Д/з на 25.09!!! Прочитать, написать краткий конспект!!!

«Виды профессиональной информационной деятельности человека с использованием технических средств и информационных ресурсов»

Информационная деятельность человека– это деятельность, связанная с процессами получения, преобразования, накопления и передачи информации.

Информационная деятельность человека связана с созданием знаний, которые образуют информационные ресурсы общества. К информационным ресурсам можно отнести научно-технические знания, произведения литературы и искусства, общественную и государственную информацию.

Все люди в своей жизни занимаются информационной деятельностью (получают письма, читают книги, хранят фото- и видеоархивы, разговаривают по телефону, решают задачи, разгадывают кроссворды и т. п.); для многих она является*профессиональной*.

Тысячелетиями предметами труда людей были материальные объекты. Все орудия труда от каменного топора до первой паровой машины, электромотора или токарного станка были связаны с обработкой *вещества*, использованием и преобразованием*энергии*. Вместе с тем человечеству всегда приходилось решать задачи управления, накопления, обработки и передачи информации, опыта, знания. Возникали группы людей, чья профессия связана исключительно *с информационной деятельностью*. В древности это были, например, жрецы, летописцы, затем — ученые и т.д.

По мере развития общества постоянно расширялся круг людей, чья профессиональная деятельность была связана с обработкой и накоплением информации. Постоянно рос и объем человеческих знаний, опыта, а вместе с ним количество книг, рукописей и других письменных документов. Появилась необходимость создания специальных хранилищ этих документов — *библиотек, архивов*. Информацию, содержащуюся в книгах и других документах, необходимо было не просто хранить, а упорядочивать, систематизировать. Так возникли*библиотечные классификаторы, предметные и алфавитные каталоги* и другие средства систематизации книг и документов, появились профессии *библиотекаря, архивариуса*.

В результате научно-технического прогресса человечество создавало все новые средства и способы сбора (запись звуковой информации с помощью микрофона, фотоаппарат, кинокамера), хранения (бумага, фотопленка, грампластинки, магнитная пленка), передачи информации (телефон, телеграф, радио, телевидение, спутники). Но важнейшее в информационных процессах — обработка и целенаправленное преобразование информации — осуществлялось до недавнего времени исключительно*человеком*.

Вместе с тем постоянное совершенствование техники, производства привело к резкому возрастанию объема информации, которой приходится оперировать человеку в процессе его профессиональной деятельности.

Во второй половине XX века выпуск научно-технической печатной продукции стал подобен нарастающей лавине. Ни отдельный человек, ни специальные организации, созданные для обработки поступающей информации, не могли не только освоить весь информационный поток, но и оперативно находить в нем то, что требовалось для тех или иных работ. Сложилась парадоксальная ситуация, когда для получения нужной информации легче и дешевле было провести исследования заново, чем разыскать ее в научной литературе. Информационная система, основанная на бумажных носителях, переросла свои возможности. Назрел *информационный кризис*, т. е. ситуация, когда*информационный поток так увеличился, что стал недоступен обработке в приемлемое время*.

Можно сказать, что нам, живущим на рубеже веков и тысячелетий, повезло стать свидетелями грандиозных изменений на нашей родной планете. И результатом этих изменений стало *ускорение появления знаний*. Информационный поток буквально обрушивается на нас. Если первое удвоение общего количества знаний на Земле произошло за период от рубежа нашей эры до 1750 года, то второе удвоение случилось уже за 150 лет, к началу двадцатого столетия, а третье — за 50 лет – к 1950 году.

В дальнейшем объемы знаний удваивались еще более стремительными темпами: до 1970 года — на протяжении 10 лет, после 1970 года — каждые 5 лет, а с 1991 года — ежегодно! По сути, мы живем в обществе, где могущество любой страны определяется ее информационным потенциалом и возможностью быстро обеспечить необходимыми и надежными сведениями всех, кто в них заинтересован.

Выходом из создавшейся ситуации явилось изобретение электронно-вычислительных машин (ЭВМ) и персональных компьютеров, создание телекоммуникационной инфраструктуры (баз данных и сетей разных типов).

Но к современным техническим средствам работы с информацией относятся не только компьютеры, но и другие устройства, обеспечивающие ее передачу, обработку и хранение:

· сетевое оборудование: модемы, кабели, сетевые адаптеры;

· аналого-цифровые и цифро-аналоговые преобразователи;

· цифровые фото- и видеокамеры, цифровые диктофоны;

· записывающие устройства (CD-R, CD-RW, DVD-RW и др.);

· полиграфическое оборудование;

· цифровые музыкальные студии;

· медицинское оборудование для УЗИ и томографии;

· сканеры в архивах, библиотеках, магазинах, на экзаменах и избирательных участках;

· ТВ-тюнеры для подачи телевизионного сигнала в компьютер;

· плоттеры и различные принтеры;

· мультимедийные проекторы;

· флэш-память, используемая также в плеерах и фотоаппаратах;

· мобильные телефоны.

Кроме персональных компьютеров существуют мощные вычислительные системы для решения сложных научно-технических и оборонных задач, обработки огромных баз данных, работы телекоммуникационных сетей (Интернет):

· многопроцессорные системы параллельной обработки данных (управление сложными технологическими процессами);

· серверы в глобальной компьютерной сети, управляющие работой и хранящие огромный объем информации;

· специальные компьютеры для проектно-конструкторских работ (проектирование самолетов и космических кораблей, мостов и зданий и пр.).

Все перечисленные технические средства и системы предназначены для работы с*информационными ресурсами* (ИР) в различных отраслях экономики. В настоящее время компьютеры прочно вошли в жизнь современного человека, широко применяются в производстве, проектно-конструкторских работах, бизнесе и многих других отраслях.

Компьютеры в производстве используются на всех этапах: от конструирования отдельных деталей изделия, его дизайна до сборки и продажи. Система автоматизированного производства (САПР) позволяет создавать чертежи, сразу получая общий вид объекта, управлять станками по изготовлению деталей. Гибкая производственная система (ГПС) позволяет быстро реагировать на изменение рыночной ситуации, оперативно расширять или сворачивать производство изделия или заменять его другим. Легкость перевода конвейера на выпуск новой продукции дает возможность производить множество различных моделей изделия. Компьютеры позволяют быстро обрабатывать информацию от различных датчиков, в том числе от автоматизированной охраны, от датчиков температуры для регулирования расходов энергии на отопление, от банкоматов, регистрирующих расход денег клиентами, от сложной системы томографа, позволяющей «увидеть» внутреннее строение органов человека и правильно поставить диагноз.

Компьютер находится на рабочем столе специалиста любой профессии. Он позволяет связаться с любой точкой земного шара, подсоединиться к фондам крупных библиотек не выходя из дома, использовать мощные информационные системы — энциклопедии, изучать новые науки и приобретать различные навыки с помощью обучающих программ и тренажеров. Модельеру он помогает разрабатывать выкройки, издателю компоновать текст и иллюстрации, художнику — создавать новые картины, а композитору — музыку. Дорогостоящий эксперимент может быть полностью просчитан и имитирован на компьютере.

Разработка способов и методов представления информации, технологии решения задач с использованием компьютеров, стала важным аспектом деятельности людей многих профессий. Можно выделить несколько основных направлений, где информационная деятельность связана с компьютерами.

Таблица. Применение технических средств и информационных ресурсов в профессиональной деятельности

|  |  |  |  |
| --- | --- | --- | --- |
| Область деятельности | Профессия | Технические средства | Информационные ресурсы |
| Средства массовой информации | Журналисты | Телевидение, радио, телекоммуникации, компьютеры, компьютерные сети | Интернет, электронная почта, библиотеки, архивы |
| Почта, телеграф, телефония | Служащие, инженеры | Телеграф, телефон, компьютерные сети | Базы данных |
| Наука | Ученые | Телекоммуникации, компьютеры, компьютерные сети | Библиотеки, архивы, базы данных, экспертные системы, Интернет |
| Техника | Инженеры | Телекоммуникации, компьютеры, компьютерные сети | Системы автоматизированного проектирования (САПР), библиотеки, патенты, базы данных, экспертные системы, Интернет |
| Управление | Менеджеры | Информационные системы, телекоммуникации, компьютеры, компьютерные сети | Базы данных, экспертные системы |
| Образование | Преподаватели | Информационные системы, телекоммуникации, компьютеры, компьютерные сети | Библиотеки, Интернет |
| Искусство | Писатели, художники, музыканты, дизайнеры | Компьютеры и устройства ввод/вывода информации, аудио- и видеосистемы, системы мультимедиа, телекоммуникации, компьютеры, компьютерные сети | Библиотеки, музеи, Интернет |

Традиционно информационная  деятельность связывается со средствами массовой информации. Журналисты имеют дело с оперативной информацией, которая иногда актуальна только в течение нескольких дней, поэтому они используют в своей работе самые современные средства передачи информации. Информацию любого вида (текст, звук, видео) можно передать по электронной почте, опубликовать на сайте, популярны видеоконференции в реальном времени.

Работники почтовой службы, кроме традиционных методов доставки корреспонденции, активно используют электронную почту. Бурно развивается сотовая связь и IP-телефония.

Наука призвана производить новые знания. Одним из ее современных инструментов является компьютерное математическое моделирование, позволяющее изучать природные, экономические и социальные явления в развитии.

Инженеры закрепляют технические изобретения в патентах. В развитых странах существуют системы научно-технической информации со специализированными изданиями и патентными службами, которые готовят обзоры, рефераты.

Автоматизированная обработка информации в экономических информационных системах с применением средств связи и оргтехники снабжает менеджеров качественной, точной, объективной информацией. Менеджеры, используя современные технологии в сфере управления, могут принимать более своевременные и объективные решения на основе  оперативной экономической информации.

Преподаватели передают знания от поколения к поколению, следовательно, участвуют в древнейшем информационном процессе. ИТ вносят и в эту консервативную сферу свои нововведения. Технологии мультимедиа создают виртуальные миры, делают процесс обучения более наглядным, сложные абстрактные выкладки становятся понятнее. Компьютерные технологии позволяют индивидуализировать обучение и контроль знаний. Развивается дистанционное образование, позволяющее обучать независимо от удаленности от образовательного учреждения.

Многие формы современного искусства используют ИТ. Создаются музыкальные произведения с использованием midi–совместимых инструментов, исполняющих компьютерную партитуру. Компьютерная графика стала основой современной полиграфии и дизайнерских работ.

Специальность – техническое обслуживание и ремонт автомобиля.

Современные автомобили оснащены бортовыми компьютерами и системой датчиков, через которые осуществляется контроль и управление работой двигателя и системами автомобиля.

В процессе эксплуатации автомобиля нарушаются некоторые параметры, которые влияют на мощность, экономичность и безопасность.

Наиболее достоверную информацию о техническом состоянии автомобиля можно получить, используя компьютерную диагностику, смысл которой заключается в обработке данных бортового компьютера диагностическим компьютером. Кроме того, микропроцессоры используются в навигационных и охранных системах, которыми оснащены современные автомобили.

Информация как экономический ресурс В рыночной среде имеют место практически все виды информации, однако наиболее актуальными являются следующие: Конъюнктурная – характеризует состояние рынка (уровень изменения цен на товары и услуги, курсы ценных бумаг, банковские ставки, биржевые котировки и т.д.). Коммерческая – представляет совокупность сведений о спросе и предложении на определенные виды товаров и услуг, соотношении спроса и предложения (маркетинговая информация, предлагаемые товары и услуги, их качество, конкуренты, конкурентоспособность на внутреннем рынке и т.д.). Финансовая – сведения о финансовой устойчивости, платежеспособности и кредитоспособности партнеров и конкурентов. Внешнеэкономическая – об объемах импорта-экспорта, ценах, качестве, конкурентоспособности на внешнем рынке, влиянии на внутренний рынок и др. Научно-техническая – о достижениях науки и техники, изобретениях, научных исследованиях и их результатах, ноу-хау, патентах, лицензиях и т.д. Статистическая – о динамике количественных и качественных изменений в экономике (в основном на уровне народного хозяйства страны, отрасли, региона). Правовая – о системе и источниках права, юридических фактах, правоотношениях, правопорядке, правонарушениях и борьбе с ними. Справочно-энциклопедическая – словари, справочники, энциклопедии и т.д. Массовая – газеты, журналы, радио, телевидение, кино, видео и т.д. Существование ряда свойств информации, аналогичных свойствам традиционных ресурсов, дало основание использовать многие экономические характеристики (цена, стоимость, издержки, прибыль и т. д.) при анализе информационного производства. В качестве экономического ресурса информация предназначена для обмена, имеется в ограниченном количестве, при этом на нее предъявляется платежеспособный спрос. Ценность, или полезность, информации состоит в возможности дать дополнительную свободу действий потребителю.

**Экономика информационной сферы. Стоимостные характеристики информационной деятельности.**

Информационная экономика имеет ряд принципиальных особенностей.

1. Информационное производство, информационные продукты и услуги являются чрезвычайно наукоемкими. Поэтому их качество и конкурентоспособность на внутреннем и внешнем рынках существенным образом зависят от уровня технологического развития той или иной страны, от уровня развития и использования новых информационных технологий.
2. Продукция информационной экономики является сегодня важнейшим фактором для ускоренного развития ряда других областей общественного хозяйства - промышленности, строительства, транспорта, добывающих отраслей.
3. Информационная экономика отличается исключительно высокой динамичностью смены моделей и даже целых поколений своей продукции, опережая в этой части все другие секторы развития экономики.
4. Многие виды информационной продукции и информационные технологии по своим функциональным возможностям являются изделиями двойного применения, которые могут использоваться как в гражданских, так и в военных целях. Поэтому, развитие информационной экономики самым тесным образом связано с развитием военно-промышленного комплекса той или иной страны и в значительной степени определяет ее обороноспособность и уровень обеспечения национальной безопасности.
5. Информационная экономика обеспечивает создание инструментальных средств для производства и эффективного использования знаний. Все это создает предпосылки для экономии других видов ресурсов развития общества (сырья, энергии, материальных и людских ресурсов).
6. Развитие информационной экономики создает новую структуру занятости населения, стимулирует развитие новых форм индивидуального труда и творчества, формирования новой информационной культуры общества и новых духовных ценностей.
7. Информационная экономика имеет дело с весьма специфическим видом ресурсов общества - информационным ресурсом, который обладает особыми свойствами при его тиражировании, распространении и использовании в качестве товара. Эти свойства и особенности еще недостаточно учитываются в правовой сфере общества.

По многим прогнозам ожидается, что XXI век будет периодом формирования глобального автоматизированного информационного пространства, которое и станет не только основой для дальнейшего развития экономики многих стран мира, но также и ареной борьбы за сферы влияния в этом мире. Развитие информационной экономики и место тех или иных стран в новом глобальном информационном пространстве приобретают решающее значение в их геополитике.

**Критерии эффективности применения информационных технологий**

Эффективность — одно из наиболее общих экономических понятий, не имеющих пока, единого общепризнанного определения.

Эффективность — это одна из возможных характеристик качества системы, а именно ее характеристика с точки зрения соотношения затрат и результатов функционирования системы.

В дальнейшем будем понимать под эффективностью информационных технологий меру соотношения затрат и результатов применения информационных технологий. В качестве основных показателей эффективности часто рассматривают показатели экономической эффективности: экономический эффект, коэффициент экономической эффективности капитальных вложений, срок окупаемости капитальных вложений и т.д.

Экономический эффект - результат внедрения какого-либо мероприятия, выраженный в стоимостной форме, в виде экономии от его осуществления.

Так, для организаций, использующих информационные технологии, основными источниками экономии являются:

* улучшение показателей их основной деятельности, происходящее в результате использования информационных технологий;
* сокращение сроков освоения новых информационных технологий за счет их лучших эргономических характеристик;
* сокращение расхода машинного времени и других ресурсов на отладку и сдачу задач  в эксплуатацию при внедрении нового инструментария информационных технологий;
* повышение технического уровня, качества и объемов информационно-вычислительных работ;
* увеличение объемов и сокращение сроков переработки информации;  повышение коэффициента использования вычислительных ресурсов, средств подготовки и передачи информации;
* уменьшение численности персонала, в том числе высококвалифицированного, занятого обслуживанием программных средств, автоматизированных систем, систем обработки информации, переработкой и получением информации;
* снижение трудоемкости работ программистов при программировании прикладных  задач с использованием новых информационных технологий в организации-потребителе информационных технологий;
* снижение затрат на эксплуатационные материалы.

Коэффициент экономической эффективности капитальных вложений показывает величину годового прироста прибыли, образующуюся в результате производства или эксплуатации информационных технологий, на один рубль единовременных капитальных вложений.

Срок окупаемости (величина, обратная коэффициенту эффективности) — показатель эффективности использования капиталовложений — представляет собой период времени, в течение которого произведенные затраты на информационные технологии окупаются полученным эффектом.

Определение эффективности информационных технологий основано на принципах оценки экономической эффективности производства и использования в народном хозяйстве новой техники, с учетом специфики информационных технологий.

Предварительный экономический эффект рассчитывается до выполнения разработки информационных технологий на основе данных технических предложений и прогноза использования. Предварительный эффект является элементом технико-экономического обоснования разработки информационных технологий и используется при планировании разработки и их внедрения.

Потенциальный экономический эффект рассчитывается по окончании разработки на основе достигнутых технико-экономических характеристик и прогнозных данных о максимальных объемах использования информационных технологий. Потенциальный эффект используется при оценке деятельности организации-разработчиков информационных технологий.

Гарантированный экономический эффект рассчитывается в виде гарантированного экономического эффекта для конкретного объекта внедрения и общего гарантированного внедрения по ряду объектов.

Гарантированный экономический эффект для конкретного объекта внедрения рассчитывается после окончания разработки для одного внедрения на основе данных о гарантированном разработчиком удельном эффекте от применения информационных технологий и гарантированных пользователем сроках и годовом объеме использования информационных технологий.

Гарантированный эффект от одного внедрения информационных технологий рассчитывается при оформлении договорных отношений между организацией-разработчиком и организацией-пользователем. Гарантированный общий эффект служит для обоснования цены на информационные технологии, выбора варианта их производства и внедрения.

Фактический экономический эффект рассчитывается на основе данных учета и сопоставления затрат и результатов при конкретных применениях информационных технологий.

Фактический эффект используется для оценки деятельности организаций, разрабатывающих, внедряющих и использующих информационные технологии, для определения размеров отчислений в фонды экономического стимулирования, а также для анализа эффективности функционирования информационных технологий и выработки технических предложений по совершенствованию информационных технологий и условий их применения.

Показатели экономической эффективности информационных технологий определяются на основе:

* экономической оценки результатов влияния информационных технологий на конечный результат их использования;
* экономической оценки результатов влияния на технологические процессы подготовки, передачи, переработки данных в вычислительных системах;
* экономической оценки результатов влияния информационных технологий на технологический процесс создания новых видов информационных технологий.

«Компьютерные вирусы и

средства антивирусной защиты»

**Содержание**

[Введение 2](#_Toc358416811)

[Глава 1. Компьютерные вирусы 3](#_Toc358416812)

[1.1. Понятие «Компьютерный вирус» 3](#_Toc358416813)

[1.2. Авторы компьютерных вирусов 4](#_Toc358416814)

[1.3. История компьютерных вирусов 5](#_Toc358416815)

[1.4. Механизм работы вирусов 6](#_Toc358416816)

[1.5. Способы распространения компьютерных вирусов 7](#_Toc358416817)

[1.6. Признаки заражения вирусом 9](#_Toc358416818)

[Глава 2. Классификация компьютерных вирусов 11](#_Toc358416819)

[Глава 3. Профилактика и лечение 15](#_Toc358416820)

[3.1. Антивирусные программы 15](#_Toc358416821)

[3.2. Виды антивирусных программ 16](#_Toc358416822)

[3.2.1 Программы-детекторы 16](#_Toc358416823)

[3.2.2 Программы-доктора 16](#_Toc358416824)

[3.2.3 Программы-ревизоры (инспектора) 17](#_Toc358416825)

[3.2.4 Программы - фильтры (мониторы) 17](#_Toc358416826)

[3.2.5 Вакцины или иммунизаторы 17](#_Toc358416827)

[3.2.6 Сканер 18](#_Toc358416828)

[3.3. Лицензионные антивирусные программы 19](#_Toc358416829)

[3.4. Альтернатива платным программам 20](#_Toc358416830)

Заключение [23](#_Toc358416831)

Библиография [24](#_Toc358416832)

Введение

Компьютеры сегодня выполняют множество задач. Практически любая организация сейчас не работает без компьютера. Рынок ИТ развивается, появляются новые интернет- ресурсы и сервисы, люди все свободное время проводят в сети Интернет. Сегодня из-за массового применения персональных компьютеров появилисьпрограммы-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Поэтому защита личной информации и нормальной работоспособности персональных компьютеров сейчас, как никогда, актуальна. Все чаще в средствах массовой информации появляются сообщения оразличного рода пиратских проделках. Увеличилось появление все более совершенных вредоносных программ.

Борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в десятках, а может быть, сотнях компаний. Ведь именно компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации.

Во многих странах были приняты законы о борьбе с компьютерными преступлениями и разработаны специальные программы 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.

Поэтому, ***цель данной работы***:

* выяснить пути проникновения вирусов;
* влияние вирусов на работу компьютера;
* определить методы защиты от них.

Исходя из цели проекта, были поставлены следующие задачи:

* определить, что является компьютерным вирусом;
* определить виды вирусов по способам проникновения их в компьютер и влиянию на работу и безопасность;
* ознакомление с существующими методами защиты от компьютерных вирусов.

Глава 1. Компьютерные вирусы

## Понятие «Компьютерный вирус»

Компьютерный вирус был назван по схожести с биологическими вирусами за подобный механизм распространения: эффект захвата компьютера вирусом полностью соответствует эффекту захвата вирусом человеческого организма. Человеческий вирус проникает в клетку, после чего начинает размножаться. Так и компьютерный: попав в компьютерную программу, вирус действует таким же образом.

Считается, что впервые слово «вирус» по отношению к программе было употреблено ГБенфордом (GregoryBenford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

***Компью́терный ви́рус***— является разновидностью компьютерных программ или вредоносный код.Его признаком является способность к размножению (саморепликация).

Попав в компьютерную систему, вирус может сопровождаться безобидными визуальными или звуковыми эффектами. Он вызывает через некоторое время потерю или искажение данных, утечку личной и конфиденциальной информации. В результате компьютерная система, куда попал вирус, становится неработоспособной или же окажется под полным контролем злоумышленника.

Даже если человек, создавший вирус не программировал вредоносных эффектов, вирус может привести к сбою компьютер из-за ошибок.Он ,просто, не учёл тонкостей взаимодействия с ОС и другими программами. К тому же, вирусы всегда занимают определенное место, иногда довольно значительное,вОП или на носителях информации и отбирают некоторые другие ресурсы системы.

Поэтому вирусы относят к вредоносным программам.

## Авторы компьютерных вирусов

Вирусы не появляются сами по себе, а создаются людьми. Наиболее возможными причинами, толкающими людей на создание и распространение вредоносного программного обеспечения являются:

- обычное *подростковое хулиганство*, молодые люди становятся увереннее придостижении такого интеллектуального уровня. Практически такое компьютерное хулиганство ничем не отличается от рядового уличного хулиганства, кроме того, что "самоутверждение" происходит либо на улице, либо в компьютерной сети;

- *мошенничество* для присвоения чужих ресурсов: незаметно можно управлять зараженным компьютером, воровать пароли доступа в Интернет, средств с "кошельков" WebMoney и кодов доступа к персональным банковским счетам (если человек использует банковский счет). Ну а, если поразились корпоративные сети, то это уже говорит о шпионаже: как правило, это проникновение в сеть для присвоения конфиденциальной информации, представляющей финансовую ценность.

Основная масса вирусов создаются студентами и школьниками, которые только что начали изучать язык программирования и хотят попробовать свои силы. Основная часть подобных вирусов их авторами не афишируются.

Другая группа составляет также молодые люди (чаще - студенты), которые хотят посвятить себя написанию и распространению вирусов. Чаще всего, они создают много "классических" вирусов, либо вирусы крайне примитивные и с огромным количеством ошибок. Чаще всего они используют макеты вирусов, с помощью которых можно создавать новые вирусы даже при небольших знаниях об ОС.

Став старше и опытнее, многие из этих вирусописателей попадают в третью, более опасную группу, которая сама создает и запускает в мир "профессиональные" вирусы. Это хорошо продуманные и отлаженные программы.

Четвертая группа авторов вирусов - "исследователи". Эта группа талантливых программистов, которые занимаются изобретением новых методов , способов заражения, скрытия, противодействия антивирусам и т.д. Эти программисты-исследователи пишут вирусы не ради собственно вирусов, а просто ради "исследования" потенциалов "компьютерной вирусологии".

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (гл. 28, ст.273).

## История компьютерных вирусов

На сегодняшний день компьютерному вирусу уже более тридцати лет.

Первыми известными вирусами являются *Virus 1,2,3* и *ElkCloner* для ПК Apple II. Он появился в 1981 году. Первых вирусов эпидемии относят к 1987 - 1989 годам. Это *Brain*(более 18 тысяч зараженных компьютеров, по данным *McAfeeJerusalem* (который был запущен в пятницу 13 мая 1988 года, уничтожая программы при их запуске). Следующий это  *червь Морриса* (свыше 6250 компьютеров, большинство сетей вышло из строя на срок до пяти суток). Также *DATACRIME* (около 100 тысяч зараженных персональных ЭВМ только в Нидерландах).

В 1990 году создали первый коммерческий антивирус Symantec NortonAntiVirus.

В несколько последующих лет были испробованы самые необычные способы проникновения в систему и заражения файлов (*Dir II* — 1991, *PMBS*, *Shadowgard*, *Cruncher* — 1993). Также, появились вирусы, поражающие объектные файлы (*Shifter*, 1994) и исходные тексты программ (*SrcVir,* 1994). С появлением пакета Microsoft Office появились и распространились макровирусы (*Concept*, 1995).

С появлением сетей и Интернета файловые вирусы всё больше направлены на них, как на основной канал работы (*Melissa*, 1999 - макровирус и сетевой червь, который побил все рекорды по скорости распространения).

В 2004 году беспрецедентные по масштабам эпидемии вызывают черви-эксплоиты[[1]](#footnote-2)*MsBlast* (по данным Microsoft - более 16 млн систем), *Sasser и Mydoom* (оценочные ущербы 500 млн и 4 млрд долл. соответственно).

Кроме того, цельные вирусы в большей мере уступают свое место комплексам вредоносного программного обеспечения с разделением ролей и вспомогательными средствами. Также расцветают социальные технологии — спам[[2]](#footnote-3) и фишинг[[3]](#footnote-4) — как средство заражения в обход механизмов защиты программного обеспечения.

Современные вирусы  - это черви-[ботнеты](http://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) , которые всё больше набирают обороты (*Rustock*, 2006, ок. 150 тыс. ботов; *Conficker*, 2008-2009, более 7 млн ботов; *Kraken*, 2009, ок. 500 тыс. ботов).

## Механизм работы вирусов

Вирусы распространяются копируя свое тело. При этомвнедряет себя в исполняемый код других программ, заменяя собой другие программы. Вирусом или его носителем могут быть как программы, содержащие машинный код, так и всякая информация, которая содержит автоматически исполняемые команды — например, пакетные файлы и документы MicrosoftWord и Excel, которые содержат макросы. Кроме того, для того чтобы проникнуть в компьютер, вирус может использовать уязвимости в популярном ПО (например, AdobeFlash, InternetExplorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) .

## Способы распространения компьютерных вирусов

Способы распространения компьютерных вирусов разнообразны, однако существуют все же наиболее распространенные, от которых можно уберечься, соблюдая элементарные меры предосторожности.

***Дискеты.*** Самымизвестным каналом заражения в 1980-1990-е годы. Сейчас их практически нет из-за появления более современных и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

*****Флеш-накопители(флешки).*** В настоящее время USB-флешкииспользуют как дискеты и повторяют их судьбу — огромное количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы).

*****Электронная почта.***Обычно вирусы в письмах электронной почты маскируются под безобидные вложения.

Например под картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки.В самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт. А этот веб-сайт может содержать вирусный код.

*****Системы обмена мгновенными сообщениями.*** Здесь тоже распространена рассылка ссылок на как-бы фото, музыку либо программы. А они в действительности являются вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

***Веб-страницы.***Также можно заразиться и через страницы Интернета из-за наличия на страницах всемирной паутины разного «активного» содержимого: скриптов, ActiveX-компонент. В этом случае используются уязвимости ПО, установленного на компьютере пользователя, либо уязвимости в программном обеспечениихозяина сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, заражают свой компьютер.

*****Интернет и локальные сети(черви).***Черви — это вирусы, которые попадают на жертву-компьютер без участия пользователя. Они используют уязвимости в ПО операционных систем.чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоделки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код. Из-за чегочервь-вирус попадает в операционную систему . Далее она начинает действия по паражению других компьютеров через локальную сеть или Интернет. Вредоносители используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Как вы видите, способов распространения компьютерных вирусов очень много. Для того, чтобы предотвратить заражениенужно соблюдать элементарные меры предосторожности:

* Использовать нужнолицензионные проверенные ресурсы в сети Интернет;
* не скачивать подозрительные программы, а также не нажимать вызывающие сомнения картинок;
* при получении электронных писем от незнакомого адресата, обратите внимание на расширение приложенных файлов. Если они имеют такие типы как:\*.bat,\*.vbs,\*.scr,\*.exe, то не нужно скачивать эти приложения, они могут быть заражены или уже являются вирусом трояном;
* применять лицензионные антивирусы.

И тогда с уверенностью можете избежать заражения.

## Признаки заражения вирусом

При заражении ПК вирусом нужно его обнаружить, для этого необходимо знать какие-нибудь признаки его проявления:

- прекращается работа какой-либо программы, которая ранее хорошо работала;

- замедляется работа ПК;

- невозможно запустить ОС;

- некоторые файлы и каталоги теряются или искажается их содержимое;

- меняются дата и время модификации файлов;

- меняется размер файлов;

- резко увеличивается количество файлов на диске;

- уменьшается размер свободнойОП;

- на экран высвечиваются непонятные сообщения или изображения;

- подаются непредусмотренные звуковые сигналы;

-компьютер часто зависает и дает сбои в работе.

Надо сказать, что все перечисленные явления необязательно вызываются вирусами, а могут быть и следствием других причин. Поэтому всегда трудно правильно диагностировать состояние компьютера. Заразиться компьютерным вирусом можно только в некоторых случаях:

- если запустить зараженную программу на компьютере;

- если загрузить компьютер с зараженного диска (дискеты);

- если подключились к системе заражённого драйвера;

- если открыли документ, заражённый макровирусом;

- при установке на компьютер заражённую ОС.

Компьютер не может быть заражён:

- если переписать на него текстовые и графические файлы (кроме файлов, которые выполняют макрокоманды);

-если производили копирование с одной дискеты на другую и ни один файл с дискет не запускался;

- если на компьютере производится обработка принесённых снаружи текстовых и графических файлов. Это файлы данных и информационных файлов (кроме файлов, предусматривающих выполнение макрокоманд);

**- если** переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение было надо либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты). Значит, заразить свой ПК можно только в том случае, если запустить на нём неизвестные программы и (или) программные продукты, установить непроверенные драйвера и (или) ОС, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

Глава 2. Классификация компьютерных вирусов

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на то, что вирусов очень много они отличаются друг от друга механизмом распространения и принципом действия. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Таким образом, вирусы можно классифицировать по следующим признакам:

* среда обитания;
* способ заражения;
* степень воздействия;
* особенности алгоритма работы.

В зависимости **от среды обитания** вирусы делят на:

* ***сетевые*** – которые распространяются по различным компьютерным сетям;
* ***файловые*** - которые поражают файлы с расширением .com, .ехе, реже .sys или оверлейные модули .ехе файлов. Эти вирусы дописывают своё тело в начало, середину или конец файла. Далее изменяют его таким образом, чтобы первыми получить управление. Получив управление, вирус может заразить другие программы. Может внедриться в оперативную память компьютера и т.д. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным и не подлежащим восстановлению;
* ***загрузочные*** - получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в конец оперативной памяти . После перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов;
* ***файлово–загрузочные*** – комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Попадая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов.

**По способу заражения среды обитания** вирусы делятся на:

* ***резидентные*** - при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть.Она потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти компьютера. Они активны вплоть до выключения или перезагрузки компьютера;
* ***нерезидентные вирусы*** не заражают память компьютера. Они являются активными на определенное, ограниченное время.

**По степени воздействия** вирусы можно разделить на:

* ***неопасные,***те, которые не мешают работе компьютера. Но они уменьшают объем свободной ОП и памяти на дисках. Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;
* ***опасные вирусы***, которые могут привести к различным сбоям в работе компьютера;
* ***особо опасные***, воздействие которых может привести к потере программ. Уничтожаются данные, стирается информация в системных областях диска.

**По особенностям алгоритма**:

* ***простейшие вирусы*** – паразитические. Они меняют содержимое файлов и секторов диска . Также они могут быть достаточно легко обнаружены и уничтожены;
* ***вирусы-невидимки (стелс-вирусы)*** – стараются скрыть свое присутствие в компьютере. Если оперативная система или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова.
* ***Макрокомандные вирусы***. Файлы документов MicrosoftOffice могут содержать в себе небольшие программы для обработки этих документов. Они составлены на языке VisualBasicforApplications. Это относится и к базам данных Access. Также относятся к файлам презентаций PowerPoint. Такие программы создаются с использованием макрокоманд. Вирусы, которые живут в офисных документах, называют макрокомандными. Они распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении.

Кроме вирусов принято выделять еще, по крайней мере, три вида вредоносных программ:

* ***Троянские программы*** - по назначению они безобидны или даже полезны. Но когда пользователь записал программу в свой компьютер и запускает ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов.
* ***Логические бомбы*** – программы, которые выполняют вредоносные действия. Например, может сработать по достижении определенной даты. Или тогда, когда в базе данных появится или исчезнет запись. Подобная бомба может быть встроена в вирусы, в трояны и даже в обычные программы.
* ***Программы-черви*** направлены на выполнение определенной функции. Например, на проникновение в систему и модификацию данных. Могут подсматривать пароль для доступа к банковской системе. Могут изменять базу данных. Некоторые вирусы-черви (например, *CodeRed*) существуют не внутри файлов, а в виде процессов в памяти зараженного компьютера. Что исключает их обнаружение антивирусами, которые сканируют файлы и оставляют без внимания ОП компьютера.
* ***Вирусы в системах документооборота*** - документы, хранящиеся в базах данных таких систем документооборота, как LotusNotes и MicrosoftExchange, тоже могут содержать вирусы, т.е., вредоносные макрокоманды. Они могут активизироваться при выполнении каких-либо действий над документом. Например, когда пользователь щелкает кнопку мышью. Так как такие вирусы расположены не в файлах, а в записях баз данных, то для защиты от них требуются специальные антивирусные программы;
* ***новые и экзотические вирусы.*** В связи с развитием компьютерных технологий совершенствуются и компьютерные вирусы. Они легко могут приспособиться к новым для себя сферам обитания. Новые вирусы могут использовать неизвестные или новые технологии внедрения в компьютерные системы.

Глава 3. Профилактика и лечение

## 3.1.Антивирусные программы

Для борьбы с вирусами программисты стали создавать антивирусные программы. Они могут обнаружить вирусы. Могут удалить их из компьютера.

Итак, что же такое антивирус? Многие программисты считают, что антивирус может обнаружить любой вирус. Запустив антивирусную программу, можно быть абсолютно уверенным в их надежности. Это не совсем правильная точка зрения. Ведь антивирусную программу тоже писали профессионалы. Они могут найти и уничтожить только известные им вирусы. Значит, антивирусная программа пишется против конкретного вируса. Если у программиста есть в наличии хотя бы один экземпляр этого вируса. Но у большинства вирусов алгоритм практически скопирован с алгоритма других вирусов.

Современные антивирусные программы могут выявить практически все уже известные вирусные программы. Они сравнивают код подозрительного файла с образцами, хранящимися в антивирусной базе. Найденные объекты подвергаются лечению, изолируются или удаляются..

## 3.2. Виды антивирусных программ

Существует несколько основополагающих методов поиска вирусов.

Они применяются антивирусными программами .Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов антивирусных программ:

1. программы-детекторы

2. программы-доктора или фаги

3. программы-ревизоры (инспектора)

4. программы-фильтры (мониторы)

5. программы-вакцины или иммунизаторы

6. сканер

### 3.2.1 Программы-детекторы

Программы-детекторы ищут конкретный вирус вОП и вфайлах и при обнаружении высвечивается сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

### 3.2.2 Программы-доктора

Программы-доктора или фаги, а также программы-вакцины находят зараженные вирусами файлы и «лечат» их. Удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы вОП. После уничтожает их, а иногда «лечит» файлы. Среди фагов выделяют полифаги, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

### 3.2.3 Программы-ревизоры (инспектора)

Программы-ревизоры это самые надежные средства защиты от вирусов. Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок. Изучают, не забрался ли вирус в файлы. Нет ли посторонних в загрузочном секторе жесткого диска. Нет ли несанкционированных изменений реестра Windows. Причем инспектор может не пользоваться средствами ОС для обращения к дискам (а значит, активный вирус не сможет это обращение перехватить).

### 3.2.4 Программы - фильтры (мониторы)

Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы. Они предназначенны для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

1. попытки коррекции файлов с расширениями COM, EXE

2. изменение атрибутов файла

3. прямая запись на диск по абсолютному адресу

4. запись в загрузочные сектора диска

5. загрузка резидентной программы.

### 3.2.5 Вакцины или иммунизаторы

Вакцины или иммунизаторы - это резидентные программы, которые предотвращают заражение файлов. Применяются вакцины для лечения этих вирусов. Вакцинация возможна только от известных вирусов. В настоящее время программы-вакцины имеют ограниченное применение.

### 3.2.6 Сканер

Антивирусные сканеры проверяют файлы, секторы и системную память. Ищут в них известные и новые (неизвестные сканеру) вирусы. Для поиска известных вирусов используются так называемые «маски». Маской вируса является последовательность кода для конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы.

В настоящее время существует много антивирусных программ, но гарантий нет, что они смогут справиться с новыми вирусами. Поэтому следует принимать меры предосторожности, в частности:

1. Не запускать незнакомые программы из сомнительных источников.

2.Блокировать несанкционированные изменения системных файлов.

3. Не заходить на подозрительные сайты.

4. Пользоваться только доверенными дистрибутивами.

5. Постоянно делать резервные копии данных.

## 3.3. Лицензионные антивирусные программы

Как выбрать антивирусную программу для домашнего пользования –самый наболевший вопрос, особенно для начинающих пользователей. Рано или поздно каждый абонент захочет установить антивирусную программу. А многие пользователи вообще не устанавливают программ для защиты своего компьютера. До тех пор пока не возникают различные сбои в работе системы. И действительно, при заражении компьютера вирусами замедляется работа системы, компьютер "тормозит" или "зависает".

Лицензионная антивирусная программа обеспечит более надежную защиту данных от незаконного доступа в компьютер.

Перечислим самые популярные лицензионные антивирусные программы, которые можно приобрести, в т.ч и через Интернет.

**Антивирус Касперского -** обеспечивает защиту в реальном времени от вирусов, червей, троянских коней. Имеются версии для мобильных устройств (18 версий).

[**Eset NOD32**](http://abisoft.ru/1/cid/2724/Eset_NOD32.html) **-** представляет полную защиту компьютера.Отличительной особенностью является экономичное использование ресурсов и высокая скорость исполнения (31 версия)

**Доктор Веб -** базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией (45 различных версий).

[**Аvast! -**](http://abisoft.ru/1/cid/2801/avast!.html) это более эффективная защита во время просмотра страниц Интернета, полнофункциональная антивирусная программа [(23 версии)](http://abisoft.ru/1/cid/2801/avast!.html).

## 3.4. Альтернатива платным программам

Часто встречаетсячто производители антивирусных программ предлагают версии своих продуктов без оплаты, которые менее функциональны, чем их платные аналоги. Это делается для продвижения и популяризации своего бренда среди пользователей.

Нужно отметить, что некоторые бесплатные программы могут защитить систему не хуже коммерческих антивирусов.Так что решать уже пользователю.

Примеры бесплатных программ-антивирусов:

Антивирус **BitDefenderFreeEdition** - программа, которая поможет защитить систему, периодически проводя проверки и сканирование.

Антивирус **avast! FreeAntivirus -** это один из лучших антивирусов среди бесплатных программ для защиты. Самый популярный на сегодня этоavast среди пользователей всего мира.

**Comodo** защитит систему от вирусов, шпионских программ, руткитов, а также от иных вредоносных программ.

Антивирус от**Microsoft**под названием **SecurityEssentials** предоставит защиту от вирусов, шпионов и других вредоносных программ. Наличие журнала проверки, планировщика, а также интуитивно понятный интерфейс для пользователей сделали этот антивирус, который распространяется бесплатно, популярным среди многих пользователей.

**RisingAntivirusFreeEdition** это бесплатная программа для защиты системы, которая поможет как при ежедневной работе, так и при работе в сети Интернет. Антивирус имеет простой и удобный интерфейс, а также множество настроек.

**Ad-Aware FREE InternetSecurity** это антивирус, который распространяется бесплатно.Он сможет обеспечить полноценную защиту при работе в сети Интернет.

**PandaCloudAntivirus** это возможность использовать передовую защиту отПанда, ничего при этом не потратив. Антивирус оказывает минимальное воздействие на систему и обеспечивает максимальную защиту.

# Заключение

Пожалуй, самым страшным кошмаром любого пользователя сети Интернет являются компьютерные вирусы. Они постоянно совершенствуются. Вирусы попадают на компьютеры часто. Иногда не сразу понятно, что же произошло с системой.

Хочу заметить, что слишком уж бояться вирусов не стоит. Особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (*Win95.CIH*), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того.

Зачем надо защищаться? Все зависит от конкретного профиля рода занятий. Для одних главной задачей является предотвращение утечки информации к конкурентам. Другие могут уделять главное внимание целостности информации. Для третьих на первое место поднимается задача безотказной работы информационных систем (например, для провайдеров Интернет). Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

# Библиография

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2001.
2. Левин А.Ш. Самоучитель полезных программ. 4-е издание. – СПБ.: Питер, 2005.
3. Мостовой Д.Ю. Современные технологии борьбы с вирусами - Мир ПК. - №8. 2001.
4. Островский С. Компьютерные вирусы Информатика, январь 2002.
5. [http://www.viruslist.com](http://www.viruslist.com/) - Все угрозы.
6. [http://www.bytemag.ru](http://www.bytemag.ru/) – BYTE/Россия – Что нужно знать о компьютерных вирусах.
7. <http://antivibest.ru> – Антивирусные программы.

1. ## Эксплойт [exploit] - компьютернаяпрограммаиспользующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

   [↑](#footnote-ref-2)
2. **Спам** (англ. *spam*) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать. [↑](#footnote-ref-3)
3. **Фи́шинг** (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведениямассовых рассылок электронных писем от имени популярных брендов. [↑](#footnote-ref-4)