабатываний антивирусных программ (AV Comparatives);
6. Тест антивирусов, блокирование вредоносных программ (NSS Labs);
7. Тест антивирусов, защита уязвимостей (эксплойтов) (NSS Labs);
8. Тестирование антивирусов по критерию защиты (AV-TEST);
9. Тестирование антивирусов по критерию восстановление системы (AV-TEST);
10. Тестирование антивирусов по критерию удобство использования (AV-TEST).

Ниже привидится краткое описание исследуемых тестов.

1. **Тест самозащиты антивирусов (anti-malware.ru).** Данный тест сравнивает возможности самозащиты антивирусных программ, т.е. Самозащита антивирусных программ позволяет им выстоять в случае наиболее сложных атак, когда вредоносная программа пытается различными методами нарушить их работу, и далее удалить инфекцию штатными средствами. В данном тесте используется следующая схема начисления баллов: 1 балл начислялся, если по одному из параметров (виду атаки) самозащита продукта сработала полностью успешно. 0.5 балла - если самозащита по данному параметру частично отсутствует, но основной функционал при этом сохранился (автоматически восстановился). И,

наконец, в случае полного отсутствия самозащиты и деактивации основного функционала антивирусу не начислялось баллов вовсе. Таким образом, максимально возможное количество набранных баллов в тесте составило 76 (или по 38 для каждой ОС).

2. **Тест антивирусов на лечение активного заражения (anti-malware.ru)**. Данный тест проверяет способность антивирусных программ успешно (не нарушая работоспособность операционной систем) обнаруживать и удалять вредоносные программы, уже проникшие на компьютер, начавшие действовать и скрывающие следы своей активности. По каждому отобранному экземпляру вредоносной программы антивирусам выставлялись оценки: 1 балл - если антивирус успешно устранил активное заражение, работоспособность системы восстановлена (не нарушена), 0 баллов - если антивирус не смог устранить активное заражение или была серьезно нарушена работоспособность системы. Максимально возможно количество баллов - 16.

3. **Тест родительских контролей (anti-malware.ru)**. Цель теста проверить, насколько эффективны популярные фильтры нежелательных для детей интернет-сайтов. Данный тест ограничивается проверкой родительских контролей по эффективности блокировки сайтов только порнографической и эротической тематики. Результат теста показывает количество заблокированных сайтов из 2400 ссылок, выбранных по специальному набору популярных ключевых слов из поисковых систем Яндекс, Google и Bing (400 на русском и 400 на английском языке для каждого из трех поисковиков). Максимально возможное количество баллов - 2400.

4. **Тест антивирусов на уровень распознавания вредоносных кодов (AV Comparatives)**. Данный тесть проверяет способность антивирусных программ распознавать вредоносные коды при сканировании по запросу. В тесте использовалось 917292 вредоносные программы, среди них: троянские программы (626105), черви (123240), вирусы (21368), макровирусы (2714) и т.д. Оценка антивирусных программ по этому тесту представляет собой

количество детектированных вредоносных программ (в абсолютных величинах и в процентах). Для дальнейшего анализа будут использоваться результаты в баллах, т.е. наивысший балл - 917292.

5. **Тестирование ложных срабатываний антивирусных программ (AV Comparatives)**. В тесте оценивается количество ложных срабатываний антивирусных программ - идентификация объектов как вредоносных, хотя они таковыми не являются. Результат данного теста представлен в следующей шкале: very few (1-3 ложных срабатывания), few (4-15), many (более 15).

6. **Тест антивирусов, блокирование вредоносных программ (NSS Labs)**. Данный тест оценивает количество заблокированных сайтов, содержащих вредоносные программы, на этапе их загрузки и исполнения. При проведении тестирования использовалось 3433 сайта с различным вредоносным содержанием[12]. Количество заблокированных сайтов вычисляется в процентах, соответственно максимальный балл, который может набрать антивирусная программа, - 100%.

7. **Тест антивирусов, защита уязвимостей (эксплоитов) (NSS Labs)**. Данный тест проверяет возможности антивирусных пакетов защищать уязвимости приложений. Для проведения теста использовались 118 эксплоитов, рассчитанных на различные приложения, в том числе CVE-2010-0806 (использующий уязвимости Internet Explorer), CVE-2009-0927 (использующий Adobe Reader) и другие.

8. **Тестирование антивирусов по критерию защиты (AV-TEST).** Данный тест включает в себя статическое и динамическое обнаружение вредоносных программ, в том числе и защита от атак нулевого дня. В результате антивирусные продукты получали от 0 до 6 очков.

9. **Тестирование антивирусов по критерию восстановление системы (AV-TEST)**. Данный тест оценивает способность антивирусной программы дезинфицировать заражённую систему, т.е. уничтожать активные компоненты вредоносного ПО на этапе лечения и восстановления

зараженных компьютеров. А также обнаружить и обезвредить скрытые в системе руткиты. В результате антивирусные продукты получали от 0 до 6 очков.

10. **Тестирование антивирусов по критерию удобство использования (AV-TEST)**. Тест анализирует воздействие антивирусного продукта на производительности системы, т.е. замедление системы, вызванное антивирусом, количество ложных срабатываний во время сканирования системы, а также количество ложных сообщений и блокировок во время установки программ. В результате антивирусные продукты получали от 0 до 6 очков.

Выбранные тесты проводились в разное время и различными компаниями, поэтому состав сравниваемых антивирусных программ в них различается, а также различаются версии антивирусных пакетов. При проведении исследования версии антивирусных программ не учитывались. Также для применения методики не важна суть и алгоритм проведения испытания - получение комплексной оценки строится только на результатах, полученных в ходе испытания.

Описание методики получения комплексных оценок антивирусных программ

Получение комплексной оценки антивирусных программ на основе нечетких математических моделей включает в себя следующие этапы:

1. Выбор тестов антивирусных программ, определение их весов с помощью метода парных сравнений и выделение шкал оценок различных тестов (испытаний).

2. Выбор единой (универсальной) шкалы, формирование требований к шкале.

3. Преобразование оценок результатов тестов в оценки по выбранной универсальной шкале. Получение оценки в виде нечеткого множества, элементами которого являются варианты оценок по

универсальной шкале, соответствующей оценкам по шкале результатов тестов.

4. Получение обобщенной оценки антивирусных программ по выбранной шкале. На основе обобщенной оценки в виде нечеткого множества методом центра тяжести вычисляется итоговая оценка антивирусного пакета. Выбор тестов антивирусных программ, определение их весов и выделение шкал оценок различных тестов.

На этом этапе определяется состав тестов (испытаний), на основании которых будет получена комплексная (итоговая) оценка антивирусных программ.

Для того чтобы итоговая оценка была комплексной необходимо выбирать тесты (испытания), которые оценивают антивирусные программы по разным критериям, таким как скорость, удобство использования, уровень детектирования вирусов, проактивная защита и т.д. Для получения наиболее объективной оценки желательно выбирать тестирования, проводимые разными компаниями. Также выбранные тесты должны быть современными, т.к. параметры антивирусных программ (уровень детектирования, скорость проверки, интерфейс и т.д.) могут со временем меняться. Таким образом, желательно, чтобы выбранные тесты были проведены разными компаниями, оценивали антивирусные программы по разным критериям, были современными. Выбранные для данного исследования тесты оценивают антивирусы по различным критериям: уровень детектирования вирусов, количество ложных срабатываний, удобство использования и т.д.

Определяется коэффициенты важности (вес) каждого теста. Для определения весов выбранных тестов используется процедура их попарного сравнения, т.е. строится матрица парных сравнений тестов, в которой указываются степени превосходства тестов, далее по матрице вычисляются и нормируются средние геометрические для строк (полученные нормированные значения и будут весами тестов). После построения матрицы парных сравнений вычисляем оценку согласованности матрицы, и если

матрица не согласованная, необходимо проверить и изменить указанные степени превосходства.

Для каждого из выбранных тестов определяется шкала, в которой представлены результаты, т.е. тип шкалы и минимальная и максимальная оценки по шкале. Для построения данной методики были выбраны тесты, результаты которых представлены в виде шкал порядков и шкал отношений.

Выбор универсальной шкалы оценок антивирусных программ

Универсальная шкала должна удовлетворять следующим требованиям:

1. Шкала должна быть сильного типа, для того, чтобы при переходе к универсальной шкале не происходило потери информации (в случае если результаты тестов представлены в шкале сильного типа).

2. Для обеспечения наглядности и удобства восприятия полученного результата универсальная шкала должна быть количественной и ее максимальная оценка должна быть не слишком большой.

3. Для того чтобы при преобразовании шкал не привносить большое количество информации выбранная шкала должна иметь не слишком большое максимальное значение.

В качестве универсальной шкалы выбрана шкала отношений, минимальная оценка которой - 0, максимальная - 10.

Преобразование оценок результатов тестов в оценки по выбранной универсальной шкале. Данные, полученные в результате проведения различных тестов (испытаний), в общем случае, имеют разный логический смысл, измерены в разных шкалах и, вообще говоря, несопоставимы между собой по диапазонам значений. Поэтому для сравнения результатов различных тестов необходимо преобразование исходных шкал к универсальной шкале. Для приведения различных шкал к единому сопоставимому виду (однородному пространству признаков) может использоваться нормализация. Нормализацию часто проводят путем деления всех значений на максимально возможное значение критерия. Данная нормализация имеет ряд недостатков: во-первых, она применима только для

шкал отношений и абсолютных шкал, во-вторых, предполагается, что предпочтения равномерно возрастают, что не всегда так.

В случае преобразования шкал методом ослабления единая (универсальная) шкала будет такого же типа, как и самая слабая шкала из шкал результатов тестов или более слабого типа. Например, если результаты хотя бы одного теста будут представлены в шкале порядка, то универсальная шкала будет шкалой порядков или наименований, в таком случае может происходить потеря существенной части информации.

При преобразовании шкал методом усиления возможна обратная проблема: добавление ложной информации, это особенно важно при преобразовании очень слабой шкалы в очень сильную шкалу (например, шкалы наименований в абсолютную шкалу).

Для преобразования шкал используются нечеткие множества [4], таким образом, любой оценке (количеству баллов) в каждой из шкал тестов соответствует нечеткое множество, элементами которого являются варианты оценок выбранной универсальной шкалы (нечеткое число баллов по выбранной универсальной шкале). Таким образом, в качестве универсальной может быть использована сильная шкала, что позволяет обходиться без потерь информации (из результатов тестов с сильной шкалой) при дальнейших расчетах[13]. Но при этом привносит меньшее количество ложной информации при преобразовании результатов тестов, представленных в слабой шкале.

При преобразовании шкал в первую очередь для каждой шкалы необходимо определить коэффициенты нечеткости (разница между модой и значением, в котором функция принадлежности равна нулю). Также коэффициенты зависят от критерия, оцениваемого в тесте; например, количество детектированных вирусов оценивается объективнее, чем удобство использования, таким образом, тесту, оценивающий удобство использования соответствует больший коэффициент нечеткости. Для данной методики значения коэффициентов нечеткости выбраны от 1 до 2.

Для каждой оценки по шкале результатов тестов можно построить нечеткое множество с функцией принадлежности треугольного или трапециевидного типа(Рис.2.2).

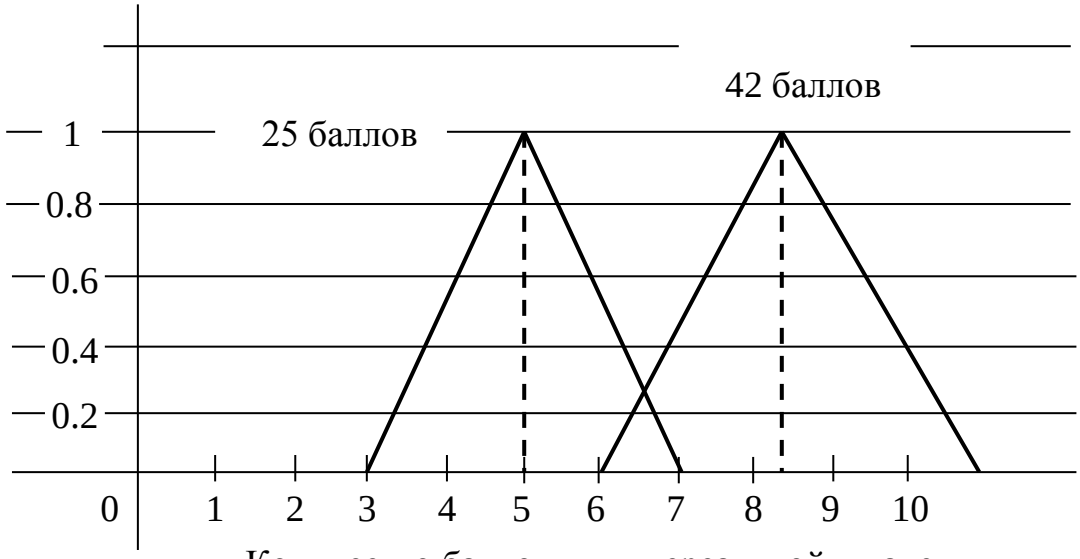


Рис.2.2. Соответствие баллов по исходной и по универсальной шкале

В связи с выбранными исходными шкалами введем следующие алгоритмы преобразования:

Для количественных шкал (шкал отношений). Оценка каждого антивируса по универсальной шкале задается с помощью моды (наиболее ожидаемого значения) и коэффициента нечеткости - параметра, характеризующего степень размытости нечеткого числа.

Наиболее вероятное значение (мода) по универсальной шкале вычисляется по формуле:

$b = \frac{K \cdot q}{K_{max}}$, если большее количество баллов соответствует лучшей оценке,

$b = q - \frac{K \cdot q}{K_{max}}$, если меньшее количество баллов соответствует лучшей оценке,

где b – мода,

q – максимальная оценка в универсальной шкале,

K – количество набранных баллов в исходной шкале,

K_{max} – максимально возможное количество баллов в исходной шкале.

Таким образом, мода - действительное число из промежутка $[0;q]$ (где q – максимальная оценка в универсальной шкале), в общем случае не целое.

Коэффициент нечеткости выбирается в соответствии с типом шкалы результатов тестов и особенностями конкретного теста[14].

Каждой оценке по шкале результатов тестов соответствует нечеткое множество, элементами которого являются варианты оценок выбранной универсальной шкалы. Для того чтобы построить это множество необходимо вычислить значение функции принадлежности для каждого варианта оценки универсальной шкалы.

Значение функции принадлежности для каждого варианта оценок универсальной шкалы вычисляется по формуле:

$$\mu(i) = \max\left\{1 - \frac{|b - i|}{k}; 0\right\},$$

где i – вариант оценки универсальной шкалы,

b– мода, вычисленная на предыдущем шаге,

k – коэффициент нечеткости. В случае если мода является целым числом, максимальное значение функции принадлежности полученного нечеткого множества равна 1. В противном случае значения функции принадлежности необходимо нормировать. Нормировка выполняется по следующей формуле:

$$\mu^*(i) = \frac{\mu(i)}{sup\,\mu\,(i)}, i \in [0; q]$$

где $\mu^*(i)$ –значение функции принадлежности для оценки i после нормирования,

$\mu^*(i)$ – значение функции принадлежности для оценки i,

q – максимально возможная оценка по универсальной шкале.

Для дальнейших вычислений будут использоваться нормированные значения функции принадлежности.

Для шкал порядка. Оценка антивирусной программы по универсальной шкале (также как и для количественных шкал) задается с помощью наиболее ожидаемого значения и коэффициента нечеткости, но в случае, если градаций по шкале порядка небольшое количество, то наиболее ожидаемое значение будет не числом, а некоторым промежутком (промежутком толерантности). В таком случае функция принадлежности имеет трапецевидную форму. Таким образом, для получения нечеткого множества необходимо задать границы толерантности и коэффициент нечеткости. Коэффициент выбирается экспертно также как и для количественных шкал, также экспертно на основании количества градаций в шкале результатов теста должна быть выбрана длина промежутка толерантности.

Для вычисления границ толерантности оценки в порядковой шкале преобразуют к оценкам от 0 до K_{max}, где K_{max} − количество градаций-1 (для шкал порядка такие преобразования допустимы). Далее вычисляют моду аналогично способу для количественных шкал.

Границы толерантности вычисляются по следующим формулам:

$$a_1 = \max\left\{b - \frac{l}{2}; 0\right\},$$

$$a_2 = \min\left\{b + \frac{l}{2}; q\right\},$$

где a_1, a_2 − левая и правая границы толерантности,

l − длина промежутка толерантности,

b − мода,

q − максимальная оценка в универсальной шкале.

Значение функции принадлежности для каждого варианта оценок универсальной шкалы вычисляется по формуле:

$$\mu(i) = \begin{cases} \max\left\{1 - \frac{|a_1 - i|}{k}; 0\right\}, i < a_1 \\ \max\left\{1 - \frac{|a_2 - i|}{k}; 0\right\}, i < a_2 \\ 1, i \in [a_1, a_2] \end{cases}$$

где $i -$ вариант оценки универсальной шкалы,

a_1, a_2 −левая и правая границы толерантности,

$k -$ коэффициент нечеткости.

Если максимальное значение функции принадлежности полученного нечеткого множества меньше 1 (это возможно в случае, если промежуток толерантности меньше 1), то полученные значения функции принадлежности необходимо нормировать.

Получение обобщенной оценки антивирусных программ по выбранной шкале. На этом этапе оценка каждой антивирусной программы по каждому из тестов представляет собой нечеткое множество, элементами которого являются варианты оценок универсальной шкалы, и максимальное значение функции принадлежности для каждого множества равно 1. Для получения обобщенной оценки используется метод аддитивной свертки. Данный метод предполагает построение интегральной оценки в виде взвешенной суммы локальных оценок. Для построения такой оценки выполнятся следующие действия:

1) значение функции принадлежности для каждой оценки умножается на коэффициент важности (вес) соответствующего теста. В результате каждому антивирусу по каждому тесту будет соответствовать нечеткое множество, состоящее из вариантов оценок универсальной шкалы, максимальное значение функции принадлежности которого равно весу соответствующего теста.

2) Значения функции принадлежности для каждого из вариантов оценок суммируются для всех тестов (по каждому из антивирусов). Таким образом, будет получено n нечетких множеств, где n −количество тестируемых антивирусов. Максимальное значение функции принадлежности для полученных оценок будет не больше 1, т.к. веса тестов нормированы, т.е. их сумма равна 1.

Таким образом, обобщенная оценка антивирусных пакетов вычисляется методом аддитивной свертки:

$$R_j = \sum_{i=1}^{n} \alpha_i R_{ij},$$

где α_i −вес i −го теста,

n −количество тестов,

R_{ij} −оценка j −ого антивирусного пакета по i −му тесту,

R_j − взвешенная оценка j −ого антивирусного пакета.

После выполнения аддитивной свертки каждой антивирусной программе соответствует обобщенная оценка по всем тестам в виде нечеткого множества, элементами которого являются варианты оценок выбранной универсальной шкалы. Для получения окончательного результата необходимо сравнить обобщенные оценки.

В качестве метода сравнения был выбран метод дефаззификации - метода центра тяжести. В таком случае, каждой антивирусной программе будет соответствовать некоторое число, которое вычисляется по формуле:

$$y = \frac{\sum_{i=1}^{n} x_i \mu(x_i)}{\sum_{i=1}^{n} \mu(x_i)},$$

где y − результат дефаззификации,

n −количество элементов множества,

x_i элемент множества,

$\mu(x_i)$ −- значение функции принадлежности.

Полученное значение является комплексной оценкой антивирусной программы. Выбор наилучшей антивирусной программы осуществляется путем поиска максимума из полученных оценок.

В проведенном эксперименте использовались результаты 10 тестов антивирусных пакетов, проведенных в 2013 году компаниями Anti-Malware, AV-Test, AV Comparative, NSS Labs. В данных тестах участвовало 30 антивирусных пакетов. По результатам проведенного эксперимента наивысшую оценку (7,51 из 10) получил антивирусный пакет Kaspersky, на втором месте F-Secure (7,25), на третьем Symantec (6,45).

2.4. Исследование алгоритма программных средств защиты компьютера от вредоносных программ

В последнее время вырос интерес к вопросам защиты информации. Это связывают с тем, что стали более широко использоваться вычислительные сети, что приводит к тому, что появляются большие возможности для несанкционированного доступа к передаваемой информации.

Выделяются различные способы защиты информации, среди них:

- физические (препятствие);
- законодательные;
- управление доступом;
- криптографическое закрытие.

Актуальность проблемы защиты информации связана с ростом возможностей вычислительной техники. Развитие средств, методов и форм автоматизации процессов обработки информации, массовость применения ПЭВМ резко повышают уязвимость информации. Основными факторами, способствующими повышению этой уязвимости, являются:

- резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью ЭВМ и других средств автоматизации;
- сосредоточение в единых базах данных информации различного назначения и различной принадлежности;
- резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;
- усложнение режимов функционирования технических средств вычислительных систем: широкое внедрение мультипрограммного режима, а также режима разделения времени;
- автоматизация межмашинного обмена информацией, в том числе и на больших расстояниях.

Общая схема, представленная на рис.2.3 позволяет представить комплексный подход к определению целостности данных в программной и аппаратной части ПЭВМ.

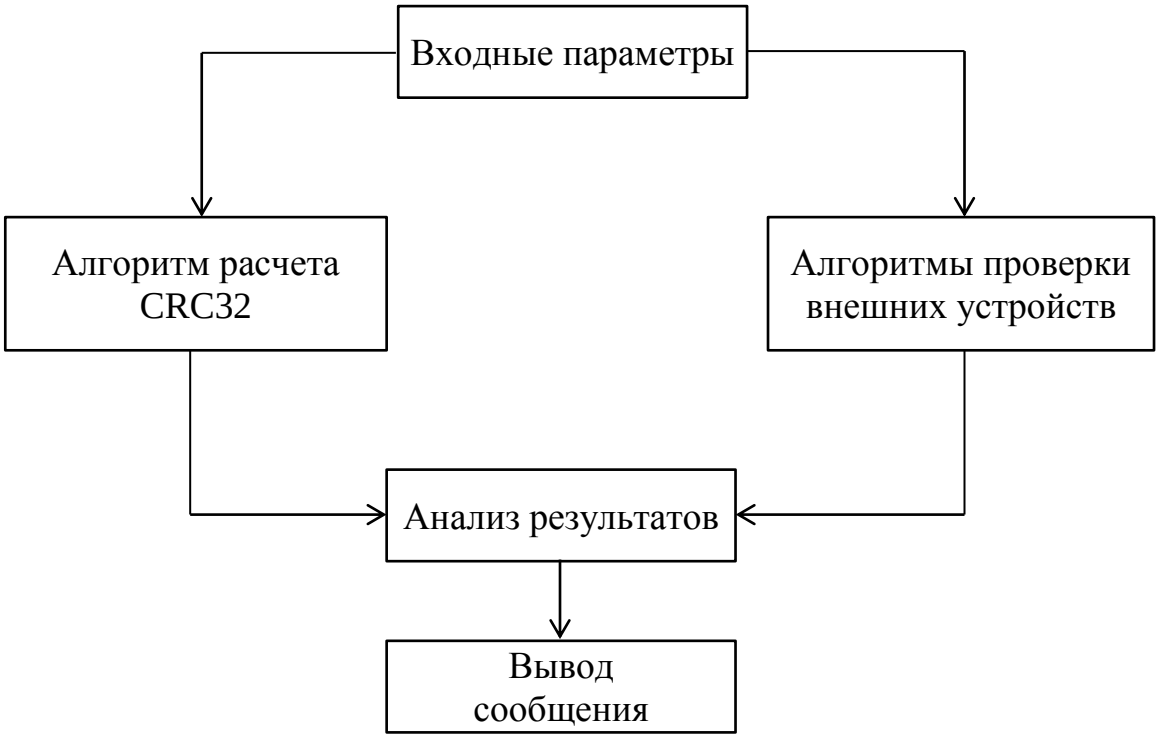


Рис.2.3. Общая схема алгоритма проверки целостности данных

1. Входные данные. Здесь под входными данными понимается как любой файл, хранящийся на жестком диске, так и внешние устройства подключенные к ПЭВМ.

2. Алгоритм расчета CRC32. Данный алгоритм позволяет отследить целостность данных в программной части персонального компьютера, а также производить их проверку через интервалы времени, выбираемые пользователем.

3. Алгоритм проверки внешних устройств. Данный алгоритм позволяет отследить изменения в аппаратной части персонального компьютера, а также производить проверку устройств через интервалы времени, выбираемые пользователем[15].

4. Анализ результатов. В данном блоке происходит сравнение эталонных данных с данными, полученными в результате работы алгоритмов.

5. Вывод сообщения. Выводится сообщение об изменении или не изменении файлов и устройств персонального компьютера, на основе чего оператор принимает решение о целостности данных системы.

Пояснено подробнее алгоритм проверки внешних устройств. Схема его приведена на Рис.2.4.

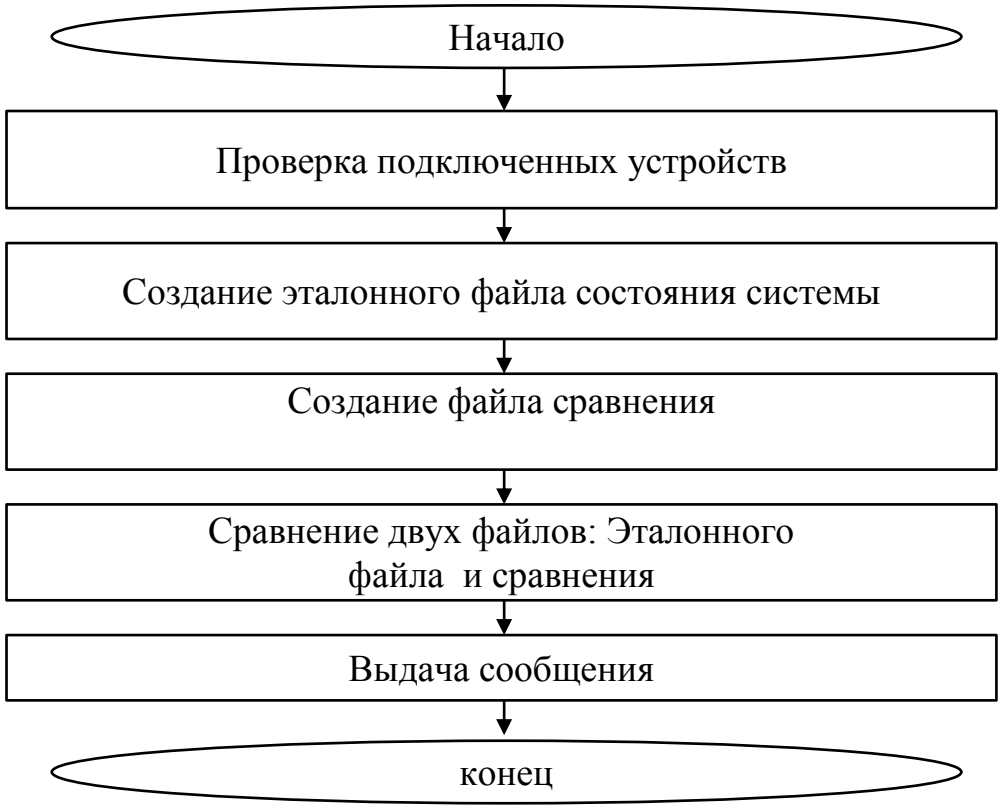


Рис.2.4. Алгоритм проверки подключенных устройств

В ней можно отметить следующие основные операции.

1. Проверка подключенных устройств. Запускается стандартная программа Windows, MSINFO32, которая содержит информацию обо всех подключенных устройствах и программном обеспечении на данном компьютере.

2. Создание эталонного файла. Из стандартной программы MSINFO32 копируется информация о всех подключенных на данный момент времени устройствах в текстовый файл, именуемый "Эталонным".

3. Создание файла сравнения. Для выяснения изменения структуры подключенных устройств по истечении некоторого времени повторяется

последовательность действий, описанных в пункте 2. За исключением того, что информация сохраняется в текстовый файл "Файл сравнения".

4. Сравнение двух файлов: эталонного и файла сравнения. В этом блоке происходит сравнение двух текстовых файлов для определения, изменялись ли устройства за прошедший интервал времени.

5. Выдача сообщения о добавлении нового устройства (или нескольких устройств) или сообщения о том, что состояние системы не изменилось.

3. Безопасность жизнедеятельности

3.1. Организация рабочего места, оснащенного компьютером

Научно-технический прогресс внес серьезные изменения в условия производственной деятельности работников умственного труда. Их труд стал более интенсивным, напряженным, требующим значительных затрат умственной, эмоциональной и физической энергии. Это потребовало комплексного решения проблем эргономики, гигиены и организации труда, регламентации режимов труда и отдыха.

В настоящее время компьютерная техника широко применяется во всех областях деятельности человека. При работе с компьютером человек подвергается воздействию ряда опасных и вредных производственных факторов: электромагнитных полей (диапазон радиочастот: ВЧ, УВЧ и СВЧ), инфракрасного и ионизирующего излучений, шума и вибрации, статического электричества и др.

Работа с компьютером характеризуется значительным умственным напряжением и нервно-эмоциональной нагрузкой операторов, высокой напряженностью зрительной работы и достаточно большой нагрузкой на мышцы рук при работе с клавиатурой ЭВМ. Большое значение имеет рациональная конструкция и расположение элементов рабочего места, что важно для поддержания оптимальной рабочей позы человека-оператора.

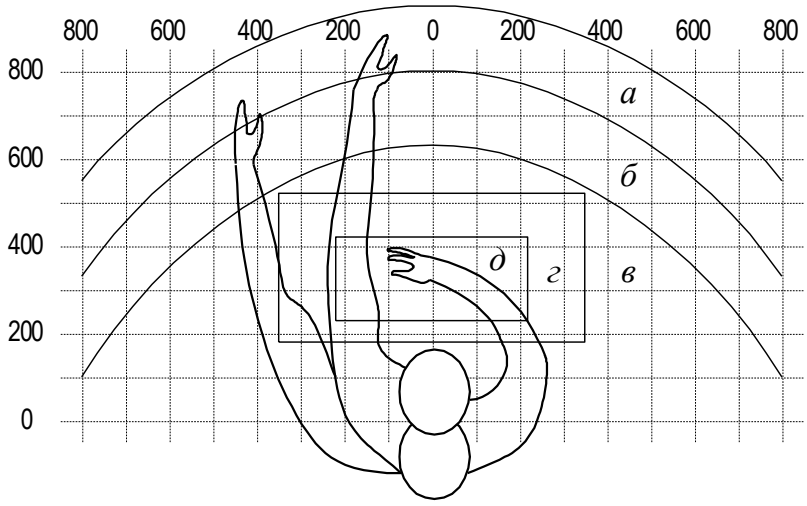
В процессе работы с компьютером необходимо соблюдать правильный режим труда и отдыха. В противном случае у персонала отмечаются значительное напряжение зрительного аппарата с появлением жалоб на неудовлетворенность работой, головные боли, раздражительность, нарушение сна, усталость и болезненные ощущения в глазах, в пояснице, в области шеи и руках[16].

Большое значение имеет также характер работы. В частности, при организации рабочего места программиста должны быть соблюдены следующие основные условия: оптимальное размещение оборудования,

входящего в состав рабочего места и достаточное рабочее пространство, позволяющее осуществлять все необходимые движения и перемещения.

Главными элементами рабочего места программиста являются стол и кресло. Основным рабочим положением является положение сидя.

Рабочая поза сидя вызывает минимальное утомление программиста. Рациональная планировка рабочего места предусматривает четкий порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства(Рис.3.1).



а - зона максимальной досягаемости;

б - зона досягаемости пальцев при вытянутой руке;

в - зона легкой досягаемости ладони;

г - оптимальное пространство для грубой ручной работы;

д - оптимальное простран-

Рис.3.1. Зоны досягаемости рук в горизонтальной плоскости.

При оборудовании рабочего места (рис.3.2) необходимо установить монитор на специальном столике так, чтобы задняя панель была обращена к стене (так как около нее зарегистрирован максимальный уровень напряженности электрического поля), экран не должен располагаться напротив окна или других прямых источников света, дающих блики на экране.

Рис.3.2. Рекомендуемое положение во время работы за компьютером

Стол, на котором устанавливается монитор, должен быть достаточной длины, чтобы расстояние до экрана составляло 60-70 (не ближе 50) см, и в то же время можно было работать с клавиатурой в непосредственной близости от пользователя (30-40 см). Конструкция рабочей мебели (столы, кресла, стулья) должна обеспечивать возможность индивидуальной регулировки соответственно росту работающего и создавать удобную позу. Часто используемые предметы труда должны находится в оптимальной рабочей зоне, на одном расстоянии от глаз работающего. На поверхности рабочего стола необходимо разместить подставку для документов, расстояние которой от глаз должно быть аналогичным расстоянию от глаз до клавиатуры. Рабочее кресло должно иметь подлокотники. На рабочем месте необходимо предусмотреть подставку для ног.

Для того чтобы устранить блики на экране, монитор должен быть установлен перпендикулярно столу, а пользователь должен смотреть на экран несколько сверху вниз (10° от горизонтальной линии) (Рис.3.2, 3.3). Условия освещенности в комнате играют большую роль в сохранении зрительного комфорта. С одной стороны, ничто не должно мешать восприятию информации с экрана, с другой - пользователь должен хорошо видеть клавиатуру, бумажные тексты, которыми приходится пользоваться, а также общую обстановку и людей, с которыми приходится общаться при работе.

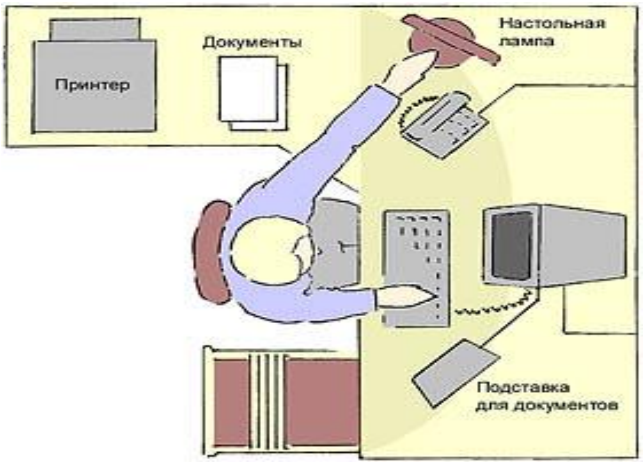
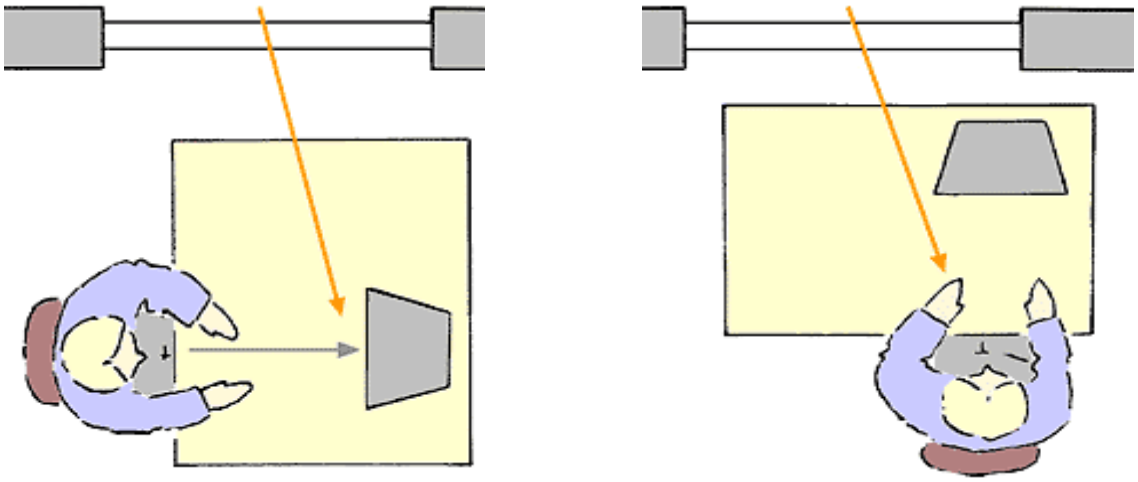


Рис.3.3. Удобное рабочее место с "Г-образным" столом

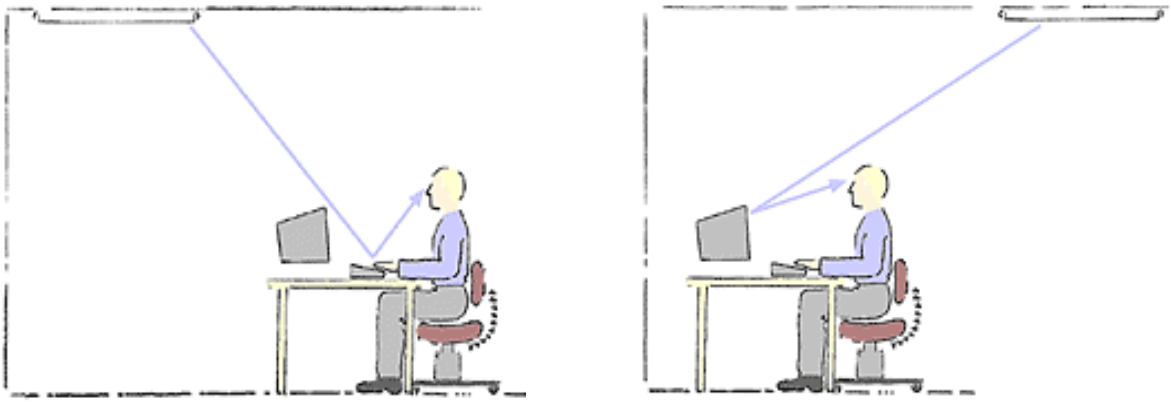
Общая освещенность в комнате не должна быть слишком большой, но и не слишком малой, она должна быть в пределах 300-500 люкс. Если помещение светлое, то окна должны иметь шторы или жалюзи. Рабочие места пользователей дисплеев желательно не располагать непосредственно у окон. Во всех случаях экран монитора следует ориентировать так, чтобы он не давал бликов, а именно - под углом к окну, близким к прямому (Рис.3.4., 3.5., 3.6.). Искусственное освещение не должно быть слишком ярким. Но помимо общих ламп, освещающих комнату, необходима местная яркая (не менее 60 Вт) лампа с хорошим плотным абажуром, освещающая только текст, с которым работает пользователь. Она должна иметь возможность ориентации в разных направлениях и быть оснащена устройством для регулирования яркости. Лампы накаливания предпочтительнее люминесцентных, т.к. последние дают пульсирующий свет, в определенных условиях усиливающий мерцание экрана дисплея.



А) Линия взора параллельна окну(рекомендуется)

Б) Яркий свет в поле зрения(не рекомендуется)

Рис.3.4. Расположение монитора относительно окна



А) Отражение света лампы от поверхности стола и клавиатуры (не рекомендуется)

Б) Блик от лампы на экране монитора (не рекомендуется)

Рис.3.5. Расположение источника искусственного освещения относительно монитора

Рис.3.6. Правильное расположение монитора относительно стены и источника света

Перед началом работы с монитором необходимо установить с помощью рукояток наиболее комфортные контрастность и яркость на экране. Они подбираются индивидуально, так как слишком низкая контрастность и высокая яркость могут приводить к быстрому утомлению.

При подборе светового режима на рабочем месте пользователя дисплея необходимо учитывать то, что у лиц после 40 лет возникают возрастные изменения в зрительной системе (сужение зрачка, пожелтение хрусталика, снижение зрительной активности и контрастной чувствительности сетчатки). Все это требует усиления яркости экрана и дополнительной освещенности рабочего места (бумажного текста). У молодых лиц при зрительно-

напряженной работе наибольшую нагрузку несет аккомодационная система глаза, которая во время работы находится в постоянном напряжении. Это может приводить к астенопическим явлениям, возникновению нарушений в аккомодационной системе глаза и, в конечном счете, к появлению и росту близорукости. Чтобы избежать этого, работа с экраном монитора должна проводиться с расстояния не менее 60-70 см, при этом напряжение аккомодации минимально.

У взрослых с близорукостью, которые постоянно носят очки, другие очки для работы с компьютером необходимы только в том случае, если в своих очках пользователь с трудом читает газетный шрифт с расстояния 60-70 см (до экрана) и 30-33 см (до печатного текста) от глаз. В случае если с одними и теми же линзами чтение с обоих расстояний невозможно, назначают бифокальные очки.

3.2. Чрезвычайные ситуации. Защита предприятия в чрезвычайных ситуациях и ликвидация последствий

Известно, что любая деятельность потенциально опасна, а сами опасности носят перманентный характер (перманентный - постоянный, непрерывно продолжающийся, от латинского permaneo - остаюсь, продолжаюсь).

Потенциальная опасность - это опасность скрытая, неопределенная во времени и пространстве. Реализуется потенциальная опасность через причины и в случае, если нежелательные последствия будут значительные, то это событие классифицируется как чрезвычайная ситуация.

Чрезвычайная ситуация (ЧС) - это обстановка на определенной территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или

окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Независимо от причин появления ЧС, в их развитии можно выделить основные пять стадий:

- *Зарождения* - возникновение условий или предпосылок для ЧС (усиление природной активности, накопление деформаций, дефектов и т.п.).
- *Инициирования* - начало ЧС. На этой стадии важен человеческий фактор, поскольку статистика свидетельствует, что до 70% техногенных аварий и катастроф происходит вследствие ошибок персонала.
- *Кульминации* - стадия высвобождения энергии или вещества. На этой стадии отмечается наибольшее негативное воздействие на человека и окружающую среду вредных и опасных факторов ЧС.
- *Затухания* - локализация ЧС и ликвидация ее прямых и косвенных последствий. Продолжительность данной стадии различна, возможны дни, месяцы, годы и десятилетия.
- *Период ликвидации* последствий.

Задачи, решаемые в ЧС. Классификация ЧС

Все ЧС можно классифицировать по трем основным принципам - масштабу распространения, темпу развития и природе происхождения.

При классификации ЧС по масштабу распространения (Рис.3.7) следует учитывать не только размеры территории, подвергнувшейся воздействию ЧС, но и возможные ее косвенные последствия[17]. К ним относятся тяжелые нарушения организационных, экономических, социальных и других существенных связей, действующих на значительных расстояниях. Кроме того, принимается во внимание тяжесть последствий, которая и при небольшой площади ЧС может быть огромной и трагичной.

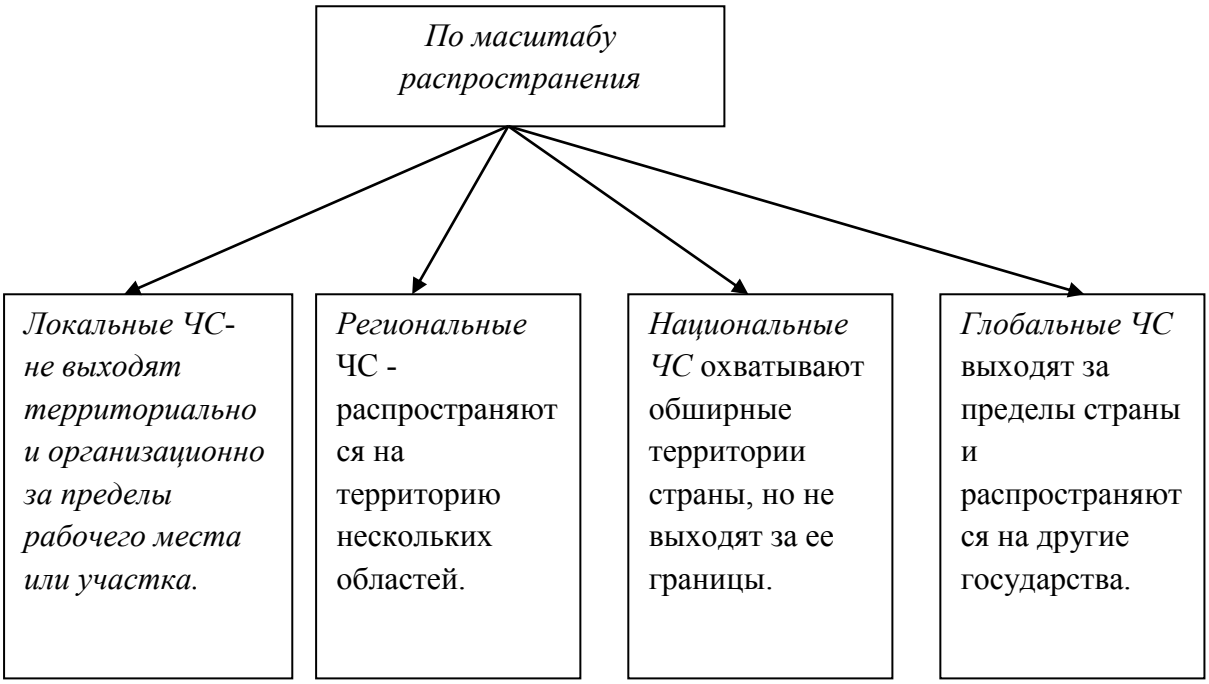


Рис.3.7. Классификация ЧС по масштабу распространения

Каждому виду ЧС свойственна своя скорость распространения опасности, являющаяся важной составляющей интенсивности протекания чрезвычайного события и характеризующая степень внезапности воздействия поражающих факторов. С этой точки зрения ЧС можно классифицировать по темпу развития(Рис.3.8).

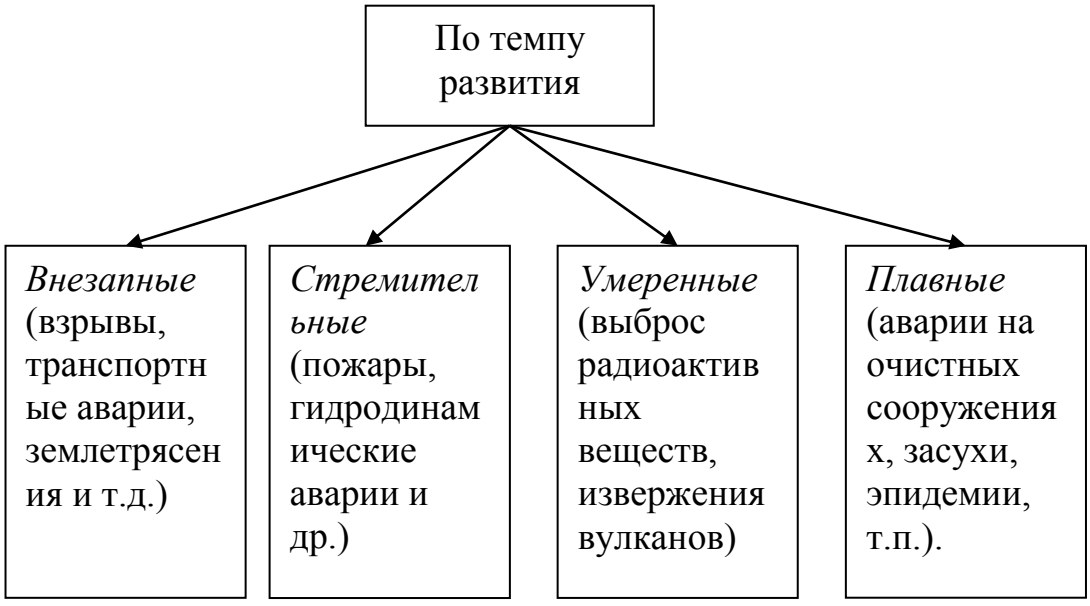


Рис.3.8. Классификация ЧС по темпу развития

Каждая ЧС имеет свои причины, в этой связи их можно классифицировать по происхождению(Рис.3.9).

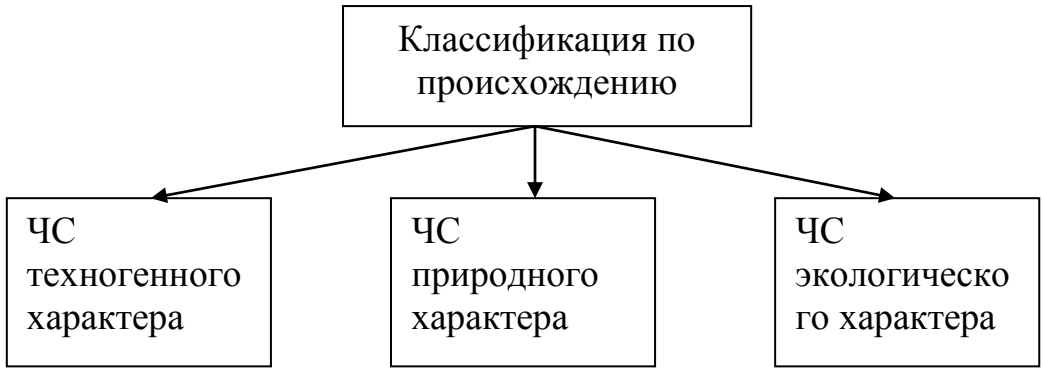


Рис.3.9. Классификация ЧС по происхождению

Планирование мероприятий по обеспечению безопасности жизнедеятельности в ЧС

В ЧС военного и мирного времени защите подлежит все население, но защищаются его отдельные группы дифференцированно. Основными способами защиты населения при ЧС в современных условиях являются:

- укрытия в защитных сооружениях, в простейших укрытиях на местности;
- рассредоточение и эвакуация населения из крупных городов в загородную зону;
- своевременное и умелое применение средств индивидуальной защиты.

Для укрытия людей заблаговременно на случай ЧС строятся защитные сооружения. Защитные сооружения подразделяются:

- по назначению (для населения или для размещения органов управления);
- по месту расположения (встроенные, отдельно стоящие, в горных выработках, метро и др.);
- по времени возведения (заблаговременно возводимые и возводимые в особый период);
- по характеру (убежища или укрытия).

Убежищем называется защитное сооружение герметичного типа, обеспечивающее защиту укрываемых в нем людей от всех поражающих факторов ядерного взрыва, отравляющих веществ, бактериальных средств, высоких температур и вредных дымов.

Убежища оборудуются всеми системами жизнеобеспечения. Система воздухоснабжения включает воздухозаборные устройства, противопылевые фильтры и фильтры-поглотители, вентиляторы, воздухорегулирующие и защитные устройства.

Отчистка воздуха осуществляется:

- в режиме чистой вентиляции, когда наружный воздух очищается только от пыли с воздухообменом 8-13 $м^3$ на человека в час;
- в режиме фильтровентиляции, когда воздух дополнительно пропускается через фильтры-поглотители для очищения от отравляющих веществ и бактериальных средств с воздухообменом не менее 2 $м^3$ на человека в час.

Регенерация воздуха осуществляется посредством соответствующих патронов. Очищенный воздух вентиляторами нагнетается по воздуховодам в отсеки убежища.

Система водоснабжения обеспечивает людей водой для питья и гигиенических нужд. Она осуществляется от наружной водопроводной сети.

Ликвидация последствий чрезвычайных ситуаций

Ликвидация ЧС включает в себя проведение в зоне происшествия и в прилегающих к ней районах силами и средствами организаций по ликвидации чрезвычайных ситуаций всех видов разведки и неотложных работ, а также организацию жизнеобеспечения пострадавшего населения и личного состава этих сил.

Ликвидация ЧС считается завершенной по окончании проведения аварийно-спасательных и других неотложных работ.

Спасательные и другие неотложные работы в очагах поражения включают:

- разведку очага поражения, в результате которой получают истинные данные о сложившейся обстановке;
- локализацию и тушение пожаров, спасение людей из горящих зданий;
- розыск и вскрытие заваленных защитных сооружений, розыск и извлечение из завалов пострадавших;
- оказание пострадавшим медицинской помощи, эвакуация пораженных в медицинские учреждения, эвакуация населения из зон возможного катастрофического воздействия (затопления, радиационного и другого заражения);
- санитарная обработка людей, обеззараживание транспорта, технических систем, зданий, сооружений и промышленных объектов;
- неотложные аварийно-восстановительные работы на промышленных объектах.

Разведка в кратчайшие сроки должна установить характер и границы разрушений и пожаров, степень радиоактивного и иного вида заражения в различных районах очага, наличие пораженных людей и их состояние, возможные пути ввода спасательных формирований и эвакуации пострадавших. По данным разведки определяют объемы работ, уточняют способы ведения спасательных и аварийных работ, разрабатывают план ликвидации последствий чрезвычайного события.

В планах ликвидации последствий намечают конкретный перечень неотложных работ, устанавливают их очередность. С учетом объемов и сроков проведения спасательных работ определяют силы и средства их выполнения. В первую очередь в плане необходимо предусматривать работы, направленные на прекращение воздействия внешнего фактора на объект (если это возможно), локализацию очага поражения, постановка средств, препятствующих распространению опасности по территории объекта.

В качестве спасательных сил используют обученные спасательные формирования, создаваемые заблаговременно, а также вновь

сформированные подразделения из числа работников промышленного объекта (подразделений гражданской обороны объекта). Спасательные формирования могут быть подчинены руководству объекта или администрации района, города, области.

В качестве технических средств используют как объектовую технику (бульдозеры, экскаваторы со сменным оборудованием, автомобили-самосвалы, автогрейдеры, моторные и прицепные катки, пневматический инструмент и т.д.), так и спецтехнику, находящуюся в распоряжении спасательных формирований (специальные подъемно-транспортные машины, корчеватели-собиратели, ручной спасательный инструмент, бетоноломы, средства контроля и жизнеобеспечения).

Заключение

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

Основные результаты ВКР могут быть сформулированы в следующем виде:

1. Отражены типы компьютерных вирусов, анализируются каналы распространения вирусов и вредоносных программ, выполняющей сканирование файлов для поиска известных вирусов и обнаружение подозрительного поведения любой из программ.

2. Описаны эвристического и сигнатурного методов анализа компьютерных вирусов и методики обнаружения вредоносных программ без использования специальных средств.

3. Рассмотрены принципы реализации единой технической политики при обосновании выбора антивирусных продуктов и охвата системой антивирусной защиты всей локальной сети организации.

4. Приведены методы защиты от вирусов. Во-первых, это межсетевые экраны, препятствующие проникновению вредоносных программ, а во-вторых, антивирусные программы, обнаруживающие «вирусы» и уничтожающие их.

5. Исследован алгоритм на основе методом Монте-Карло, позволяющий изменить выбранный случайным образом элемент матрицы и вычислить время заражения и модели распространения компьютерных вирусов на основе цепей Маркова, определяющей вероятности изменения состояния и заражения компьютера.

6. Описана методика комплексной оценки антивирусных программ на основе нечетких математических моделей, выполняющая тестировать антивирусов по различным критериям.

7. Разработан алгоритм проверки внешних устройств, позволяющий отслеживать изменения в аппаратной части компьютера.

Использованные литературы

1. Постановление Президента Республики Узбекистан «О дополнительных мерах по дальнейшему развитию информационно-коммуникационных технологий». от 21 марта 2012 года, ПП – 1730.
2. Н.Н. Безруков «Классификация компьютерных вирусов и методы защиты от них», Москва, СП "ICE", 2009 г. 238 с.
3. Безруков Н.Н. «Компьютерные вирусы», Москва, Наука, 2010. 178 с.
4. Мостовой Д.Ю. «Современные технологии борьбы с вирусами» // Мир ПК. - №8. – 2012г. 16 с.
5. Денисов Т.В. «Антивирусная защита»//Мой Компьютер-№4-2011 г. 148 с.
6. Ф.Файтс, П.Джонстон, М.Кратц «Компьютерный вирус: проблемы и прогноз», Москва, "Мир", 2011 г. 276 с.
7. Атака из Internet/И. Д. Медведовский, П.В. Семьянов, Д.Г. Леонов, А.В. Лукацкий - М.: Солон-Р, 2009. - 368 с.
8. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов.- М: Солон-Р, 2010.- 458 с.
9. Нейлор К. Как построить свою экспертную систему: Пер. С англ. - М.: Энергоатомиздат, 1991. - 286с.: ил.
10. Хатч, Брайн, Ли. Секреты хакеров. Безопасность Linux – готовые решения, 2-е издание.: Пер. С англ. - М.: Издательский дом «Вильямс», 2013. - 704 с.:ил. - Парал. Тит. Англ.
11. Анин Б.Ю. Защита компьютерной информации. - СПб.: БХВ – Санкт-Петербург, 2006. - 384 с.:ил.
12. Касперски К. Записки исследователя компьютерных вирусов. - Спб.:Питер, 2005. - 316 с.: ил.
13. Соколов А., Степанюк О. Защита от компьютерного терроризма. - Спб.: БХВ – Петербург, 2010. - 496 с.
14. **http://www.nsslabs.com/resources/blog.html**

15. **http://www.anti-malware.ru/tests**

16. Русак О.Н., Малаян К.Р., Занько Н.Г. Безопасность жизнедеятельности. Учебное пособие. Омега. С. Петербург-М.-Краснодар. 2004.

17. Субанов Б.Д., Додобаев Ю.Т. Экология и жизнедеятельность. Уч. Пособие. Ташкент. 2003.