МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине
«ТЕХНОЛОГИИ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ И ИНЦИДЕНТОВ»
для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Анализ безопасности информационных систем

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ.....

Предисловие.....

КРАТКАЯ ИСТОРИЯ РАЗВИТИЯ ЭВМ.....

ОСНОВНЫЕ..... НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕР
ПРЕСТУПНОСТИ.....

ПРАВОВОЕ.....ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕР
ИНФОРМАЦИИ.....

ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНОЕ ОБЕСПЕЧЕНИЕ
БЕЗОПАСНОСТИ ИНФОРМАЦИИ.....

ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОМПЬЮТЕРНОЙ
ИНФОРМАЦИИ.....

Физические средства защиты компьютерной информации.....

Аппаратные средства защиты компьютерной информации.....

Программные средства защиты компьютерной информации.....

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Технологии расследования компьютерных преступлений и инцидентов» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» умения проводить анализ данных, полученных в ходе исследования электронных носителей информации, компьютерной аппаратуры и других систем.

Задачи освоения дисциплины:

осуществлять проведение технической диагностики компьютерного оборудования, направленное на поиск, обнаружение, анализ и оценку информации;

проверить целостность компьютерной системы или ее отдельных элементов, аппаратных и программных средств

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Предисловие

Существующие реалии таковы, что информация и современные информационно-телекоммуникационные технологии являются одним из наиболее важных факторов в формировании общества XXI века, фактором, пронизывающим все стороны и аспекты человеческой деятельности. Однако, наряду с той положительной ролью, которую играет дальнейшая информатизация нашего общества, данный процесс вызвал и целый ряд негативных последствий.

Одним из таких негативных социальных явлений, сопровождающих внедрение новых информационных технологий в деятельность различных предприятий, учреждений, организаций, является компьютерная преступность. Общественная опасность и размер ущерба, наносимого собственнику информации или автоматизированной системе, позволяет говорить не просто о нарушении безопасности или несанкционированном доступе к информации, а уже о

«компьютерных преступлениях», борьба с которыми является одной из важнейших задач правоохранительных органов на современном этапе.

Ситуация в этой сфере такова, что приходится говорить о недостаточности принимаемых мер по противодействию компьютерной преступности. Наблюдается устойчивая тенденция роста числа правонарушений в сфере компьютерной информации, повреждений линий и сооружений связи. Особенно остро обозначилась проблема распространения вредоносных компьютерных программ, представляющих угрозу государственным и региональным информационным ресурсам. Правоохранительные органы констатирует, что криминальные структуры активизируют попытки использовать открытые телекоммуникационные и ведомственные вычислительные сети для проведения крупных финансовых махинаций и мошеннических акций. Кроме того, дальнейшее распространение получает практика использования специальных программ для контрольно-кассовых машин в интересах уклонения от уплаты налогов. Со стороны криминала фиксируются многочисленные попытки незаконного проникновения в базы и банки данных различных государственных организаций и правоохранительных органов.

Все это обуславливает не только необходимость повышения эффективности деятельности правоохранительных органов по борьбе с компьютерной преступностью, но и необходимость принятия собственниками информации системы мер по обеспечения надежной защиты компьютерной информации от преступных посягательств.

Человечество неотвратимо вступает в информационную эру, в которой информация выступает как один из важнейших факторов общественного развития. Данный подход к пониманию той роли, которую играет информация в современном мире, нашел свое отражение в документах ЮНЕСКО, в которых информация рассматривается как *универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и мнений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения*.

По подсчетам науковедов с начала нашей эры для удвоения знаний потребовалось 1750 лет, второе удвоение произошло в 1900 году, а третье – к 1950 году, т.е. уже за 50 лет, при росте объема информации за эти полвека в 8-10 раз .

Причем эта тенденция все более усиливается. Это явление, получившее название «информационный взрыв», указывается среди симптомов, свидетельствующих о начале века информации и включающих:

- быстрое сокращение времени удвоения объема накопленных научных знаний;
- превышение материальных затрат на хранение, передачу и переработку информации аналогичных расходов на энергетику;
- возможность впервые реально наблюдать человечество из космоса (уровни радиоизлучения Солнца и Земли на отдельных участках радиодиапазона сблизились) .

Таким образом, XXI век – это не только историческая веха, характеризующая определенный временной этап развития человечества, но и период завершения одного гигантского этапа в развитии человечества и перехода к другому.

`

См.:
1 Васильев Р.Ф. Охота за информацией. – М.: Знание, 1973. – С.20.

2 См. об этом: Громов Г.Р. Очерки информационной технологии. – 2-е изд., перераб. и доп. – М.: Инфоарт, Б.г. – 1991. – С.19-20.

Завершаемый период – индустриальное общество, наступающий – общество информационное, в котором именно информация является определяющим фактором общественной жизни.

Вообще термин «информация» происходит от латинского *informatio*, означающего «ознакомление, разъяснение, представление, понятие» и первоначально был связан исключительно с коммуникативной деятельностью людей. В России он появился, по-видимому, в петровскую эпоху , но широкого распространения не получил. Лишь в начале XX века он стал использоваться в документах, книгах, газетах и журналах и употреблялся в смысле сообщения, осведомления, сведения о чем-либо.

Однако стремительное развитие в 20-х годах прошлого века средств и систем связи, зарождение информатики и кибернетики настоятельно потребовали научного осмысления понятия информации и разработки соответствующей теоретической базы. Это привело к формированию и развитию целого «семейства» самых различных учений об информации и соответственно подходов к определению самого понятия информации.

История учений об информации начиналась с рассмотрения ее *математического (синтаксического) аспекта,* связанного с количественными показателями (характеристиками) информационных систем.

В 1928 г. Р. Хартли в своей работе «Transmission of Information» определил меру количества информации для равновероятных событий , а в 1948 г. Клод Шеннон предложил формулу определения количества информации для

совокупности событий с различными вероятностями . И хотя еще в 1933 г. вышла

в свет работа нашего выдающегося ученого В. А. Котельникова о квантовании электрических сигналов, содержащая знаменитую

«теорему отсчетов»[5], в мировой научной литературе считается, что именно 1948 г. – это год зарождения теории информации и количественного подхода к информационным процессам.

`

См.: Советский энциклопедический словарь/Гл. ред. А.М. Прохоров. – 3-е изд. – М.: Сов. энциклопедия, 1985. – С.498.

См.: Смирнов Н.А. Западное влияние на русский язык в Петровскую эпоху. – Спб.: тип. Акад. наук, 1910. – С.123.

См.: Hartley R.V. Transmission of Information//Bell System Technical Journal. – 1928. – № 7(3). – P. 535-563.

См.: Шеннон К. Работы по теории информации и кибернетике. – М.: Изд. ин. лит., 1963.

См.: Котельников В. А., Николаев А. М. Основы радиотехники. Ч.1. – М.: Связь - издат, 1950.

Сформулированная К. Шенноном статистическая теория информации оказала заметное влияние на самые различные области знаний. Было замечено, что формула Шеннона очень похожа на используемую в физике формулу Больцмана для статистического определения энтропии, взятую с обратным

знаком. Это позволило Л. Бриллюэну охарактеризовать информацию как *отрицательную энтропию (негэнтропию)* .

Значение статистического подхода к определению понятия информации заключалось еще и в том, что в его рамках было получено первое определение информации, удовлетворительное в том числе и с философской точки зрения**:** *информация есть устраненная неопределенность*. По замечанию А.Д. Урсула:

«Если в наших знаниях о каком-либо предмете существует неясность, неопределенность, а получив новые сведения об этом предмете, мы можем уже более определенно судить о нем, то это значит, что сообщение содержало в себе информацию»[2]. А по мнению же французского ученого И. Ложе, указанное определение информации вообще является всеобъемлющим, так как оно, с его точки зрения, охватывает все уровни, на которых присутствует информация, будь то число градусов, характеризующих температуру, или выводы следственной комиссии .

Однако выделения в информации только количественного ее аспекта оказалось явно недостаточно. Как верно заметил В.А. Бокарев, в статистической теории информации установилось слишком абстрактное понимание информации, «сделавшее эту теорию, с одной стороны, предельно широкой, но с другой – мешающее ей стать наукой, исследующей информацию всесторонне»[4]. Все это заставило искать иные, более универсальные подходы к определению понятия информации.

Таким, по существу, другим, дополнительным подходом, стал подход кибернетический, охватывающий структуры и связи систем. С появлением кибернетики как науки «об общих законах преобразования информации в сложных управляющих системах» , способах восприятия, хранения,

`

С.11.

1 См.: Бриллюэн Л. Наука и теория информации. – М.: Физматгиз, 1960. –

См.: Урсул А. Д. Отражение и информация. – М.: Мысль, 1973. – С. 32.

См.: Ложе И. Информационные системы. Методы и средства/Пер. с фр. под ред. К.Л. Горфана, Т.В. Молчановой. – М.: Мир, 1979. – С. 10-20.

Бокарев В.А. Кибернетика и военное дело. Философский очерк. – М.: Воениздат, 1969. – С.105.

Глушков В.М. О кибернетике как науке//Кибернетика, мышление, жизнь. – М. : Мысль, 1964. – С. 53.

переработки и использования информации, термин «информация» стал научным понятием, своего рода инструментом исследования процессов управления.

Еще в 1941 году Н. Винер опубликовал свой первый труд об аналогиях между работой математической машины и нервной системы живого организма, а в 1948 году – фундаментальное исследование «Кибернетика, или управление и связь в животном и машине», предложив свое «информационное видение» кибернетики как науки об управлении и связи в живых организмах, обществе и машинах. Информация по Винеру – это «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших органов чувств» . Кибернетическая концепция подвела к необходимости оценить информацию как некоторое знание, имеющее одну ценностную меру по отношению к внешнему миру (*семантический аспект*), и другую – по отношению к получателю, накопленному им знанию, познавательным целям и задачам (*прагматический аспект*). Это обусловило формирование и развитие целого ряда *семантических* теорий информации.

и *прагматических*

Таким образом, становление и дальнейшее развитие различных учений об информации, взглядов и подходов к определению ее сущности привело к тому, что информация переросла из интуитивно понятной категории обыденного общения в категорию общенаучную, потребовавшую и своего философского осмысления. Попытки выработки не специально-научного, а философского определения информации, охватывающего все ее аспекты и не противоречащего ни одной из существующих частных теорий, привели к появлению концепций информации, базирующихся на такой философской категории, как «различие», «разнообразие».

Так, с точки зрения Грегори Бейтсона, впервые изложенной в его работе «Двойное послание», опубликованной в августе 1969 года, «Различимое различие *(a difference which make a difference – авт.)* есть идея.

`

Винер Н. Кибернетика и общество. – М.: Изд. ин. лит., 1958. – С. 31.

См., например: Carnap R., Bar-Hillel Y. Semantic Information//British J. for Philosopy of Science. – 1952. – v. 4. – pp. 147-157; Hintikka J. The Principles of Mathematics Revisited. – London: Cambridge University Press, 1996; Шрейдер Ю.А. Семиотические основы информатики. Лекции. Изд. 2-е, стереотип. – М.: ИПКИР, 1975.

3 См., например: Харкевич А.А. Избранные труды в 3 т. Т.3. Теория информации. Опознание образов. – М.: Наука, 1973; Бонгард М.М. Проблемы узнавания. – М.: Наука, 1967; Гришкин И.И. Понятие информации. Логико-методологический аспект. – М.: Наука, 1973.

Это «бит», единица информации» . Позднее этот подход автора к определению понятия информации нашел свое отражение и в других его работах.

«Бит» информации, – писал Грегори Бейтсон в работе «Кибернетика «Я»: теория алкоголизма», – можно определить как *различимое различие (a difference that makes a difference).* Такое различие, перемещающееся вдоль цепи и претерпевающее в ней последовательные трансформации, есть элементарная идея» .

По мнению автора, аргументы, лежащие в основе определения информации как «различимого различия», очевидны: «Очевидно, что разум не является совокупностью объектов или событий…Разум содержит в себе лишь трансформы, объекты (результаты) перцепции, образы и т.д…Воспринимаемый мир не может управляться различиями и образами, а только лишь «силами» и «импульсами». С другой стороны, мир формы и коммуникации управляется не материальными субстанциями, силами или импульсами, а лишь различиями и образами» .

К категории «различия» обратился и известный немецкий социолог и философ Никлас Луман при выработке своего подхода к определению понятия и сущности информации: «…Такое различие, которое существует в окружающей среде и которое порождает различие для самой системы…мы определим как информацию. Информация как «*различие, порождающее различие*» *(a difference which finds a difference – авт.)* всегда является собственным продуктом системы, аспектом принятия решения» .

Используя материал статистической теории информации в середине 50-х годов прошлого века У. Р. Эшби изложил концепцию разнообразия, суть которой заключается в утверждении, что теория информации изучает процессы «передачи разнообразия» по каналам связи, причем «информация не может передаваться в большем количестве, чем это позволяет количество разнообразия» .

5

`

Bateson G. Steps to an Ecology of Mind: collected essays in anthropology, psychiatry, evolution, and epistemology. – New York: Ballantine Books, 1972. – P. 271.

[2] Там же. – P. 375.

[3] Там же. – P. 271.

[4] Luhmann N. Organisation und Entscheidung. – Wiesbaden: Westdeutscher Verlag, 2000. – P. 173.

[5] См.: Ashby W. Ross. An Introduction to Cybernetics/Second Impression. – London: Chapman & Hall Ltd, 1957. – P. 152.

Таким образом, согласно этой концепции, *природа информации заключается в разнообразии, а количество информации выражает количество разнообразия*. По замечанию Б.В. Бирюкова, «Информация налицо там, где имеется разнообразие, неоднородность. Она «появляется» тогда, когда хотя бы два «элемента» в совокупности различаются, и она «исчезает», если объекты «склеиваются», «отождествляются» .

Подход к определению информации, близкий к концепции разнообразия, имеется и в работах академика В. М. Глушкова. Он характеризует информацию как *меру неоднородности в распределении энергии (или вещества) в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы* .

Развитием подхода к определению информации на основе понятия различия, разнообразия явилось установление связей между информацией и такой философской категорий, как «отражение». Под отражением в широком смысле понимается процесс и результат воздействия одной материальной системы на другую, который представляет собой воспроизведение в иной форме особенностей одной системы в особенностях другой . В соответствии с этим,

информация есть не что иное, как содержание отражения, т.е. те изменения, различия в отражающей системе, которые соответствуют внутренним различиям отражаемой системы. Однако при этом, как совершенно справедливо указывают некоторые авторы [4], нельзя смешивать два таких понятия, как «информация» и «отражение».

Данный подход к определению содержательного аспекта понятия информации получил наибольшее признание в научной среде. Исходя из анализа положений данного подхода можно сделать вывод, что:

- информация – это продукт материального взаимодействия объектов;
- информация не материальна;
- чем сложнее объект материального мира или процесс, тем больше информации он в себе несет.

`

Бирюков Б.В. Кибернетика и методология науки. – М.: Наука, 1974. – С. 243.

См.: Глушков В.М. Мышление и кибернетика//Вопросы философии. – 1963. – № 1. – С.36.

См.: Диалектический и исторический материализм/Под общ. ред. А.П. Шептулина. – М.: Политиздат, 1985. – С. 79.

См., например: Сетров М.И. Основы функциональной теории организации. Филос. очерк. – Л.: Наука, 1972. – С. 58; Коршунов А.М. Отражение, деятельность, познание. – М.: Политиздат, 1979. – С.39.

Вместе с тем рассмотренные подходы к определению понятия информации составляют лишь малую часть сформировавшихся к настоящему времени взглядов по данному вопросу, поскольку, как замечает Н.И. Жуков, «история науки, пожалуй, еще не знала такого широкого спектра разноречивых толкований, какой приходится на долю этой категории» .

Данное утверждение вполне справедливо и в отношении понятия «компьютерная информация»: действующее российское законодательство не содержит правового определения подобного рода информации, а в специальной литературе существуют различные точки зрения по поводу данной дефиниции.

Рассматривая информацию в качестве объекта правоотношений, нельзя не отметить то обстоятельство, что с точки зрения действующего российского законодательства информация представляет собой весьма специфический продукт, который может быть представлен как в материальном, так и в нематериальном виде.

Согласно ч. 2 ст. 2 **Федерального закона РФ от 20.02.1995 г. № 24ФЗ «Об информации, информатизации и защите информации»** , ***под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления***.

В этом законе, наряду с «информацией», законодатель выделяет еще один объект права – «информационный ресурс», который состоит из

«документированной информации» (документов), то есть информации, зафиксированной на материальном носителе с реквизитами, позволяющими ее идентифицировать. Причем, согласно статьи 5 закона, документирование информации, осуществляемое в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизации документов и их массивов, безопасность Российской Федерации является обязательным условием для ее включения в информационные ресурсы, которые, согласно статьи 4 закона, собственно и являются объектом регулируемых правом отношений и подлежат защите.

Таким образом, с позиций действующего законодательства документированная информация представляет собой такую организационную форму, которая может быть определена как единая совокупность:

а) содержания информации;

б) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры;

`

Жуков Н.И. Информация (Философский анализ информации – центрального понятия кибернетики). – Минск: Наука и техника, 1966. – С.39.

См.: Российская газета. – 1995. – 22 февр.

в) материального носителя информации, на котором ее содержание и реквизиты закреплены.

По замечанию В.А. Копылова, понятие «документированная информация» основано на «двуединстве – информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений…» .

Анализ специальной литературы позволяет сделать вывод о том, что все имеющиеся попытки конструирования понятия компьютерной информации осуществляются именно в рамках данного подхода.

Так, с точки зрения авторов комментария к Уголовному кодексу Российской Федерации *компьютерная информация – это информация, зафиксированная на машинном носителе*[2]

или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ .

У.А. Мусаева, рассматривая вопросы организации разыскной деятельности следователя по делам о преступлениях в сфере компьютерной информации, приходит к выводу, что эта информация характеризуется следующими обязательными признаками: всегда является интеллектуальной собственностью, не обладает натуральными физическими параметрами, охраняется законом, содержится в электронном виде на техническом носителе . По мнению автора,

компьютерная информация – это обработанные компьютером данные, полученные на его выходе в форме, доступной восприятию ЭВМ либо человека, или передающиеся по телекоммуникационным каналам [5].

`

См.: Копылов В.А. Информационное право: Учебное пособие. – М.: Юрист, 1997. – С.23.

К машинным носителям относятся всякого рода жесткие магнитные диски разных типов, которые являются частью системного блока ЭВМ или присоединяются к ней с помощью специальных устройств, гибкие магнитные диски (дискеты), оптические диски (компакт-диски), полупроводниковые схемы и т.п.

Комментарий к Уголовному кодексу Российской Федерации. Особенная часть.

Под общей редакцией Генерального прокурора Российской Федерации, профессора Ю.И. Скуратора и Председателя Верховного Суда Российской Федерации В.М. Лебедева. – М.: Издательская группа ИНФРА-М – НОРМА, 1996. – С.412.

Мусаева У.А. Розыскная деятельность следователя по делам о преступлениях в

сфере компьютерной информации: Автореф. дис.… канд. юрид. наук. – М., 2002. – С.8.

Там же.

С точки зрения В.С. Пущина компьютерная информация – это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ. При этом

автор подразделяет ее на смысловую (несущую в себе определенные сведения об окружающем мире) и управляющую (программные средства обеспечения) .

В исследовании В.В. Крылова, посвященного вопросам борьбы с информационными компьютерными преступлениями, под компьютерной информацией понимаются «сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях, – идентифицируемый элемент

информационной системы, имеющий собственника, установившего правила ее использования» .

Однако наиболее удачное определение компьютерной информации сформулировано В.А. Мещеряковым «информация, представленная в специальном виде, предназначенном и пригодном для ее автоматизированной обработки, хранения и передачи, находящуюся на материальном носителе и

имеющую собственника или иного законного владельца, установившего порядок ее создания (генерации), обработки, передачи и уничтожения» .

При этом под собственником информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения указанными объектами.

Владельцем же информационных ресурсов, информационных систем, технологий и средств их обеспечения является субъект, осуществляющий владение и

пользование указанными объектами и реализующий полномочия распоряжения ими в пределах, установленных законом.

И, наконец, пользователем (потребителем) информации признается субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

`

2000.

1 См. Пущин В.С. Преступления в сфере компьютерной информации. – М.,

Крылов В.В. Информационные компьютерные преступления. – М.: Издательская группа ИНФРА-М – НОРМА, 1996. – С.27.

3 Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: Автореф. дис.… док. юрид. наук. – Воронеж., 2001. – С.1415.

КРАТКАЯ ИСТОРИЯ РАЗВИТИЯ ЭВМ

. В середине и конце XIX века главным героем в истории вычислительной техники был англичанин Ч. Бэббедж – создатель аналитической машины, предвосхитивший в ней многие черты современных электронных вычислительных машин.

В первые сорок лет двадцатого столетия в вычислительной технике произошло не так уж много принципиально важных событий. Правда, конструкторы обратили внимание на возможность применения в счетных устройствах новых элементов – электромагнитных реле. В середине 30-х годов в Германии инженер К. Цузе построил вычислительное устройство, работающее на таких реле. К 1943 году была готова релейная машина

«Марк-I» (позднее «Марк-II»), которая воплощала в себе предельные параметры, свойственные этой элементной базе. «Марк-1» имел в длину 15 и в высоту 2,5 метра, содержал 800 тысяч деталей, располагал 60 регистрами для констант, 72 запоминающими регистрами для сложения, центральным блоком умножения и деления, мог вычислять элементарные трансцендентные функции. Машина работала с 23-значными десятичными числами и выполняла операции сложения за 0,3 секунды, а умножения – за 3 секунды. Примерно .в то же время в Англии начала работать первая вычислительная машина на реле, которая использовалась для расшифровки сообщений, передававшихся немецким кодированным передатчиком.

Работа по созданию электронной вычислительной машины была начата, по-видимому, в 1937 году в США профессором Джоном Атанасовым, болгарином по происхождению. Эта машина была специализированной и предназначалась для решения задач математической физики. В ходе разработок Атанасов создал и запатентовал первые электронные устройства, которые впоследствии применялись довольно широко в первых компьютерах. Полностью проект Атанасова не был завершен, однако через три десятка лет в результате судебного разбирательства профессора признали родоначальником электронной вычислительной техники.

Первая действующая машина, построенная на вакуумных лампах, официально введена в эксплуатацию 15 февраля 1946 года. В истории компьютеров она известна под названием ЭНИАК, ее авторами были американцы Эккерт и Моучли. Эту машину пытались использовать для решения некоторых задач, подготовленных фон Нейманом и связанных с проектом атомной бомбы. Затем она была перевезена на Абердинский испытательный полигон, где работала до 1955 года.

Представление о первом электронном компьютере дают следующие данные. Он содержал 18 тысяч вакуумных ламп, занимал площадь 9Х15 метров, весил 30 тонн и потреблял мощность 150 киловатт. ЭНИАК складывал числа за 0,2 миллисекунды (миллисекунда равна одной тысячной секунды), а перемножал за 2,8 миллисекунды. Это было примерно в тысячу раз быстрее, чем на релейных машинах. В компьютере использовалась десятичная система, он оперировал с десятиразрядными числами. ЭНИАК имел и существенный недостаток – управление им осуществлялось с помощью коммутационной панели. Для изменения программы оператор должен был переключить провода, что занимало не один день. Но подлинным бичом была ужасающая ненадежность компьютера, так как за день работы успевало выйти из строя около десятка вакуумных ламп.

ЭНИАК стал первым представителем первого поколения компьютеров. Любая классификация условна, но большинство специалистов согласилось с тем, что различать поколения следует исходя из тон элементной базы, на основе которой строятся машины. Таким образом, первое поколение представляется ламповыми машинами.

Необходимо отметить огромную роль американского математика фон Неймана в становлении техники первого поколения. Нужно было осмыслить сильные и слабые стороны ЭНИАКа и дать рекомендации для последующих разработок. В отчете фон Неймана и его коллег Г. Голдстайна и А. Беркса (июнь 1946 года) были четко сформулированы требования к структуре компьютеров, важнейшими из которых являются следующие:

- машины на электронных элементах должны работать не в десятичной, а в двоичной системе счисления;
- программа, как и исходные данные, должна размещаться в памяти машины;
- программа, как и числа, должна записываться в двоичном коде;
- трудности физической реализации запоминающего устройства, быстродействие которого соответствует скорости работы логических схем, требуют иерархической организации памяти (то есть выделения оперативной, промежуточной и долговременной памяти);
- арифметическое устройство (процессор) конструируется на основе схем, выполняющих операцию сложения; создание специальных устройств для выполнения других арифметических и иных операций нецелесообразно;
- в машине используется параллельный принцип организации вычислительного процесса (операции над числами производятся одновременно по всем разрядам).

В этой связи компьютер, прежде всего, должен иметь следующие устройства:

- АЛУ – арифметико – логическое устройство;
- УУ – устройство управления;
- ЗУ – запоминающее устройство;
- УВВ – устройства ввода – вывода;
- ПУ – пульт управления.

`

В современных ЭВМ АЛУ и УУ объединены в общее устройство, называемое центральным процессором. Обобщенная логическая структура ЭВМ показана на рис. 1.

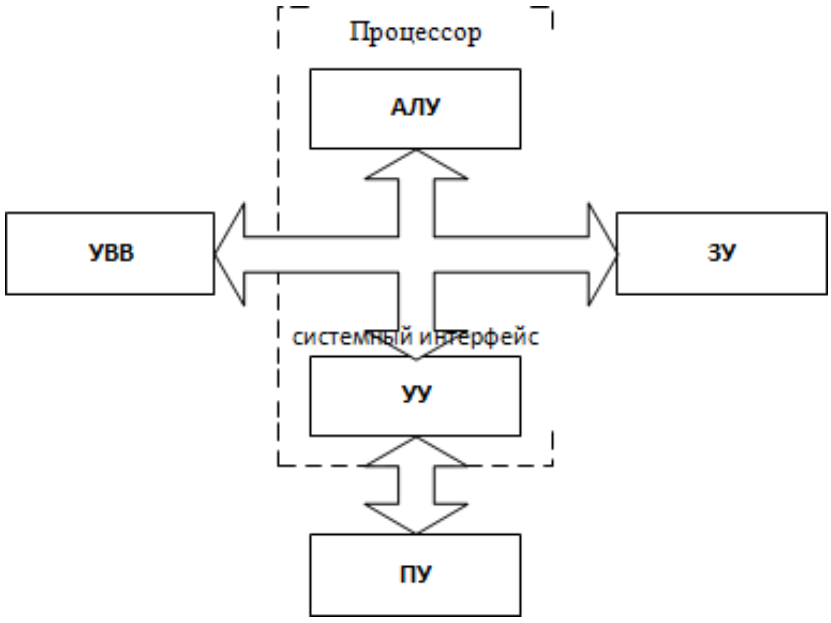


Рис. 1. Обобщенная логическая структура ЭВМ по фон Нейману.

Практически все рекомендации фон Неймана впоследствии использовались в машинах первых трех поколений, их совокупность получила название

«архитектура фон Неймана».

Новые машины первого поколения сменяли друг друга довольно быстро. В 1951 году заработала первая советская электронная вычислительная машина МЭСМ. В 1952 году на свет появилась американская машина ЭДВАК. Стоит также отметить построенный ранее, в 1949 году, английский компьютер ЭДСАК – первую машину с хранимой программой. В 1952 году советские конструкторы ввели в эксплуатацию БЭСМ – самую быстродействующую машину в Европе, а в следующем году в СССР начала работать

«Стрела» – первая в Европе серийная машина высокого класса. Среди создателей отечественных машин в первую очередь следует назвать имена С.А. Лебедева, Б.Я. Базилевского, И.С. Брука, Б.И. Рамеева, В.А. Мельникова, М.А. Карцева, А.Н. Мямлина.

В конце 50-х годов Джеком Килби была разработана первая интегральная микросхема. В 1965 году появились миникомпьютеры. Они уже не были всецело предназначены для обработки данных и решения задач; зачастую они входили как составные части в системы, требовавшие быстрого принятия решения, – *системы*

реального времени.

Элементной базой машин второго поколения стали полупроводники. Без сомнения, транзисторы можно с основанием считать одним из наиболее впечатляющих чудес XX века. Первые исследования в области полупроводниковых элементов провели в конце 30-х годов И. Мотт (Англия), А. С. Давыдов (СССР), В. Шотки (Германия). Патент на открытие транзистора был выдан в 1948 году американцам Д. Бардину и У. Браттейну, а через восемь лет они вместе с теоретиком В. Шокли стали лауреатами Нобелевской премии. Впоследствии было создано много типов транзисторов, но эта тема заслуживает отдельного разговора. Сейчас же важно отметить, что скорости переключения уже первых транзисторных элементов оказались в сотни раз выше, чем ламповых, надежность и экономичность – тоже.

Благодаря перечисленным достоинствам, транзисторы нашли применение в конструкциях машин второго поколения. Приблизительно на два порядка возросло их быстродействие, на несколько порядков величины улучшились показатели надежности и приблизительно на порядок возросла плотность монтажа. Намного уменьшилась относительная стоимость ЭВМ (то есть стоимость в пересчете на производительность), резко снизилась потребляемая мощность, улучшились условия эксплуатации.

Скачкообразное улучшение характеристик немедленно привело к существенному расширению областей применения полупроводниковых машин. Так, впервые стало возможным устанавливать ЭВМ на движущихся объектах (кораблях, самолетах и т. д.), В свою очередь, это увеличило спрос на них и оказалось мощным фактором, стимулирующим рост парка ЭВМ. Одним из таких стимуляторов стало эффективное применение машин в космических исследованиях в СССР и в США. Например, в 1961 году наземные компьютеры фирмы «Бэрроуз» управляли космическими полетами ракет «Атлас», а машины фирмы IBM контролировали полет астронавта Гордона Купера. Под контролем ЭВМ проходили полеты беспилотных кораблей типа «Рейнджер» к Луне в 1964 году, а также корабля «Маринер» к Марсу. Аналогичные функции выполняли и

советские компьютеры.

Наиболее яркими представителями второго поколения были машины СТРЕТЧ (США, 1961), «Атлас» (Англия, 1962), БЭСМ-6 (СССР, 1966).

Пожалуй, построение таких систем, имевших в своем составе около 10 переключательных элементов, было бы просто невозможным на основе ламповой техники. Второе поколение рождалось в недрах первого, перенимая многие его черты. Первая 1 бортовая ЭВМ для установки на межконтинентальной ракете «Атлас» была введена в эксплуатацию в США в 1955 году. В машине использовалось 20 тысяч транзисторов и диодов, она потребляла 4 киловатта. Первые серийные универсальные ЭВМ на транзисторах были выпущены в 1958 году одновременно в США, ФРГ и Японии.

В Советском Союзе первые безламповые машины «Сетунь», «Раздан» и «Раздан-2» были созданы в 1959-1961 годах. В 60-х годах советские конструкторы разработали около 30 моделей транзисторных компьютеров, большинство которых стали выпускаться серийно. Наиболее мощный из них – «Минск-32» – выполнял 65 тысяч операций в секунду. Появились целые семейства машин: «Урал», «Минск», БЭСМ. Рекордсменом среди ЭВМ второго поколения стала БЭСМ-6, имевшая быстродействие около миллиона операций в секунду, – одна из самых производительных в мире. Архитектура и многие технические решения в этом компьютере были настолько прогрессивными и опережающими свое время, что он успешно используется до сих пор. Интересно, что огромная производительность БЭСМ-6 обеспечивалась при умеренных аппаратных затратах (в серийном варианте машины содержится всего 60 тысяч транзисторов и 200 тысяч диодов).

Таким образом, созрели условия для перехода к новой технологии, которая позволила бы приспособиться к растущей сложности схем путем исключения традиционных соединений между их элементами. Идея интегральных схем носилась в воздухе. Еще в 1952 году английский электронщик Г. Даммер пророчески утверждал: «С появлением транзистора и работ в области полупроводниковой техники вообще можно себе представить электронное оборудование в виде твердого блока, не содержащего соединительных проводов. Блок может состоять из слоев изолирующих, проводящих, выпрямляющих и

усиливающих материалов, в которых определенные участки вырезаны таким образом, чтобы они могли непосредственно выполнять электрические функции».

Приоритет в изобретении интегральных схем, ставших элементной базой ЭВМ третьего поколения, принадлежит американским ученым Д. Килби и Р. Нойсу, сделавшим это открытие независимо друг от друга. В начале 1959 года Килби окончил разработку интегрального триггера (переключательной схемы из двух активных элементов) на кусочке монолитного германия размерами 1,6х9,5 миллиметра. Это достижение специалисты встретили скептически. Р. Нойс после сообщения о твердом триггере высказал идеи, используя которые удалось уже через год получить первые образцы интегрированных логических элементов.

Массовый выпуск интегральных схем начался в 1962 году. Были разработаны методы автоматизированного изготовления шаблонов-масок, через которые слой за слоем на исходные пластины производили напыление элементов интегральных схем. В процессе развития электронно-лучевой литографии удалось добиться того, что рисунок на шаблон наносился в. натуральную величину с помощью микроскопического электронного луча. Уже в 1964 году было объявлено о планах выпуска дешевого настольного калькулятора, в котором вместо 21 тысячи дискретных элементов (как в обычных калькуляторах) предполагалось использовать 29 интегральных схем. Средним показателем степени интеграции в то время можно было считать возможность размещения 16-

20 транзисторов на кристалле размером 1,25Х1,25 миллиметра. Уже упоминавшийся ЭНИАК в 1971 году мог бы быть собран на пластине в полтора квадратных сантиметра. Началось перевоплощение электроники в микроэлектронику.

Первая массовая серия машин на интегральных элементах стала выпускаться в 1964 фирмой IBM. Эта серия, известная под названием IBM360, оказала значительное влияние на развитие вычислительной техники второй

половины 60-х годов. Она объединила целое семейство ЭВМ с широким диапазоном производительности, причем совместимых друг с другом. Последнее означало, что машины стало возможно связывать в комплексы, а также без всяких

переделок переносить программы, написанные для одной ЭВМ, на любую другую из этой серии. Таким образом, впервые было выявлено коммерчески выгодное требование стандартизации аппаратного и программного обеспечения ЭВМ.

В СССР первой серийной ЭВМ на интегральных схемах была машина «Наири-3», появившаяся в 1970 году. Со второй половины 60-х годов Советский Союз совместно со странами СЭВ приступил к разработке семейства универсальных машин, аналогичного системе IZBM-360. В 1972 году началось серийное производство стартовой, наименее мощной модели Единой системы – ЭВМ ЕС-1010, а еще через год – пяти других моделей. Их быстродействие находилось в пределах от десяти тысяч (ЕС-1 010) до двух миллионов (ЕС-1 060) операций в секунду.

Начало 70-х годов знаменует переход к компьютерам четвертого поколения – на сверхбольших интегральных схемах (СБИС). Другим признаком ЭВМ нового поколения являются резкие изменения в архитектуре. С появлением в 1971 году микропроцессоров началась эра программируемой логики. В эту эру понятия программирования и принципы проектирования логических схем сблизились настолько, что их взаимопроникновение потребовало и от ученых, и от инженеров полного понимания как принципов программирования, так и аппаратуры. Только при этом условии можно было успешно использовать все заложенные в микропроцессорах возможности.

Началом развития микропроцессорных средств вычислительной техники считается 1972 год, когда компании Intel Corporation удалось создать интегральную схему с полным набором элементов, характерным для центрального процессора. Размер слова первого МП составлял всего 4 бита, т.е. длину двоично-кодированного десятичного числа. В калькуляторах, промышленных системах управления и некоторых других устройствах МП приходится использовать только двоично-десятичные числа. Поэтому

использование 4-разрядного МП явилось идеальным решением.
Этот микропроцессор содержал 2250 транзисторов, размещенных на кристалле с размерами 3х4 мм. Он обрабатывал четырехразрядные слова в среднем за 10 мкс.

Через год появился 8-разрядный микропроцессор, а затем улучшенный его вариант (Intel-8000), оснащенный интегральными схемами памяти и другими компонентами, что привело к созданию первых программируемых микропроцессоров для управления производственными процессами.

Первый отечественный микропроцессор появился в 1974 году.

В дальнейшем почти за тридцатилетний период развития микропроцессорных средств вычислительной техники как за рубежом, так и в нашей стране были созданы сотни различных моделей универсальных микропроцессоров общего назначения.

Исторически принято считать, что презентация первого персонального компьютера состоялась 01 апреля 1976 года. Он был разработан и создан в примитивной мастерской, расположившейся в обыкновенном гараже, двумя американскими техниками Стефаном Возняком и Стивом Джобсом. Это было первое подобие маленького, но многообещающего компьютера. Первый персональный компьютер получил название «APPLE». Стив Джобс впоследствии основал известную фирму «Эппл компьютер». Разумеется, четко определить границу между интегральными схемами и СБИС трудновато, так как технология интеграции развивается непрерывно, например, за 20 лет в США зарегистрированы 237 технологических нововведений, из них 67 революционных.

Точно так же непрерывно улучшаются параметры интегральных схем, однако в случае СБИС интеграция не может быть бесконечно большой и ограничивается физическими законами.

ОСНОВНЫЕ СПОСОБЫ ХРАНЕНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Как совершенно верно отмечается в специальной литературе, основные способы хранения компьютерной информации следует рассматривать в двух аспектах: логическом и техническом

. Логический аспект имеет в виду

организацию и хранение данных в компьютере. Технический – основные устройства персонального компьютера, в которых хранится информация.

Как известно, компьютер может обрабатывать только информацию, представленную в числовой форме. Вся другая информация (например, звуки, изображения, показания приборов и т. д.) для обработки на компьютере должна быть преобразована в числовую форму. Для представления этой информации в компьютерах используется двоичная система счисления. В ЭВМ используют двоичную систему потому, что она имеет ряд преимуществ перед другими:

- для ее реализации используются технические *элементы с двумя возможными состояниями* (есть ток – нет тока, намагничен – не намагничен);
- представление информации посредством только двух состояний *надежно и помехоустойчиво*;
- возможно *применение аппарата булевой алгебры* для выполнения логических преобразований информации;
- двоичная арифметика проще десятичной (двоичные таблицы сложения и умножения предельно просты).

`

1 Расследование неправомерного доступа к компьютерной информации/Под ред. Н.Г. Шурухнова. – М.: Издательство «Щит-М», 1999. – С.15.

При вводе информации в компьютер специальными аппаратными и программными средствами каждый символ преобразуется в двоичный код. При выводе информации осуществляется обратное преобразование: двоичный код каждого символа преобразуется в привычный пользователю символ (например, букву или цифру).

Рост объемов перерабатываемой с помощью вычислительной техники информации требует четкой организации процессов хранения, обработки и передачи данных. Поэтому вся компьютерная информация должна быть упорядочена определенным образом и иметь стройную структуру. Минимальной единицей информационной записи, хранящейся в ЭВМ, является **бит** – сокращение от английских слов *binary digit,* что означает двоичная цифра.

В компьютерной технике бит соответствует физическому состоянию носителя информации: намагничено – не намагничено, есть отверстие – нет отверстия. При этом одно состояние принято обозначать цифрой 0, а другое – цифрой 1. Выбор одного из двух возможных вариантов позволяет также различать логические истину и ложь. Последовательностью битов можно закодировать текст, изображение, звук или какую-либо другую информацию.

В информатике также часто используется величина, называемая **байтом** (byte) и равная 8 битам. В большинстве современных ЭВМ при кодировании каждому символу соответствует своя последовательность из восьми нулей и единиц, т. е. байт. Соответствие байтов и символов задается с помощью таблицы, в которой для каждого кода указывается свой символ. Так, например, в широко распространенной кодировке Koi8-R буква «М» имеет код 11101101, буква «И» – код 11101001, а пробел – код 00100000.

Наряду с байтами, для измерения количества информации используются более крупные единицы:

1 Кбайт (один килобайт) = 2^{10} байт = 1024 байта;

1 Мбайт (один мегабайт) = 2^{10} Кбайт = 1024 Кбайта; 1 Гбайт (один гигабайт) = 2 Мбайт = 1024 Мбайта.

При хранении информации в памяти ЭВМ она структурируется в файлы. Основное назначение файлов – хранить информацию. Они также предназначены для передачи данных от программы к программе и от системы к системе. Другими словами, файл – это хранилище стабильных и мобильных данных. Но файл – это

нечто большее, чем просто хранилище данных. Обычно файл имеет *имя, атрибуты, время модификации и время создания.*

Следует отметить, что понятие файла менялось с течением времени. Операционные системы первых больших ЭВМ представляли файл как хранилище для базы данных, и поэтому файл являлся набором записей. Обычно все записи в файле были одного размера, часто по 80 символов каждая. При этом много времени уходило на поиск и запись данных в большой файл.

В конце 60-х годов наметилась тенденция к упрощению операционных систем, что позволило использовать их на менее мощных компьютерах. Это нашло свое отражение и в развитии операционной системы Unix. В Unix под файлом понималась *последовательность байтов.* Стало легче хранить данные на диске, так как не надо было запоминать размер записи. Unix оказал очень большое влияние на другие операционные системы персональных компьютеров. Почти все они поддерживают идею Unix о том, что файл – это просто последовательность байтов. Файлы, представляющие собой поток данных, стали использоваться при обмене информацией между компьютерными системами. Если используется более сложная структура файла (как в операционных системах OS/2 и Macintosh), она всегда может быть преобразована в поток байтов, передана и на другом конце канала связи воссоздана в исходном виде.

Итак, ***файл*** *– это ограниченное поименованное место для хранения информации, которое существует на физическом (дискета, лазерный диск, винчестер) либо виртуальном (оперативная память, виртуальный логический диск) носителе в ЭВМ, системе ЭВМ или в сетях ЭВМ.*

Способ, которым информация организована в байты, называется *форматом файла.*

Для того чтобы прочесть файл, например, электронной таблицы, необходимо знать, каким образом байты представляют числа (формулы, текст) в каждой ячейке; чтобы прочесть файл текстового редактора, надо знать, какие байты представляют символы, а какие шрифты или поля, а также другую информацию.

Программы могут хранить данные в файле таким способом, какой выберет программист. Зачастую предполагается, однако, что файлы будут использоваться различными программами. По этой причине многие прикладные программы поддерживают некоторые наиболее распространенные форматы, так что другие программы могут понять данные в файле. Компании по производству программного обеспечения (которые хотят, чтобы их программы стали «стандартами»), часто публикуют информацию относительно форматов, которые они создали, чтобы их можно было бы использовать в других приложениях.

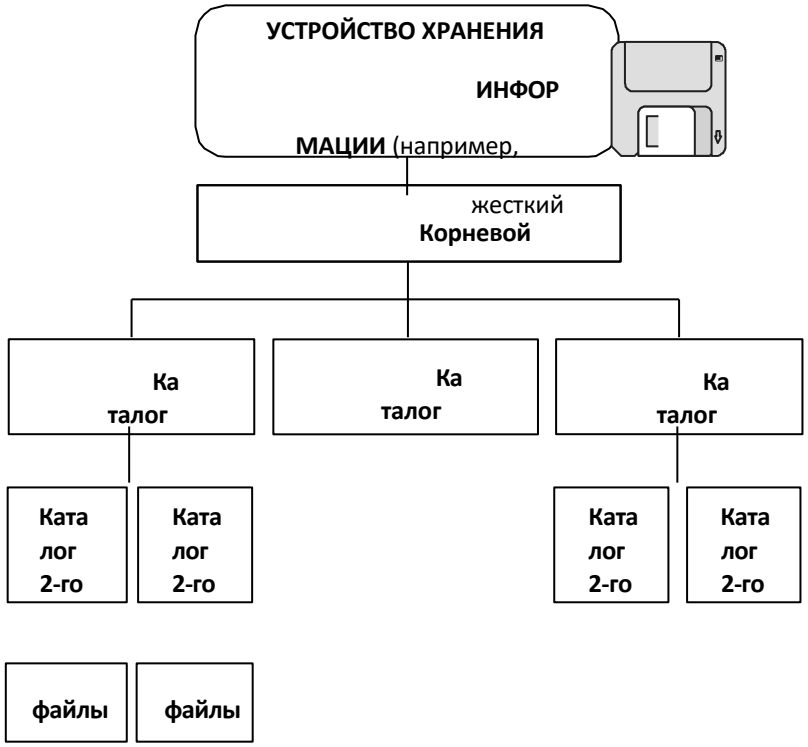
Все файлы условно можно разделить на две части – текстовые и двоичные. **Текстовые** файлы – наиболее распространенный тип данных во всем компьютерном мире. Для хранения каждого символа чаще всего отводится один байт, а кодирование текстовых файлов выполняют с помощью специальных таблиц, в которых каждому символу соответствует определенное число, не превышающее 255. Файл, для кодировки которого используется только 127 первых чисел, называется **ASCII-файлом** (сокращение от American Standard Code for Information Interchange – американский стандартный код для обмена информацией), но в таком файле не могут быть представлены буквы, отличные от латиницы (в том числе и русские). Большинство национальных алфавитов можно закодировать с помощью восьмибитной таблицы. Для русского языка наиболее популярны на данный момент три кодировки: Koi8-R, Windows-1251 и так называемая, альтернативная (alt) кодировка.

Но чисто текстовые файлы встречаются все реже. Люди хотят, чтобы документы содержали рисунки и диаграммы и использовали различные шрифты. В результате появляются форматы, представляющие собой различные комбинации текстовых, графических и других форм данных.

Двоичные файлы, в отличие от текстовых, не так просто просмотреть, и в них обычно нет знакомых нам слов – лишь множество непонятных символов. Эти файлы не предназначены непосредственно для чтения человеком. Примерами двоичных файлов являются исполняемые программы и файлы с графическими изображениями.

Вся совокупность файлов, хранящихся в памяти компьютера или любом ином носителе, определенным образом структурирована. *Файловая структура* представляет собой систему хранения файлов на запоминающем устройстве, например, диске. Файлы организованы в каталоги (иногда называемые директориями или папками). Каталог – это специальное место на диске, в котором хранятся имена файлов, сведения о размере файлов, времени их последнего обновления, атрибуты (свойства) файлов и т.д. Любой каталог может содержать произвольное число подкаталогов, в каждом из которых могут храниться файлы и другие каталоги.

При форматировании диска (подготовке его к работе) на нем формируется один главный, или корневой, каталог. В нем регистрируются файлы и подкаталоги – каталоги 1-го уровня. В каталогах 1-го уровня регистрируются файлы и каталоги 2-го уровня и т.д. Получается иерархическая древообразная структура каталогов на магнитном диске (рис. 2).



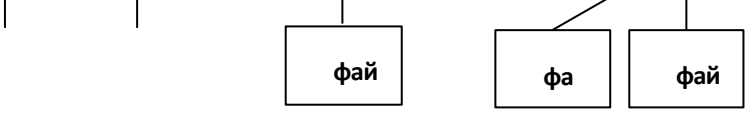


Рис. 2. Схема организации структуры каталогов

Каталог, с которым в настоящее время работает пользователь, называется текущим. Число уровней подкаталогов – до 256.

Кратко рассмотрев содержание основных способов хранения компьютерной информации в логическом аспекте, полагаем необходимым рассмотреть эти вопросы и в технической плоскости.

В минимальный состав любого компьютера входят три устройства: *системный блок*, *клавиатура*, *монитор (дисплей)*. Системный блок представляет собой основной узел, внутри которого установлены наиболее важные компоненты компьютера. Устройства, находящиеся внутри системного блока, называют *внутренними,* а устройства, подключаемые к нему снаружи, называют *внешними.* Внешние дополнительные устройства, предназначенные для ввода, вывода и длительного хранения данных, также называют *периферийными.*

Внутри системного блока. ***Материнская плата (системная плата, motherboard)*** – важнейшая часть компьютера, с помощью которой осуществляется взаимодействие между различными устройствами системы. На ней расположены основные элементы, такие, как:

- *процессор* – основная микросхема, выполняющая большинство математических и логических операций;
- *микропроцессорный комплект (чипсет)* – набор микросхем, управляющих работой внутренних устройств компьютера и определяющих основные функциональные возможности материнской платы;
- *шины* – наборы проводников, по которым происходит обмен сигналами между внутренними устройствами компьютера;
- *оперативная память (оперативное запоминающее устройство, ОЗУ)* – набор микросхем, предназначенных для временного хранения данных, когда компьютер включен;
- *ПЗУ (постоянное запоминающее устройство* BIOS*)* – микросхема, предназначенная для длительного хранения данных, в том числе и когда компьютер выключен;

- *контроллеры*;
- разъемы для подключения дополнительных устройств *(слоты).*

Рассмотрим наиболее важные из вышеперечисленных элементов подробнее.

Процессор – основная микросхема компьютера, в которой и производятся все вычисления. Конструктивно процессор состоит из ячеек, похожих на ячейки оперативной памяти, но в этих ячейках данные могут не только храниться, но и изменяться. Внутренние ячейки процессора называют регистрами. Важно также отметить, что данные, попавшие в некоторые регистры, рассматриваются не как данные, а как команды, управляющие обработкой данных в других регистрах. Среди регистров процессора есть и такие, которые в зависимости от своего содержания способны модифицировать исполнение команд. Таким образом, управляя засылкой данных в разные регистры процессора, можно управлять обработкой данных. На этом и основано исполнение программ.

С остальными устройствами компьютера и, в первую очередь, с оперативной памятью, процессор связан несколькими группами проводников, называемых шинами. Основных шин три: шина данных, адресная шина и командная шина.

Основными параметрами процессоров являются *рабочее напряжение, разрядность, рабочая тактовая частота, коэффициент внутреннего умножения тактовой частоты* и размер *кэш-памяти.*

Рабочее напряжение процессора обеспечивает материнская плата, поэтому разным маркам процессоров соответствуют разные материнские платы (их надо выбирать совместно). По мере развития процессорной техники происходит постепенное понижение рабочего напряжения. Ранние модели процессоров x86 имели рабочее напряжение 5 В. С переходом к процессорам Intel Pentium оно было понижено до 3,3 В, а в настоящее время оно составляет менее 3 В. Причем ядро процессора питается пониженным напряжением 2,2 В. Понижение рабочего напряжения позволяет уменьшить расстояния между структурными элементами в

кристалле процессора до десятитысячных долей миллиметра, не опасаясь электрического пробоя. Пропорционально квадрату напряжения уменьшается и тепловыделение в процессоре, а это позволяет увеличивать его производительность без угрозы перегрева.

Разрядность процессора показывает, сколько бит данных он может принять и обработать в своих регистрах за один раз *(за один такт).* Первые процессоры x86 были 16-разрядными. Начиная с процессора 80386, они имеют 32-разрядную архитектуру. Современные процессоры семейства Intel Pentium остаются 32-разрядными, хотя и работают с 64-разрядной шиной данных (разрядность процессора определяется не разрядностью шины данных, а разрядностью командной шины).

В основе работы процессора лежит тот же тактовый принцип, что и в обычных часах. Исполнение каждой команды занимает определенное количество тактов. В настенных часах такты колебаний задает маятник; в ручных механических часах их задает пружинный маятник; в электронных часах для этого есть колебательный контур, задающий такты строго определенной частоты. В персональном компьютере тактовые импульсы задает одна из микросхем, входящая в микропроцессорный комплект (чипсет), расположенный на материнской плате. Чем выше частота тактов, поступающих на процессор, тем больше команд он может исполнить в единицу времени, тем выше его производительность. Первые процессоры x86 могли работать с частотой не выше 4,77 МГц, а *сегодня рабочие частоты* некоторых процессоров уже превосходят 500 миллионов тактов в секунду (500 МГц).

Тактовые сигналы процессор получает от материнской платы, которая, в отличие от процессора, представляет собой не кристалл кремния, а большой набор проводников и микросхем. По чисто физическим причинам материнская плата не может работать со столь высокими частотами, как процессор. Сегодня ее предел составляет 100-133 МГц. Для получения более высоких частот в процессоре происходит *внутреннее умножение частоты* на коэффициент 3; 3,5; 4; 4,5; 5 и более.

Обмен данными внутри процессора происходит в несколько раз быстрее, чем обмен с другими устройствами, например, с оперативной памятью. Для того чтобы уменьшить количество обращений к оперативной памяти, внутри процессора создают буферную область – так называемую *кэш-память.* Это как бы

«сверхоперативная память». Когда процессору нужны данные, он сначала обращается в кэш-память, и только если там нужных данных нет, происходит его обращение в оперативную память. Принимая блок данных из оперативной памяти, процессор заносит его одновременно и в кэш-память. «Удачные» обращения в кэш-память называют *попаданиями в кэш.* Процент попаданий тем выше, чем больше размер кэш-памяти, поэтому высокопроизводительные процессоры комплектуют повышенным объемом кэш-памяти.

Нередко кэш-память распределяют по нескольким уровням. Кэш первого уровня выполняется в том же кристалле, что и сам процессор, и имеет объем порядка десятков Кбайт. Кэш второго уровня находится либо в кристалле процессора, либо в том же узле, что и процессор, хотя и исполняется на отдельном кристалле. Кэш-память первого и второго уровня работает на частоте, согласованной с частотой ядра процессора.

Кэш-память третьего уровня выполняют на быстродействующих микросхемах типа *SRAM* и размещают на материнской плате вблизи процессора. Ее объемы могут достигать нескольких Мбайт, но работает она на частоте материнской платы.

Оперативная память (RAM – Random Access Memory) – это массив кристаллических ячеек, способных хранить данные. Существует много различных типов оперативной памяти, но с точки зрения физического принципа действия различают *динамическую память (DRAM)* и *статическую память (SRAM).*

Ячейки динамической памяти (DRAM) можно представить в виде микроконденсаторов, способных накапливать заряд. Это наиболее распространенный и экономически доступный тип памяти. Недостатки этого типа связаны, во-первых, с тем, что как при заряде, так и при разряде конденсаторов неизбежны переходные процессы, то есть запись данных происходит

сравнительно медленно. Второй важный недостаток связан с тем, что заряды ячеек имеют свойство рассеиваться в пространстве, причем весьма быстро. Если оперативную память постоянно не «подзаряжать», утрата данных происходит через несколько сотых долей секунды. Для борьбы с этим явлением в компьютере происходит постоянная *регенерация (освежение, подзарядка)* ячеек оперативной

памяти. Регенерация осуществляется несколько десятков раз в секунду и вызывает непроизводительный расход ресурсов вычислительной системы.

Ячейки статической памяти (SRAM) можно представить как электронные микроэлементы – *триггеры,* состоящие из нескольких транзисторов. В триггере хранится не заряд, а состояние *(включен/выключен),* поэтому этот тип памяти обеспечивает более высокое быстродействие, хотя технологически он сложнее и соответственно дороже.

Микросхемы динамической памяти используют в качестве основной оперативной памяти компьютера. Микросхемы статической памяти используют в качестве вспомогательной памяти (так называемой *кэш-памяти),* предназначенной для оптимизации работы процессора.

Постоянное запоминающее устройство (ПЗУ). В момент включения компьютера в его оперативной памяти нет ничего: ни данных, ни программ, поскольку оперативная память не может ничего хранить без подзарядки ячеек более сотых долей секунды, но процессору нужны команды, в том числе и в первый момент после включения.

Поэтому сразу после включения на адресной шине процессора выставляется стартовый адрес. Это происходит аппаратно, без участия программ (всегда одинаково). Процессор обращается по выставленному адресу за своей первой командой и далее начинает работать по программам. Этот исходный адрес не может указывать на оперативную память, в которой пока ничего нет. Он указывает на другой тип памяти — *постоянное запоминающее устройство (ПЗУ).* Микросхема ПЗУ способна длительное время хранить информацию, даже когда компьютер выключен. Программы, находящиеся в ПЗУ, называют «зашитыми» — их записывают туда на этапе изготовления микросхемы.

Комплект программ, находящихся в ПЗУ, образует *базовую систему ввода- вывода (BIOS – Basic Input Output System).* Основное назначение программ этого пакета состоит в том, чтобы проверить состав и работоспособность компьютерной системы и обеспечить взаимодействие с клавиатурой, монитором, жестким диском

и дисководом гибких дисков. Программы, входящие в *BIOS,* позволяют нам наблюдать на экране диагностические сообщения, сопровождающие запуск компьютера, а также вмешиваться в ход запуска с помощью клавиатуры.

Накопители на жестких магнитных дисках (HDD) – основное устройство для долговременного хранения больших объемов данных и программ. На самом деле это не один диск, а группа соосных дисков, имеющих магнитное покрытие и вращающихся с высокой скоростью. Таким образом, этот «диск» имеет не две поверхности, как должно быть у обычного плоского диска, а 2n поверхностей, где *n* – число отдельных дисков в группе.

Над каждой поверхностью располагается головка, предназначенная для чтения-записи данных. При высоких скоростях вращения дисков (90 об/с) в зазоре между головкой и поверхностью образуется аэродинамическая подушка, и головка парит над магнитной поверхностью на высоте, составляющей несколько тысячных долей миллиметра. При изменении силы тока, протекающего через головку, происходит изменение напряженности динамического магнитного поля в зазоре, что вызывает изменения в стационарном магнитном поле ферромагнитных частиц, образующих покрытие диска. Так осуществляется запись данных на магнитный диск.

Операция считывания происходит в обратном порядке. Намагниченные частицы покрытия, проносящиеся на высокой скорости вблизи головки, наводят в ней ЭДС самоиндукции. Электромагнитные сигналы, возникающие при этом, усиливаются и передаются на обработку.

Управление работой жесткого диска выполняет специальное аппаратно-логическое устройство – *контроллер жесткого диска.* В прошлом оно представляло собой отдельную *дочернюю плату,* которую подключали к одному из свободных слотов материнской платы. В настоящее время функции контроллеров дисков выполняют микросхемы, входящие в микропроцессорный комплект (чипсет), хотя некоторые виды высокопроизводительных контроллеров жестких дисков по-прежнему поставляются на отдельной плате.

К основным параметрам жестких дисков относятся *емкость* и *производительность*. Емкость дисков зависит от технологии их изготовления. В

настоящее время большинство производителей жестких дисков используют изобретенную компанией *IBM* технологию с использованием *гигантского магниторезистивного эффекта (GMR — Giant Magnetic Resistance).* Теоретический предел емкости одной пластины, исполненной по этой технологии, составляет порядка 20 Гбайт. В настоящее время достигнут технологический уровень 6,4 Гбайт на пластину, но развитие продолжается.

Накопители на гибких магнитных дисках (HDD). Информация на жестком диске может храниться годами, однако иногда требуется ее перенос с одного компьютера на другой. Несмотря на свое название, жесткий диск является весьма хрупким прибором, чувствительным к перегрузкам, ударам и толчкам. Теоретически переносить информацию с одного рабочего места на другое путем переноса жесткого диска возможно, и в некоторых случаях так и поступают, но все-таки этот прием считается нетехнологичным, поскольку требует особой аккуратности и определенной квалификации.

Для оперативного переноса небольших объемов информации используют так называемые *гибкие магнитные диски* (дискеты), которые вставляют в специальный накопитель – *дисковод.* Приемное отверстие накопителя находится на лицевой панели системного блока. Правильное направление подачи гибкого диска отмечено стрелкой на его пластиковом кожухе.

Основными параметрами гибких дисков являются *технологический размер* (измеряется в дюймах), *плотность записи* (измеряется в кратных единицах) и *полная емкость*.

Первый компьютер *IBM PC* (родоначальник платформы) был выпущен в 1981 году. К нему можно было подключить внешний накопитель, использующий односторонние гибкие диски диаметром 5,25 дюйма. Емкость диска составляла 160 Кбайт. В следующем году появились аналогичные двусторонние диски емкостью 320 Кбайт. Начиная с 1984 года, выпускались гибкие диски 5,25 дюйма высокой плотности (1,2 Мбайт). В наши дни диски размером 5,25 дюйма не используются, и соответствующие дисководы в базовой конфигурации персональных компьютеров после 1994 года не поставляются.

Гибкие диски размером 3,5 дюйма выпускают с 1980 года. Односторонний диск *обычной плотности* имел емкость 180 Кбайт, двусторонний

– 360 Кбайт, а *двусторонний двойной плотности* – 720 Кбайт. Ныне стандартными считают диски размером 3,5 дюйма *высокой плотности.* Они имеют емкость 1440 Кбайт (1,4 Мбайт) и маркируются буквами *HD (high density – высокая плотность).*

С нижней стороны гибкий диск имеет центральную втулку, которая захватывается шпинделем дисковода и приводится во вращение. Магнитная поверхность прикрыта сдвигающейся шторкой для защиты от влаги, грязи и пыли. Если на гибком диске записаны ценные данные, его можно защитить от стирания и перезаписи, сдвинув защитную задвижку так, чтобы образовалось открытое отверстие. Для разрешения записи задвижку перемещают в обратную сторону и перекрывают отверстие. В некоторых случаях для безусловной защиты информации на диске задвижку выламывают физически, но и в этом случае разрешить запись на диск можно, если, например, заклеить образовавшееся отверстие тонкой полоской липкой ленты.

Гибкие диски считаются малонадежными носителями информации. Пыль, грязь, влага, температурные перепады и внешние электромагнитные поля очень часто становятся причиной частичной или полной утраты данных, хранившихся на гибком *диске.* Поэтому использовать гибкие диски в качестве основного средства хранения информации недопустимо. Их используют только для транспортировки информации или в качестве дополнительного (резервного) средства хранения.

Дисковод компакт-дисков (CD-ROM). В период 1994-1995 годах в базовую конфигурацию персональных компьютеров перестали включать дисководы гибких дисков диаметром 5,25 дюйма, но вместо них стандартной стала считаться установка дисковода *CD-ROM,* имеющего такие же внешние размеры.

Аббревиатура *CD-ROM (Compact Disc Read-Only Memory)* переводится на русский язык как *постоянное запоминающее устройство на основе компакт-диска.* Это устройство, являющееся частью компьютера, которое осуществляет считывание данных с компакт-дисков. В настоящее время все программные

комплексы, игры, энциклопедии и т. д. распространяются на компакт-дисках. Привод CD-ROM также может использоваться и для проигрывания аудиодисков.

Цифровая запись на компакт-диске отличается от записи на магнитных дисках очень высокой плотностью, и стандартный компакт-диск может хранить примерно 650 Мбайт данных. Большие объемы данных характерны для *мулътимедийной информации* (графика, музыка, видео), поэтому дисководы *CD- ROM* относят к аппаратным средствам мультимедиа. Программные продукты, распространяемые на лазерных дисках, называют *мультимедийными изданиями.* Сегодня мультимедийные издания завоевывают все более прочное место среди других традиционных видов изданий. Так, например, существуют книги, альбомы, энциклопедии и даже периодические издания (электронные журналы), выпускаемые на *CD-ROM.*

Основным недостатком стандартных дисководов *CD-ROM является* невозможность записи данных, но параллельно с ними существуют и устройства однократной записи *CD-R (Compact Disk Recorder),* и устройства многократной записи *CD-RW.* В настоящее время существуют восемь типов накопителей *CD*:

- *CD-ROM* – постоянное запоминающее устройство (ПЗУ);
- *CD-WORM* – накопители, обеспечивающие однократную запись информации на компакт-диск;
- *CD-W* – «пишущие» накопители;
- *CD-RW* – «пишущие» и «читающие» накопители;
- *DVD-ROM* – (*Digital Versatile Disk*) – *ROM*;
- *DVD-R* – (*Digital Versatile Disk*) – *R* (*write once*);
- *DVD-RAM* – (*Digital Versatile Disk*) – *RW*;
- *DVD-RW* – (*Digital Versatile Disk*) – *RW*.

Важнейшими элементами современного компьютера являются также ***периферийные устройства***. К ним относятся всевозможные устройства обмена информацией между памятью компьютера и его «внешним» миром.

К числу периферийных устройств относятся, прежде всего, *клавиатура* и *дисплей*, предназначенные для ввода и вывода символьной информации.

Кроме них, в состав компьютера могут входить следующие устройства:

- ❑ *принтер*, предназначенный для вывода информации на бумажный носитель;
- ❑ *графопостроитель* – устройство для вывода графической информации на бумагу;
- ❑ *сканер* – устройство для оптического считывания текстовой и графической информации;
- ❑ *манипуляторы* (джойстик, мышь трекбол), облегчающие ввод информации в компьютер;
- ❑ *сетевые адаптеры* – устройства для подключения персонального компьютера к сети;
- ❑ *модем* – устройство для передача компьютерной информации по каналам связи и т.д.

Вместе с тем особую ценность компьютеру придает не только его аппаратная часть, являющаяся его материальной базой, но и программы, которые установлены на эту базу. Такое разделение на аппаратную и программную части позволило превратить компьютер в универсальное средство обработки информации. На одной и той же базе можно получить компьютеры с самыми различными возможностями именно благодаря замене на них программных компонентов.

Под ***программой*** понимают объективную форму представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы,

полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения (ст. 1 Закона Российской Федерации от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»).

Программное обеспечение компьютера – это совокупность программ, предназначенных для выполнения различных действий. В состав программного обеспечения входят программы и необходимые для их функционирования данные. Различают системные программы, предназначенные для управления и обслуживания компьютера, и несистемные – программы (приложения). Все программы состоят из совокупности операторов и данных, описанных на некотором языке программирования, и создаются с помощью инструментальных программ. Все программы хранятся в файлах в виде либо текста программы на определенном языке программирования, либо в виде исполняемой программы. В первом случае для выполнения программы необходимо наличие транслятора или соответствующей системы программирования. Во втором случае для выполнения программы достаточно просто запустить ее.

Программное обеспечение принято классифицировать на три группы: п

- системное;
- прикладное;
- инструментальное

Системное программное обеспечение. В состав компьютера входит большое число функциональных элементов, таких, как оперативная память, процессор, контроллеры, внешние запоминающие устройства, периферийные устройства и др. Для эффективного управления работой этими устройствами как системой используют программы, получившие название системными или системное программное обеспечение. Без системного программного обеспечения работа на компьютере невозможна.

Операционные системы. Основой системного программного обеспечения является операционная система (ОС), предназначенная для управления аппаратными и

программными ресурсами компьютера, а также для организации взаимодействия (интерфейса) пользователя с компьютером. Операционная система представляет собой набор программ, хранимых в виде файлов на диске. Она автоматически загружается в оперативную память при включении и остается там до выключения компьютера. Эта операция загрузки выполняется загрузчиком программой, которая вызывается базовой системой ввода-вывода (BIOS). BIOS размещается в постоянном запоминающем устройстве (ПЗУ), к которому доступ пользователя запрещен. Кроме вызова программы загрузчика BIOS также выполняет тестирование основных аппаратных компонентов. BIOS иногда относят к аппаратным средствам, иногда к программным. В зависимости от аппаратных ресурсов компьютера различают однозадачные и многозадачные ОС, ОС с текстовым и графическим интерфейсом. К однозадачным ОС с текстовым интерфейсом относят ОС, такие, как MS DOS, к многозадачным с графическим интерфейсом – UNIX, WINDOWS 98/2000/NT. Многозадачные ОС управляют, распределяют ресурсы компьютера и обеспечивают:

- *процессор* – основная микросхема, выполняющая большинство математических операций;
- возможность одновременной или поочередной работы нескольких программ;
- возможность обмена данными между программами;
- возможность совместного использования ресурсов компьютера несколькими программами.

Основные функции операционных систем заключаются в обеспечении удобного взаимодействия пользователя с аппаратным и программным обеспечением компьютера:

- организация и управление файловой системой (системой размещения файлов на диске);
- установка, удаление, запуск программ;
- обслуживание аппаратных ресурсов компьютера (с помощью дополнительных программ).

Примером часто используемых дополнительных программ по обслуживанию файловой системы и аппаратных ресурсов компьютера являются программы архивации файлов

Прикладное программное обеспечение. Прикладное программное обеспечение используется для решения задач определенной прикладной области. В качестве примеров можно привести системы тестирования знаний, системы автоматизации бухгалтерских расчетов, системы мониторинга, системы анализа эффективности инвестиций, системы документооборота, системы автоматизации рабочих мест, программы по учету потерь и многое другое. Разработка таких систем выполняется в несколько этапов и осуществляется на основе инструментального программного обеспечения.

Инструментальное программное обеспечение. Инструментальное программное обеспечение предназначено для создания программных продуктов общего назначения, не зависящих от предметной прикладной области. Программный продукт – это некоторый файл, содержащий информацию, полученную с помощью программы. Программный продукт может содержать как элементы информационного обеспечения , например, массив чисел и формул, список фамилий, текст документа, базы данных, так и элементы программного обеспечения, к которой относят прикладные программы, призванные сами создавать программные продукты. Различают следующие виды инструментальных программ:

- текстовые и графические редакторы;
- трансляторы языков программирования, системы программирования;
- системы управления базами данных;
- электронные таблицы;
- программы создания электронных презентаций и др.

Следует отметить, что оболочки для создания прикладных программ создаются также инструментальными программами и поэтому могут быть отнесены к прикладным программам.

ОСНОВНЫЕ СРЕДСТВА ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Широкое внедрение ЭВМ в область практической деятельности предопределило необходимость организации эффективного обмена данными между различными пользователями и приложениями. Это обусловило появление и развитие компьютерных сетей, создаваемых как в рамках небольшой организации, так и охватывающих компьютеры, находящиеся друг от друга на расстоянии в сотни, а то и тысячи километров.

Самая простая сеть состоит как минимум из двух компьютеров, соединенных друг с другом кабелем, что позволяет им совместно использовать данные. Все сети (независимо от сложности) основываются именно на этом простом принципе. Хотя идея соединения компьютеров с помощью кабеля не кажется нам особо выдающейся, в свое время она явилась значительным достижением в области коммуникаций.

Группа соединенных компьютеров и других устройств называется сетью. А концепция соединенных и совместно использующих ресурсы компьютеров носит название сетевого взаимодействия.

Компьютеры, входящие в сеть, могут совместно использовать:

- данные;
- сообщения;
- принтеры;
- факсимильные аппараты;
- модемы;
- другие устройства.

Этот список постоянно пополняется, т.к. возникают новые способы совместного использования ресурсов.

Несмотря на то, что все сети имеют определенное сходство, они разделяются на два типа:

- ❑ *одноранговые*;
- ❑ *на основе выделенного сервера*.

В одноранговой сети все компьютеры равноправны: нет иерархии среди компьютеров и нет выделенного сервера. Обычно каждый компьютер функционирует и как клиент, и как сервер; иначе говоря, нет отдельного компьютера, ответственного за всю сеть. Пользователи сами решают, какие данные на своем компьютере сделать доступными по сети.

Одноранговые сети чаще всего объединяют не более 10 компьютеров. Отсюда их другое название – рабочая группа, т.е. небольшой коллектив пользователей.

Однако промышленным стандартом в настоящее время являются сети с выделенным сервером. Выделенным называется такой сервер, который функционирует только как сервер и не используется в качестве клиента или рабочей станции. Он оптимизирован для быстрой обработки запросов от сетевых клиентов и для повышения защищенности файлов или каталогов.

Круг задач, который должны выполнять серверы, многообразен и сложен. Чтобы серверы отвечали современным требованиям пользователей, в больших сетях их делают специализированными. Например, в сети Windows NT могут работать различные типы серверов:

- *серверы файлов и печати* – управляют доступом пользователей к файлам и принтерам;
- *серверы приложений.* На этих серверах выполняются прикладные задачи клиент-серверных приложений, а также находятся данные доступные клиентам;
- *почтовые серверы* – управляют сообщениями электронной почты между серверами сети;
- серверы факсов – управляют потоком входящих и исходящих факсимильных сообщений через один или несколько факс-модемов;
- *коммуникационные серверы (серверы связи)* – управляют проходящим через модем и телефонную линию потоком данных и почтовых сообщений между своей сетью и другими сетями, мэйнфреймами или удаленными пользователями;
- *серверы служб каталога* – содержат данные о серверах, позволяя пользователям находить, сохранять и защищать информацию в сети.

Все сети строятся на основе трех базовых топологий (физическое расположение компьютеров, кабелей и других сетевых компонентов):

- *шина*;
- *звезда*;
- *кольцо*.

Шинная топология сети. Топологию «шина» часто называют «линейной шиной». В ней используется один кабель, именуемый магистралью или сегментом, к которому подключены все компьютеры сети. Данная топология является наиболее простой и распространенной реализацией сети.

Самая простая форма топологии физической шины представляет собой один основной кабель, оконцованный с обеих сторон специальными типами разъемов – терминаторами. При создании такой сети основной кабель прокладывают последовательно от одного сетевого устройства к другому. Сами устройства подключаются к основному кабелю с использованием подводящих кабелей и Т-образных разъемов. Пример такой топологии приведен на рисунке 3.

терминаторы предотвращают появление отраженного сигнала

сеть

отрезок кабеля

Рис. 3. Шинная топология компьютерной сети

В сети с топологией «шина» компьютеры адресуют данные конкретному компьютеру, передавая их по кабелю в виде электрических сигналов. Данные виды электрических сигналов передаются всем компьютерам сети; однако информацию принимает только тот компьютер, чей адрес соответствует адресу получателя, зашифрованному в этих сигналах. Причем в каждый момент времени вести передачу может только один компьютер.

Топология компьютерной сети типа «звезда». При топологии «звезда» все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту – концентратору. Сигнал от передающего компьютера поступает через концентратор ко всем остальным (рис. 3.1).

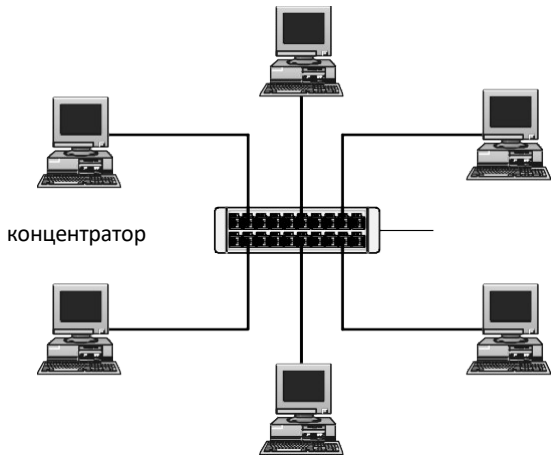


Рис. 3.1. Звездообразная топология компьютерной сети

В сетях с топологией «звезда» подключение компьютеров к сети выполняется централизованно. Но есть и недостаток: т.к. все компьютеры подключены к центральной точке, для больших сетей значительно увеличивается расход кабеля. К тому же, если центральный компонент выйдет из строя, остановится вся сеть. А если выйдет из строя только один компьютер (или кабель, соединяющий его с

концентратором), то лишь этот компьютер не сможет передавать или принимать данные по сети. На остальные компьютеры по сети

этот сбой не повлияет.

Топология компьютерной сети типа «кольцо». При топологии «кольцо» компьютеры подключаются к кабелю. Сигналы передаются по кольцу в одном направлении и проходят через каждый компьютер. В отличие от пассивной топологии «шина» здесь каждый компьютер выступает в роли повторителя, усиливая сигналы и передавая их следующему компьютеру. Поэтому, если выйдет из строя один компьютер, прекращает функционировать вся сеть.

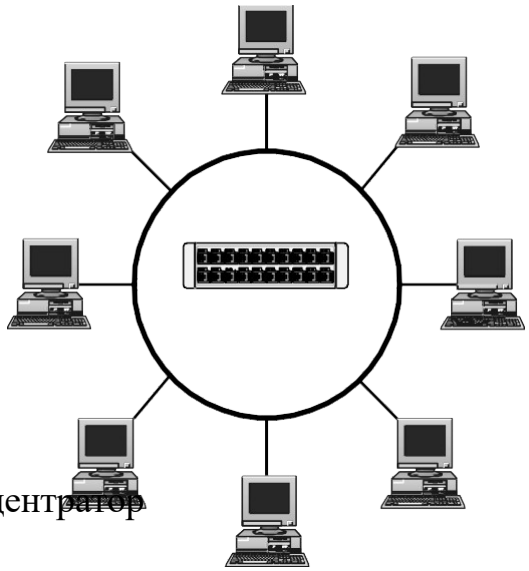


Рис. 4. Кольцевая топология компьютерной сети

В настоящее время при компоновке сети все чаще используется комбинированная топология, которая сочетает отдельные свойства шин, звезды и кольца.

Говоря о средствах передачи компьютерной информации, нельзя не сказать несколько слов и о таком явлении наших дней, как глобальная компьютерная сеть **Интернет**.

История Интернет отсчитывается с момента создания департаментом безопасности США (Department of Defense – DoD) специального исследовательского подразделения (Advanced Research Project AgencyARPA). Это подразделение было создано в ответ на запуск первого спутника бывшим СССР. Агентство ARPA, позже переименованное в DARPA, спонсировало научные

исследования, посвященные созданию средств, обеспечивающих возможность использования нескольких университетских суперкомпьютеров множеством научно-исследовательских институтов США по всей стране. В 1969 году появилась первая компьютерная сеть, получившая название ARPANET. Эта сеть обеспечивала взаимодействие института в Стэнфорде (Stanford Research Institute), института UC Santa Barbara в Калифорнии с университетом штата Юта. Спустя некоторое время, к сети присоединились новые организации.

Сейчас Интернет является крупнейшей мировой сетью, состоящей из сотен различных сетей и насчитывающей миллионы подключенных к ней компьютеров по всему миру. Связанные между собой сети и компьютеры принадлежат частным людям, государственным агентствам, коммерческим фирмам, университетам, школам, больницам и другим различным организациям, работающим по всему миру. Ежедневно миллионы пользователей посылают и получают электронную почту, скачивают файлы, занимаются исследованиями и делают свой бизнес в Интернет. По оценкам экспертов, рост рынка сервисов электронной коммерции (E-commerce) оценивается в несколько миллиардов долларов в течение ближайших нескольких лет.

Благодаря повсеместному распространению и популярности Интернет, множество ее технологий были взяты на вооружение во внутренние корпоративные сети различных организаций. Две наиболее значимые технологии, взятые из Интернет, –

это семейство протоколов TCP/IP и сервис World Wide Web (WWW), базирующийся на протоколах HTTP и HTML. Эти технологии и схемы адресации тесно интегрированы в существующие сети и будут являться основой будущего в компьютерной индустрии.

Впервые о компьютерных преступлениях в России заговорили более 20 лет назад. Так, в 1979 г. в г. Вильнюсе на одном из предприятий было совершено хищение денежных средств с использованием ЭВМ на сумму свыше 78000 рублей. При том, что для абсолютного большинства служащих месячная заработная плата в то время составляла в среднем 200 рублей, названная сумма

равнялась заработку за 30 лет. Этот случай был занесен в международный реестр, уже тогда учитывающий уголовные компьютерные правонарушения.

Однако уже в период с 1991 по 1995 года правоохранительными органами было возбуждено десять уголовных дел по фактам совершения тяжких преступлений с использованием компьютерной техники. По данным МВД России, в 1997 году было зарегистрировано уже 309 преступлений, совершенных с применением компьютерной техники, программ для ЭВМ, цифровых средств электросвязи и магнитных носителей, в 1998 году их было свыше 500, а с 1999 года наметилась устойчивая тенденция ежегодного увеличения их числа на 25- 30%. Вот лишь некоторые, наиболее «выдающиеся» компьютерные преступления, совершенные отечественными злоумышленниками за последние двенадцать лет.

1991 год. В конце августа в Москве была пресечена деятельность преступной группы, состоявшей из начальника отдела автоматизации неторговых операций Вычислительного центра ВЭБ СССР Е. и сотрудника данного отдела Б., которой было осуществлено хищение 125,5 тыс. долларов США во

«Внешэкономбанке» (ВЭБ) СССР и подготовлено хищение еще свыше 500 тыс. Имея неконтролируемый доступ к компьютерным программам, обеспечивающим автоматическую переоценку банком остатков денежных средств в иностранной валюте к курсу рубля по счетам клиентов ВЭБ, преступниками были умышленно внесены в них несанкционированные изменения, в результате которых курсовая разница по счетам лиц, обслуживаемых ВЭБ, стала негласно завышаться.

Полученные таким образом денежные средства аккумулировались преступниками на нескольких определенных счетах, открытых Б. по подложным паспортам и справкам. По мере начисления с помощью тех же поддельных документов Б. получал валюту наличными и делился с Е., которому впоследствии удалось скрыться от следствия и суда. Б. же был осужден судом к 11,5 годам лишения свободы, однако освобожден по амнистии в 1994 году.

1992 год. Отечественным преступным группировкам с помощью средств электронно-вычислительной техники, соответствующего программного обеспечения и новейших электронных средств спутниковой связи удалось подключиться к международной подпольной банковской системе для проведения собственных расчетно-кассовых операций в целях финансового обеспечения преступной деятельности.

1993 год. В сентябре совершена попытка хищения с технологического счета ГРКЦ ГУ ЦБ по г. Москве более 68 млрд. руб. Механизм совершения преступления заключался в несанкционированном доступе в систему обработки платежей и введении в программу фиктивных данных о перечислении по 12 платежам на счета 8 коммерческих банков г. Москвы указанной суммы. Данные действия сопровождались изготовлением и предъявлением в банки фальшивых платежных поручений с поддельными печатями ГРКЦ.

В г. Черкесске Карачаево-Черкесской Республики оператором ЭВМ отдела автоматизации банковской информации Уникомбанка Д. было совершено хищение 82,5 тыс. рублей путем имитации отключения компьютерной программы, автоматически начисляющей процентные ставки на суммы кредитов, выдаваемых банком своим клиентам.

1994 год. Хищение в особо крупных размерах 122 тыс. дол. США из филиала «Чистые пруды» АКБ «Инкомбанк», совершенное главным бухгалтером отдела валютных операций В. Способ совершения преступления аналогичный способу хищения денежных средств во ВЭБ СССР в 1991 году.

В апреле экономист учетно-операционного отдела РКЦ г. Махачкала А. в сговоре с главным экономистом того же отдела И. и неустановленными лицами оформила

фиктивные мемориальные ордера. Затем, используя компьютерную систему и некорреспондирующий счет, она осуществила проводку 8 млрд неденоминированных рублей на корреспондирующие счета 4 коммерческих банков, обслуживаемых данным РКЦ. Счета были открыты по поддельным документам на несуществующие лица. Деньги были сняты со счетов участниками преступной группы.

Несколькими месяцами позднее мир узнал о так называемом «деле Владимира Левина», отнесенном международной уголовной полицией к категории «транснациональных сетевых компьютерных преступлений». С конца

июня по октябрь международная организованная преступная группа в составе 12 человек (10 граждан Российской Федерации и русских по происхождению и 2 – граждан Нидерландов), используя Интернет и сеть передачи данных

«Спринт/Теленет», вводила в систему управления наличными фондами «Ситибанка» (Нью-Йорк) ложные сведения. Группа действовала через персональные компьютеры, установленные в офисе АО «Сатурн», принадлежащего на правах частной собственности жителям СанктПетербурга В.Левину и А. Галахову. Преодолев семь рубежей многоконтурной защиты от несанкционированного доступа, преступники попытались осуществить 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка, находящихся в 9 странах мира (США, Канаде, Мексике, Аргентине, Новой Зеландии, Колумбии, Гонконге, Индонезии и Уругвае) на счета, расположенные в США, Финляндии, Израиле, Швейцарии, Германии, России, Нидерландах. Однако реально им удалось похитить только 400 тыс. долларов, после чего их преступная деятельность была пресечена. Следствие так и не смогло установить, каким образом главному исполнителю замысла В.Левину удалось получить доступ к двойным паролям и идентификационным кодам клиентов, используемым в системе управления денежными операциями

«Сити банка».

1995 год. В начале года в Зеленограде Московской области неустановленные лица совершили несанкционированный доступ в систему передачи платежных документов из ОСБ в ОПЕРУ, увеличив первоначальную сумму на 2 млрд. руб.

путем изготовления фиктивного сообщения и переданного повторно с неустановленного места по линии «Инфотел». На следующий день при сверки сообщений был выявлен факт передачи поддельного платежного документа на указанную сумму через Автобанк для Стройинвеста. При попытке снятия денег преступление было предотвращено.

Летом 1995 года факт совершения компьютерного преступления был зафиксирован и в Калининградской области. Отделение одного из банков в г. Калининграде стало его жертвой летом 1995 г. По некоторым данным,

незаконный вход в банковскую систему произошел через американскую сеть международных денежных переводов. Внеся изменения в производимые расчеты, преступники перевели 10 тысяч долларов США в банки Литвы, где впоследствии их получили наличными.

1996 год. В марте сотрудниками ГУВД г. Москвы было предотвращено хищение с использованием средств электронно-вычислительной техники. В банковскую систему были внедрены четыре поддельных векселя с реквизитами Московского филиала «С.» банка России на сумму 20 млрд. рублей. В ходе расследования было установлено, что общая сумма предотвращенного ущерба составила 375 млрд. 80 млн. рублей. К уголовной ответственности было привлечено 9 участников организованной преступной группы.

В сентябре лицам, входящим в состав организованной преступной группы, по заказу одной московской коммерческой структуры с целью устранения конкурента удалось организовать и провести следующую криминальную операцию. Свыше десяти сетевых операторов одновременно осуществили незаконный доступ к информационно-вычислительной системе австрийского банка и блокировали его работу в течение рабочего дня. Данные лица использовались «в темную» и не знали об истинной цели виртуального нападения. В момент максимальной дезорганизации электронной системы банка главный исполнитель совершил ряд несанкционированных финансовых операций, приведших к падению делового рейтинга и репутации этого кредитно- финансового учреждения. Операции были профессионально закамуфлированы под законные. Все это обошлось «заказчику» в 25 тыс. долларов США.

1997 год. В начале января неизвестные преступники с внутреннего счета волгоградского коммерческого банка «К.» отправили по сети передачи данных фиктивное платежное поручение на сумму 500 млн 125 тыс. рублей в адрес филиала московского «И.Банка», находящегося в городе Волжском Волгоградской области, на счет частного предпринимателя Ч. Этот человек получил наличными 200 млн руб. из приведенной выше суммы и по контракту передал их представителю фиктивной фирмы «П.», представившему поддельные документы на имя несуществующего лица.

В октябре месяце 17-летний студент московского технического вуза Ш., раздобыв на хакерской странице в Интернете программу для генерирования номеров пластиковых карт и паролей доступа к специальным карточным счетам (Pin-кодов), совершил покупки компьютерных аксессуаров в ряде американских виртуальных магазинов на сумму 11 тыс. долларов США. При оплате заказанного товара он указал выданные программой по соответствующему криптоалгоритму числа, идентифицирующие реально не существующего плательщика. В 1998 году преступник был осужден Нагатинским районным судом г. Москвы на пять лет лишения свободы условно.

1998 год. В сентябре сотрудниками отделения ГУЭП МВД России по борьбе с хищениями денежных средств, совершаемых с использованием ЭВМ и компьютерной информации, удалось раскрыть мошенничество, ущерб по которому превысил 20 тыс. долл. США. Организатор преступления – студент гуманитарного московского вуза Г. незаконно скопировал обнаруженную им в Интернете специализированную программу «PC Authorise», отвечающую за проведение бухгалтерских операций по оплате товаров, покупаемых в виртуальных магазинах, с помощью кредитных карт. Г. стал выступать в роли двойника-фантома подлинного магазина. Во время сеанса работы в Интернете Г. договорился с В. и его другом Ф. – студентами-сокурсниками одного из московских технических вузов, проживающими в одном доме в Мытищах, о соучастии и роли каждого в совершении преступлений. Так, В. на свое имя открыл несколько специальных карточных счетов, на которые Г. переводил похищенные денежные средства. Ф., в свою очередь, отвечал за обналичивание денег, поступающих на эти счета, из

которых 40% оставались в распоряжении двоих подручных, а 60% в дипломате помещались в ту или иную ячейку камеры хранения различных железнодорожных вокзалов, согласно указаниям Г. по сотовому телефону.

1999 год. Летом суд города Березняки Пермской области заслушал дело бывшего работника отделения Сбербанка Ч-на, безработного Ч-го и двух их

находящихся в розыске подельников, проникших в электронную систему местного отделения Сбербанка и похитивших более 1,5 млрд неденоминированных рублей.

Ч-н работал на должности старшего инженера с функциями администратора безопасности системы расчетов по пластиковым картам системы

«Сберкарт» с лета 1996 года, но через год неожиданно уволился, заблокировав перед этим пароль базы данных. Затем им была написана программа, позволявшая делать так называемое безадресное зачисление средств: при подключении компьютера через модем по телефонной сети в любой точке за пределами банка программа автоматически, без участия оператора, при помощи средств идентификации вносила изменения в таблицу остатков на счетах с известными номерами. После отражения денежных изменений на пластиковые карты через банкомат программа приводила таблицу в первоначальный вид. Тем временем остальные члены преступной группы по краденому паспорту открыли два карточных счета в различных отделениях Сбербанка.

Реализовать задуманное было решено с телефона общего знакомого Т., которому было обещано вознаграждение в сумме 5 млн рублей. Через березняковский Сбербанк преступники зачислили на открытый ими счет 2 млрд рублей, после чего стали обналичивать их через банкоматы в Перми, Санкт- Петербурге и Москве, пока их преступная деятельность не была пресечена.

2000 год. В январе неизвестным преступником, назвавшимся «19-летним Максимом из России», был осуществлен несанкционированный доступ к базе данных американской фирмы «Си-Ди юниверс», торгующей через Интернет музыкальными компакт-дисками с использованием пластиковых платежно-расчетных карт, в результате чего им незаконно были скопированы основные

реквизиты 300 тысяч пластиковых карт и их держателей, являвшихся клиентами указанной компании. После этого он за 100 тысяч долларов США предложил фирме ликвидировать прорехи в ее системе защиты от несанкционированного доступа, пообещав в противном случае продать незаконно полученную им информацию и предать данный случай огласке, что в дальнейшем и было им сделано.

Проведенный ретроспективный анализ компьютерной преступности свидетельствует о том, что наиболее «привлекательным» сектором российском экономики для преступников является кредитно-финансовая система. Наиболее типичными способами совершения преступлений с использованием компьютерной техники в этой сфере являются следующие:

- ❑ наиболее распространенными являются компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей;
- ❑ за последнее время не отмечено ни одно компьютерное преступление, которое было бы совершено одним человеком. Более известны случаи, когда преступными группировками нанимались бригады из хакеров, которым предоставлялось отдельное охраняемое помещение, оборудованное по последнему слову техники, для того, чтобы они осуществляли хищение крупных денежных средств путем несанкционированного проникновения в компьютерные сети крупных коммерческих банков;
- ❑ большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков. Результаты исследовании, проведенных с привлечением банковскою персонала, показывают, что доля таких преступлении приближается к 70% от общего количества преступлении в банковской сфере [1].

Изложенные выше факты позволяют говорить уже не о каких-то единичных случаях совершения компьютерных преступлений, а уже о настоящей «эпидемии». По данным начальника Управления по борьбе с преступлениями в сфере высоких технологий ГУВД Москвы Дмитрия Чепчугова, в 2000 г. в России

было зарегистрировано уже 1 тыс. 11 преступлений в сфере высоких технологий (в том числе и компьютерных преступлений), хотя в 1999 г. подобных преступлений было всего 287. При этом компьютерная преступность перестает быть внутренней проблемой только России. По сведениям ФБР, русские хакеры

уже похитили со счетов американских банков и корпораций миллионы долларов «электронных денег», не говоря уже о похищенных объектах интеллектуальной собственности, общая стоимость которых составляет миллиарды долларов.

В ближайшие несколько лет специалистами Интерпола прогнозируется резкий рост числа компьютерных преступлений. Анализ социальных предпосылок, характерных для России, позволяет подтвердить этот прогноз. При этом необходимо учитывать высокий уровень профессиональной подготовки российских программистов, а также то, что большинство из них в ходе преобразований российской экономики покинули государственные предприятия, ушли в коммерцию, в том числе и в такие структуры, которые занимаются не совсем честным бизнесом.

Итак, что же такое компьютерное преступление? Как представляется, под ***компьютерным преступлением следует понимать предусмотренное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного ее собственником или государством порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба владельцу информации или автоматизированной системы, в которой эта информация генерируется (создается), обрабатывается, передается или уничтожается, или повлекло иные тяжкие последствия.***

`

1 См.: Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ- Петербург, 2000. – С.4.

Как известно, существенную помощь в исследовании какого-либо предмета оказывает проведение классификации этого предмета или явления. В самом общем случае все многообразие видов преступлений в сфере компьютерной информации можно подразделить на две основные группы:

- ❑ преступления, в которых компьютер используется как *средство совершения преступлений*;
- ❑ преступления, в которых компьютер является *предметом преступных посягательств*.

Однако следует отметить, что в специальной литературе приводится значительное количество и иных классификаций преступлений в сфере компьютерной информации[1]. Так, например, в зависимости от мотивов совершения преступных деяний компьютерные преступления могут быть подразделены на следующие виды (рис. 5):

1. ***корыстные:***
   - совершенные из чувства мести;
   - с целью получения денежной выгоды;
   - совершенные из хулиганских побуждений;
   - терроризм;
2. ***неумышленные***:
   - совершенные из любопытства;
   - совершенные с целью самоутверждения.

Значительный опыт уголовно-правовой классификации преступлений в сфере компьютерной информации, накопленный в ведущих промышленно развитых государствах мира, вылился в появление списков, называемых «Минимальный список нарушений» и «Необязательный список нарушений». Они были разработаны государствами – участниками Европейского сообщества и официально оформлены как «Руководство Интерпола по компьютерной преступности».

Так, «Минимальный список нарушений» содержит восемь основных видов

компьютерных преступлений:

- компьютерное мошенничество;
- подделка компьютерной информации;
- повреждение данных ЭВМ или программ ЭВМ;
- компьютерный саботаж;
- несанкционированный доступ;

`

См., например: Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991; Крылов В.В. Информационные компьютерные преступления. – М.: ИнфраМ-НОРМА, 1997.

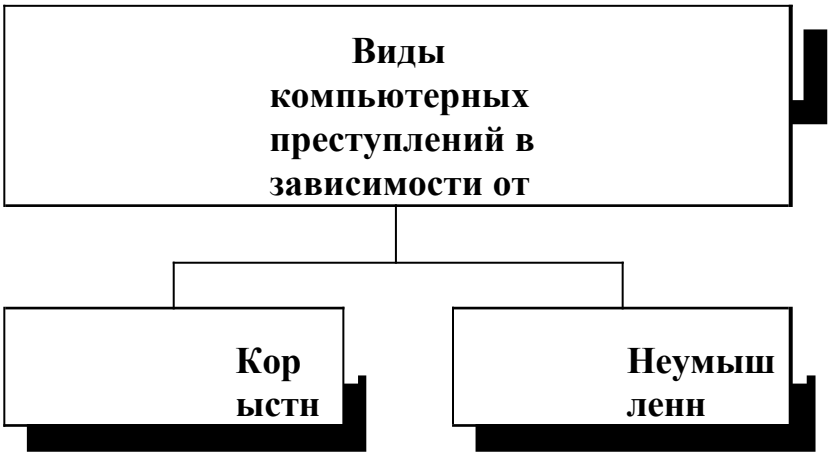


Рис. 5. Классификация компьютерных преступлений в зависимости от мотивов их совершения

- несанкционированный перехват данных;
- несанкционированное использование защищенных компьютерных программ;
- несанкционированное воспроизведение схем.

«Необязательный список» включает в себя четыре вида компьютерных преступлений:

- изменение данных ЭВМ или программ ЭВМ;
- компьютерный шпионаж;
- неразрешенное использование ЭВМ;
- неразрешенное использование защищенной программы ЭВМ. Еще одной из наиболее распространенных классификаций преступлений в сфере компьютерной информации является кодификатор Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время

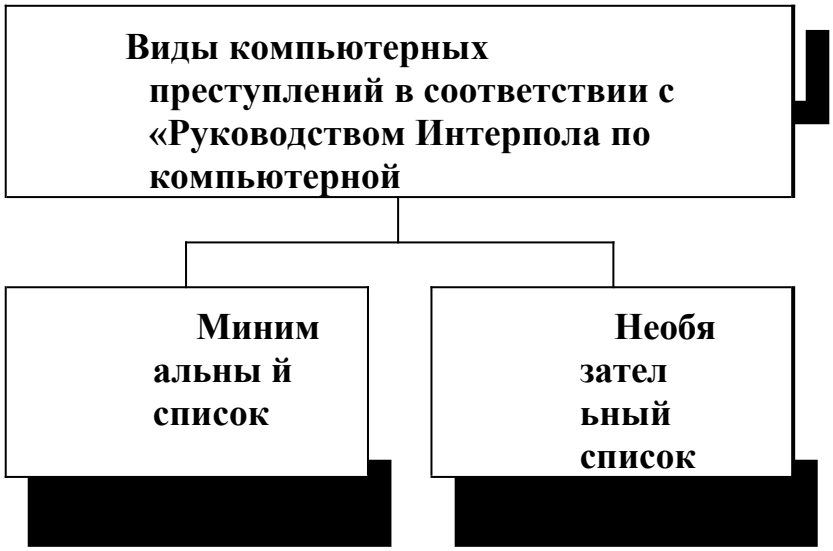


Рис. 6. Классификация компьютерных преступлений в соответствии с «Руководством Интерпола по компьютерной преступности» доступен НЦБ более чем 100 стран. Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

В соответствии с названным кодификатором, все компьютерные преступления классифицированы следующим образом:

QA Несанкционированный доступ и перехват:

QAH – компьютерный абордаж (несанкционированный доступ); QAI – перехват с помощью специальных технических средств; QAT – кража времени (уклонение от платы за пользование АИС); QAZ – прочие виды несанкционированного доступа и перехвата.

QD – Изменение компьютерных данных:

QDL – логическая бомба; QDT – троянский конь;

QDV – компьютерный вирус; QDW – компьютерный червь;

QDZ – прочие виды изменения данных

QF – Компьютерное мошенничество: QFC – мошенничество с банкоматами; QFF – компьютерная подделка;

QFG – мошенничество с игровыми автоматами; QFM – манипуляции с программами ввода-вывода; QFP – мошенничества с платежными средствами; QFT – телефонное мошенничество;

QFZ – прочие компьютерные мошенничества.

QR – Незаконное копирование:

QRG – компьютерные игры;

QRS – прочее программное обеспечение;

QRT – топология полупроводниковых устройств; QRZ – прочее незаконное копирование.

QS – Компьютерный саботаж:

QSH – с аппаратным обеспечением (нарушение работы ЭВМ);

QSS – с программным обеспечением (уничтожение, блокирование информации);

QSZ – прочие виды саботажа.

QZ – Прочие компьютерные преступления:

QZB – с использованием компьютерных досок объявлений;

QZE – хищение информации, составляющей коммерческую тайну; QZS – передача информации, подлежащей судебному рассмотрению; QZZ – прочие компьютерные преступления.

Кратко охарактеризуем некоторые виды компьютерных преступлений, согласно приведенному кодификатору.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:

QAH – «Компьютерный абордаж» (хаКинг – hacking): доступ в компьютер или сеть без права на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

QAI – перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

- *«Жучок»* (bugging) – характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
- *«Откачивание данных»* (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности, о технологии ее прохождения в системе;
- *«Уборка мусора»* (scavening) – характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности – физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных

в памяти машины;

❑ метод следования «з*а дураком»* (piggbackiiig), характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись

законного пользователя, можно пройти в дверь помещения вместе с ним;

❑ метод «з*а хвост»* (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;

❑ метод *«неспешного выбора»* (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

❑ метод «*Поиск бреши»* (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

❑ метод «*Люк»* (trapdoor), являющийся развитием предыдущего. В найденной «бреши» программа «разрывается», и туда вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу;

❑ метод «*Маскарад»* (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

❑ метод «*Мистификация»* (spoofing), который используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например, коды пользователя.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:

QDL/QDT – логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь – заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV – вирус (virus): изменение компьютерных данных или программ, без права на то, путем внедрения или распространения компьютерного вируса.

Компьютерный вирус – это специально написанная программа, которая может «приписать» себя к другим программам (т.е. «заражать» их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

QDW – червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:

QFC – компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.). **QFG** – мошенничества и хищения, связанные с игровыми автоматами.

QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них

путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

QFP – компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

QFT – телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлении:

QRG/QRS – незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

QRT – незаконное копирование топографии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

Компьютерный саботаж (QS) составляют следующие виды преступлений:

QSH – саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

QSS – компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие:

QZB – использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

QZE – хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну, без права на то, или другого законного обоснования с намерением причинить экономический ущерб или получить незаконные экономические преимущества;

QZS – использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия.

- ❑ *«Временная бомба»* – разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;
- ❑ *«Асинхронная атака»* (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей;
- ❑ *«Моделирование»* (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется «оптимизация» способа совершения преступления.

Данная классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола. Одним из ее достоинств является введение литеры «Z», отражающей прочие виды преступлений и позволяющей совершенствовать и дополнять используемую классификацию.

Однако полагаем необходимым согласиться с мнением Пущина В.С., что приведенная выше система классификации компьютерных преступлений, впрочем, как и ряд других, например, рассмотренные ранее «минимальный» и

«необязательный» списки нарушений «Руководства Интерпола по компьютерной преступности», страдают одним общим недостатком: в них происходит смешение уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что приводит к неоднозначности толкования и еще большей неопределенности понятия

«компьютерное преступление».

В этой связи значительный интерес представляет классификация компьютерных преступлений, предложенная В.А. Мещеряковым .

Неправомерное завладение информацией или нарушение исключительного права ее использования.

Неправомерное завладение информацией как совокупностью сведений, документов (нарушение исключительного права владения).

Неправомерное завладение информацией как товаром.

Неправомерное завладение информацией как идеей (алгоритмом, методом решения задачи).

`

1 Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации // Защита информации. Конфидент. – 1999. – № 4-5.

Неправомерная модификация информации.

Неправомерная модификация информации как товара с целью воспользоваться ее полезными свойствами (снятие защиты).

Неправомерная модификация информации как идеи, алгоритма и выдача за свою (подправка алгоритма).

Неправомерная модификация информации как совокупности фактов, сведений.

Разрушение информации.

Разрушение информации как товара.

Уничтожение информации.

Действие или бездействие по созданию (генерации) информации с заданными свойствами.

Распространение по телекоммуникационным каналам информационно-вычислительных сетей информации, наносящей ущерб государству, обществу и личности.

Разработка и распространение компьютерных вирусов и прочих вредоносных программ для ЭВМ.

Преступная халатность при разработке (эксплуатации) программного обеспечения, алгоритма в нарушение установленных технических норм и правил.

Действия, направленные на создание препятствий пользования информацией законным пользователям.

1.1. Неправомерное использование ресурсов автоматизированных систем (памяти, машинного времени и т. п.).

1.2. Информационное «подавление» узлов телекоммуникационных систем (создание потока ложных вызовов).

Следует отметить, что в связи с той общественной опасностью, которую представляют собой компьютерные преступления, в Уголовном кодексе Российской Федерации предусмотрена целая глава – глава 28, посвященная преступлениям в сфере компьютерной информации. Анализ содержащихся в данной главе статей (их всего три) позволяет выделить соответственно три вида компьютерных преступлений:

Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» предусматривает уголовную ответственность за *неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.*

Вообще под охраной понимается защита от любого а) не предусмотренного законом и б) совершенного не в соответствии с волей собственника информации вторжения, могущего быть осуществленным в любой форме. Указанное вторжение и представляет собой **неправомерный доступ** к информации.

Однако здесь важно иметь в виду, что уголовная ответственность наступает за неправомерный не к любой, а только к ***охраняемой законом*** компьютерной информации, т.е. информации ограниченного доступа.

В соответствии со статьей 10 Федерального закона «Об информации, информатизации и защите информации», вся информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к ***государственной тайне,*** и ***конфиденциальную*** (ч. 2 ст. 10 Закона), причем под последней, в соответствии со ст. 2 закона, понимается

«документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации».

Указом Президента РФ № 188 от 06.03.97 «Об утверждении перечня

сведений конфиденциального характера»
отнесены (рис. 7.):

к конфиденциальной информации

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность **(персональные данные)**, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

сведения, составляющие **тайну следствия и судопроизводства**;

служебные сведения, доступ к которым ограничен органами государственной власти, в соответствии с Гражданским кодексом Российской Федерации и федеральными законами **(служебная тайна)**;

сведения, связанные с профессиональной деятельностью, доступ к которым ограничен, в соответствии с Конституцией Российской Федерации и федеральными законами **(профессиональная тайна)**;

сведения, связанные с коммерческой деятельностью, доступ к которым ограничен, в соответствии с Гражданским кодексом Российской Федерации и федеральными законами **(коммерческая тайна)**;

сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них. Более подробно содержание каждого из перечисленных видов конфиденциальной информации

рассматривается в монографии «Защита информации. Часть 2: Организационно-

1

правовые методы и средства» . Здесь только отметим, что в настоящее время в

научной среде не выработано единой классификации видов конфиденциальной информации, хотя действующими нормативными актами установлено свыше 30 ее разновидностей. Отсутствие четкой классификации видов конфиденциальной информации, неоформленность их правовых режимов в законодательстве неизбежно приводит к значительному числу противоречий и пробелов, проблем в правоприменительной практике.

`

1

См.: Российская газета. – 1997. – 14 марта.

Объективную сторону данного вида компьютерных преступлений составляет неправомерный доступ к охраняемой законом компьютерной информации, если это

деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под *доступом* к компьютерной информации подразумевается всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, модифицировать, блокировать, копировать).

Под *уничтожением* понимается такой вид воздействия на компьютерную информацию, при котором навсегда теряется возможность ее дальнейшего использования кем бы то ни было. Как известно, в широко распространенных ныне операционных системах MS-DOS и MS WINDOWS при удалении файла происходит лишь замена первого символа его имени в таблице размещения файлов, при этом само содержимое файла сохраняется на диске до тех пор, пока поверх него не будет записана новая информация, та же ситуация может складываться при удалении отдельных записей из файла базы данных. Для окончания преступления в уголовно-правовом смысле достаточно выполнения команд, специально предназначенных для удаления структурного элемента информации (файла, записи), например, команд DOS «delete» или «format», независимо от возможности последующего восстановления информации с помощью специальных средств.
`

1 См.: Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 2:

Организационно-правовые методы и средства: Монография/Под ред. д-ра юрид. наук, проф. В.М. Мешкова. – Калининград: Калининградский ЮИ МВД России, 2003.

Таким образом, наступление преступных последствий будет налицо с того момента, когда файл или его часть станут «невидимыми» для средств программного обеспечения, используемого законным пользователем, и недоступными для их стандартных команд.

Модификация компьютерной информации – это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных.

Адаптация программы для ЭВМ или базы данных – «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя» (ч. 1 ст. 1 Закона РФ от 23 сентября 1992 г. № 3523-1

«О правовой охране программ для электронных вычислительных машин и баз данных»).

Блокирование компьютерной информации – это создание условий, при которых невозможно или существенно затруднено использование информации при

сохранности такой информации. Понятие «блокирование информации» во многом совпадает с понятием «модификация информации» и отличается лишь тем, что модификации подвергается не смысловая, а управляющая информация. Например, для блокирования доступа легального пользователя к базам данных необходимо произвести изменения в системных файлах администратора сети, сама охраняемая база данных при этом не подвергается модификации.

Следует отметить, что понятия «модификация», «уничтожение», «блокирование» тесно связаны между собой, т.к. на физическом уровне представления информации технически возможно выполнение всего лишь трех действий – чтения, записи (в т.ч. и «нулевых» значений) и разрушения самого носителя. Независимо от конкретного наименования указанные последствия считаются наступившими, если в результате операций чтения/ записи на охраняемую законом информацию оказано какое-либо воздействие. Различать эти три последствия необходимо по результату подобного воздействия. В связи с высокой скрытностью процессов, протекающих в ЭВМ и их сетях, а также необходимостью специальных познаний факты копирования, модификации, блокирования, уничтожения информации должны устанавливаться специальной компьютерно-технической экспертизой [1].

`

[1] См. об этом также: Пущин В.С. Преступления в сфере компьютерной информации. – М., 2000.

Копирование компьютерной информации – это повторение и устойчивое запечатление ее на машинном или ином носителе. Копирование компьютерной информации может быть осуществлено путем записи содержащегося во внутренней памяти ЭВМ файла на дискету, его распечатки и т.д. Копирование компьютерной информации от руки, путем фотографирования текста с экрана дисплея, а также считывание информации путем перехвата излучений ЭВМ, расшифровки шумов принтера и проч. не образует состава преступления в рамках данной статьи УК.

Нарушение работы ЭВМ, системы ЭВМ или их сети – это временное или устойчивое создание помех для их функционирования, в соответствии с назначением. Подобные нарушения могут выразиться в их произвольном

отключении, в отказе выдать информацию, в выдаче искаженной информации и т.п. при сохранении целостности ЭВМ и их систем. Нарушение работы ЭВМ может быть следствием поражения управляющей компьютерной информации, выхода из строя программного обеспечения при активизации недокументированных команд, захвата вычислительных ресурсов ЭВМ и мощностей каналов связи.

При этом речь идет не только о затруднениях, непосредственно связанных с манипуляциями в памяти ЭВМ, но и о помехах, проявляющихся на экране дисплея, при распечатывании и копировании компьютерной информации, а также на всякого рода периферийных устройствах и управляющих датчиках оборудования.

Статья 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» предусматривает уголовную ответственность за *создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, о равно использование либо распространение таких программ или машинных носителей с такими программами.*

Вредоносность или полезность соответствующих программ для ЭВМ

определяется не в зависимости от их назначения, а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной. По данным «Лаборатории Касперского» – одного из крупнейших отечественных производителей

антивирусного программного обеспечения, «горячая десятка» самых вредоносных

1

программ в 2002 году выглядела следующим образом .

№	Название	%2	Индекс распространенности
1	I-Worm.Klez	61,22	10,0
2	I-Worm.Lentin	20,52	3,4
3	I-Worm.Tanatos	2,09	0,3
4	I-Worm.BadtransII	1,31	0,2
5	Macro.Word97.Thus	1,19	0,2
6	I-Worm.Hybris	0,60	0,1

7	I-Worm.Bridex	0,32	0,1
8	I-Worm.Magistr	0,30	0,1
9	Win95.CIH	0,27	0,1
10	I-Worm.Sircam	0,24	0,1

Как можно заметить, несомненным лидером по количеству вызванных инцидентов в 2002 году является Интернет-червь Klez. Данная вредоносная программа была впервые обнаружена 26.10.01 и с тех пор не выходила из списка наиболее распространенных угроз. Необходимо отметить, что в истории компьютерной вирусологии еще ни разу не случалось, чтобы вредоносная программа смогла так долго продержаться на высших позициях «десятки». В общей сложности каждые 6 из 10 зарегистрированных случаев заражения были вызваны Klez.

В связи с той опасностью, которую представляют собой вредоносные программы, рассмотрим их наиболее широко распространенные виды.

Программы получения паролей – это две большие группы программ, которые предназначены для получения идентификаторов и паролей

пользователей. Подразделяются на две группы: а) программы открытия паролей;

б) программы захвата паролей.

`

Самые распространенные вредоносные программ//Защита информации.

Конфидент. – 2003. – № 1 (49). – С.5.

Доля от общего количества зарегистрированных инцидентов.

Программы открытия паролей последовательно генерируют все возможные варианты пароля и выдают их системе до тех пор, пока не будет определен необходимый пароль.

Программы захвата паролей специально предназначены для их кражи. Они выводят на экран терминала последовательно пустой экран, экран, появляющийся после крушения системы или сигнализирующий об окончании сеанса работы. При попытке входа имитируется ввод имени и пароля, которые пересылаются владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже становятся известны владельцу программы-захватчика. Перехват пароля может осуществляться и другим способом: с помощью воздействия на программу, управляющую входом пользователей в систему и ее наборы данных.

«Люки» или «back door» – не описанные в документации возможности работы с программным продуктом. Сущность использования люков состоит в том, что при реализации пользователем не описанных в документации действий он получает доступ к ресурсам и данным, которые в обычных условиях для него закрыты (в частности, вход в привилегированный режим обслуживания).

Люки могут появиться в программном продукте следующими путями:

а) люки чаще всего являются результатом забывчивости разработчиков. В процессе разработки программы создаются временные механизмы, облегчающие ведение отладки за счет прямого доступа к продукту. Одним из примеров использования забытых люков является инцидент с вирусом Морриса. Одной из причин, обусловившей распространение этого вируса, являлась ошибка разработчика программы электронной почты, входящей в состав одной из версий ОС UNIX, приведшая к появлению малозаметного люка;

6) люки могут образоваться также в результате часто практикуемой технологии разработки программных продуктов «сверху – вниз». При этом программист приступает к написанию управляющей программы, заменяя

предполагаемые в будущем подпрограммы так называемыми «заглушками» – группами команд, имитирующими или обозначающими место присоединения будущих подпрограмм. В процессе работы эти заглушки заменяются реальными подпрограммами.

На момент замены последней заглушки реальной подпрограммой программа считается законченной. Но на практике подобная замена выполняется не всегда. Во-первых, из-за нарушения сроков разработки и сдачи в эксплуатацию и, во-вторых, из-за невостребованности данной подпрограммы. Таким образом, заглушка остается, представляя собой слабое место системы с точки зрения информационной безопасности;

в) программист пишет программу, которой можно управлять с помощью определенных команд или, например, путем ввода «Y» («Да») или «N» («Нет»). А что произойдет, если в ответ на запрос будет вводиться «А» или «В» и т. д.? Если программа написана правильно, то на экране должно появиться сообщение типа «Неправильный ввод» и повтор запроса. Однако может быть ситуация, когда программа не учитывает такое, предполагая, что пользователь будет действовать правильно. В таком случае реакция программы на неопределенный ввод может быть непредсказуемой. Такую ситуацию в программе можно специально создать для того, чтобы получить доступ к определенным ресурсам и данным.

Таким образом, люк может присутствовать в программном продукте вследствие умышленных или неумышленных действий со стороны программиста для обеспечения:

тестирования и отладки программного продукта;

окончательной сборки конечной программы;

скрытого средства доступа к программному продукту и данным. В первом случае люк – это неумышленная, но тем не менее потенциальная брешь в безопасности системы. Во втором – серьезная угроза безопасности системы. В третьем случае – первый шаг к атаке системы.

Логические бомбы (logic bomb) – программный код, который является безвредным до выполнения определенного условия, после которого реализуется

логический механизм. Логические бомбы, в которых срабатывание скрытого модуля определяется временем (текущий датой), называют *бомбами с часовым механизмом* (time bomb). Подобные программы, реализующие свой механизм после конкретного числа исполнений, при наличии или, наоборот, отсутствии определенного файла, а также соответствующей записи в файле, и получили название *логической бомбы* (logic bomb). Основной целью функционирования программ данного типа следует считать нарушение нормальной работы компьютерной системы.

«Троянский конь» – программа, которая, кроме своей основной деятельности, выполняет некоторые дополнительные (разрушительные), не описанные в документации функции, о чем пользователь не подозревает.

Реализация дополнительных функций выполняется скрытым от пользователя модулем, который может встраиваться в системное и прикладное программное обеспечение. При реализации пораженной программы троянский конь получает доступ к ресурсам вместе с пользователем.

Троянские кони чаще всего встраиваются в хорошо зарекомендовавшие себя программные продукты – инструментальные средства, пакеты прикладных программ, текстовые редакторы, компьютерные игры и т. д. – и выступают в качестве средства несанкционированного доступа к содержащейся в системе информации. Компьютерные системы, использующие дескрипторные (т.е. описательные) методы управления доступом (и том числе такие, как полномочия, списки управления доступом и др.), являются практически беззащитными против программ типа троянский конь.

Репликаторы – это программы, которые могут создавать одну или более своих копий в компьютерной системе. Это приводит к быстрому переполнению памяти компьютера, но данные действия могут быть обнаружены опытным пользователем и достаточно легко устранены. Устранение программы репликатора усложняется в тех случаях, когда репликация выполняется с модификацией исходного текста программы, что затрудняет распознавание ее новых копий. Репликаторные программы становятся особенно опасными, когда к

функции размножения будут добавлены другие разрушающие воздействие.

Программные закладки – программы, которые сохраняют вводимую с клавиатуры информацию (в том числе и пароли) в некоторой зарезервированной для этого области.

Данный тип программных злоупотреблений включает:

закладки, ассоциируемые с программно-аппаратной средой (BIOS);

закладки, ассоциируемые с программами первичной загрузки, находящимися в Master Boot Record или Root секторов активных разделов;

закладки, ассоциируемые с загрузкой драйверов операционной системы, командного интерпретатора, сетевых драйверов;

закладки, ассоциируемые с прикладным программным обеспечением общего назначения (встроенные в клавиатурные или экранные драйверы, программы тестирования, утилиты и оболочки типа Norton Commander);

исполняемые модули, содержащие только код закладки (как правило, внедряемые в пакетные файлы типа BAT);

модули-имитаторы, совпадающие по внешнему виду с программами, требующими ввода конфиденциальной информации;

закладки, маскируемые под программные средства оптимизационного назначения (архиваторы, ускорители и т.д.);

закладки, маскируемые под программные средства игрового и развлекательного назначения.

Компьютерные вирусы. *Компьютерным вирусом называют программу, способную создавать способные к дальнейшему распространению копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия* (ГОСТ Р 51188-98. Защита информации. Испытание программных средств на наличие компьютерных вирусов).

Преступления, связанные с распространением компьютерных вирусов получили довольно широкое распространение в России, особенно с ростом числа российских пользователей Internet, значительная часть которых уже испытала на

себе действия подобных программ. Достаточно сказать, что на момент написания этой работы популярный антивирусный пакет «Norton AntiVirus» был способен распознать уже свыше 65 тыс. разновидностей вредоносных программ. Еженедельно этот список пополняется в среднем на 50-100 наименований.

По степени возможного причинения вреда компьютерные вирусы варьируются от «почти безобидных», изредка дающих знать о себе какимилибо сообщениями с непристойным содержанием, до опасных, способных привести к полной потере информации на носителе и даже к выводу из строя аппаратной части ЭВМ.

В тех случаях, когда в результате действия «вирусов» происходят существенные разрушения файловой системы, уничтожение информации и т.п.,

«вирус» является опасным, если же в результате его действия на экране монитора, например, появляются только какие-либо надписи или брань, то «вирус» считается безопасным.

В общем случае компьютерные вирусы подразделяются на классы по следующим признакам [1].

По среде обитания:

сетевые, распространяющиеся по компьютерной сети;

файловые, внедряющиеся в выполняемый файл;

загрузочные, внедряющиеся в загрузочный сектор жесткого диска или дискеты.

`

[1] Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и устройства для защиты объектов и информации. Справочное пособие. – СПб.: Лань, 1996. – С.164.

По способу заражения:

резидентные, загружаемые в память персонального компьютера;

нерезидентные, не заражающие память персонального компьютера и остающиеся активными ограниченное время;

По возможностям:

безвредные, не влияющие на работу персонального компьютера;

неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими звуковыми и прочими эффектами;

опасные, которые могут привести к серьезным сбоям в работе персонального компьютера;

очень опасные, которые могут привести к потере программ, уничтожению данных, стереть информацию в системных областях памяти и даже преждевременному выходу из строя периферийных устройств.

И, наконец, **статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»** предусматривает уголовную ответственность за *нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.*

Правила эксплуатации ЭВМ определяются соответствующими техническими нормативными актами. Они также излагаются в паспортах качества, технических

описаниях и инструкциях по эксплуатации, передаваемых пользователю при приобретении вещественных средств компьютерной техники (ЭВМ и периферийных устройств), в инструкциях по использованию программ для ЭВМ. Соответствующие инструкции могут излагаться на бумажных и машинных носителях; в последнем случае они включаются в программу, которая обеспечивает к ним доступ при желании пользователя.

Таким образом, нарушения правил эксплуатации ЭВМ могут быть подразделены на *физические* (неправильная установка приборов, нарушение температурного режима в помещении, неправильное подключение ЭВМ к

источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных приборов и узлов) и *интеллектуальные* (неверное ведение диалога с компьютерной программой, ввод данных, обработка которых непосильна данным средствам вычислительной техники).

Таковы, в общем, основные черты компьютерных преступлений, ответственность за совершение которых предусмотрена действующим уголовным законодательством Российской Федерации.

Сопоставляя компьютерные преступления с другими составами правонарушений, предусмотренных уголовным кодексом, можно выделить их следующие ***отличительные особенности***:

высокая скрытность (латентность), сложность сбора улик по установленным фактам;

сложность доказательства в суде подобных дел;

«интернациональность» компьютерных преступлений. В настоящее время с развитием телекоммуникационных систем реальностью стала возможность совершения компьютерного преступления злоумышленником, находящимся за тысячи километров от места преступления. Достаточно вспомнить хотя бы рассмотренную нами ранее нашумевшую историю с Владимиром Левиным, который в 1994 г. сумел проникнуть в компьютерную систему Ситибанка. «Дело Левина» было отнесено по классификации международной уголовной полиции к категории «транснациональных сетевых компьютерных преступлений»;

высокий ущерб даже от единичного преступления;

вполне определенный контингент лиц, совершающих правонарушения в сфере компьютерной информации: это, как правило, высококвалифицированные программисты, специалисты в области телекоммуникационных систем, системные и банковские программисты.

В отношении последнего небезынтересным представляется проведенная в 1998 г. в Экспертно-криминалистическом центре МВД классификация

компьютерных преступников . Обобщенный портрет отечественного

преступника в сфере компьютерной информации, созданный на основе этого анализа, выглядит примерно так:

мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере либо почти не обладающий таким опытом;

в прошлом к уголовной ответственности не привлекался;

`

1 См.: Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ- Петербург, 2000. – С.6.

яркая мыслящая личность;

способен принимать ответственные решения;

хороший, добросовестный работник, по характеру нетерпимый к насмешкам и к потере своего социального статуса среди окружающих его людей;

любит уединенную работу;

приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуск и отгулы..

Вообще специалисты выделяют **четыре основные группы правонарушителей в кибернетическом пространстве**.

Первая группа – так называемые хакеры, т.е. пользователи информационных систем, занимающиеся поиском незаконных способов получения доступа к защищенным данным. Они представляют самую многочисленную группу, включающую обычно программистов, имеющих, как правило, фанатичное стремление преодолеть защиту какой-либо системы. В перспективе эта группа правонарушителей останется лидирующей по численности.

Вторая группа – это преступники, преследующие цели обогащения путем непосредственного внедрения в финансовые системы для получения коммерческой и другой информации для организации действий уголовного характера. Она формируется в основном из тех хакеров, которые пришли к выводу о возможности заработать на своем «хобби». Доля криминальных элементов среди пользователей информационных систем будет нарастать.

Третью группу составляют террористы и другие экстремистские группы, использующие внедрение в информационные системы для совершения устрашающих действий, шантажа и в других целях. В перспективе

«кибертерроризм» может стать реальностью.

К четвертой группе можно отнести различные коммерческие организации и структуры, стремящиеся вести промышленный шпионаж и борьбу с конкурентами путем добычи или искажения конфиденциальной финансовой,

технологической, проектной, рекламной и другой информации. Рыночные отношения стимулируют совершенствование методов скрытого проникновения в файлы данных конкурирующих фирм.

К числу ***обстоятельств, способствующих совершению компьютерных преступлений***, можно отнести следующие:

Рост числа ЭВМ, используемых в России, и, как следствие этого, рост числа их пользователей, увеличение объемов информации, хранимой и обрабатываемой ЭВМ. Этому обстоятельству способствует целый ряд фактор, в том числе:

широкое внедрение современных информационных технологий в различные сферы деятельности;

снижение цен на персональные компьютеры и периферийное оборудование;

структурное изменение компьютерного рынка России: все больше компьютеров не ввозится в готовом виде в страну, а собирается непосредственно в России.

Недостаточность мер по защите ЭВМ и их систем, недопонимание многими руководителями предприятий, организаций важности проблем обеспечения информационной безопасности, защиты информации. Примером этого может служить отмеченное ранее уголовное дело, возбужденное в августе 1991 г. СО Калининского РУВД г. Москвы по факту хищения сотрудниками Внешэкономбанка денежных средств в размере 125,5 тысяч долларов США путем умышленного внесения изменений в компьютерную программу.

Несовершенство используемого программного обеспечения с точки зрения обеспечения защиты информации, обрабатываемой с его помощью. Например, в операционной системе Windows 95 используются неэффективные алгоритмы шифрования сохраняемых паролей пользователей, что может привести к несанкционированному доступу к хранимой в компьютере информации со стороны посторонних лиц.

Несовершенство самих технических средств защиты информации. Не

всегда используемые технические средства защиты информации оказываются эффективными и позволяют достичь прогнозируемого уровня безопасности информации.

Широкий выход российских пользователей ЭВМ в мировые информационные сети для обмена информацией, заключения контрактов, осуществления платежей и т.п. Подобный обмен в настоящее время нередко производится без должного контроля со стороны государственных органов.

Использование в преступной деятельности современных технических средств, в том числе и ЭВМ. Во-первых, организованная преступность включена в

крупномасштабный бизнес, выходящий за рамки отдельных государств, где без компьютеров невозможно руководить и организовывать сферу незаконной деятельности. Во-вторых, из организаций, использующих ЭВМ, значительно удобнее «вытягивать» деньги с помощью такой же техники, дающей возможность повысить прибыль и сократить риск.

Ошибки и небрежность в работе пользователей ЭВМ. Последние не всегда серьезно относятся к обеспечению конфиденциальности информации и часто пренебрегают элементарными требованиями по ее защите: не уничтожают секретные файлы с компьютеров общего пользования; используют упрощенные пароли, устанавливаемые для защиты информации и т.д.

Имеет место также ряд упущений организационного характера, к которым можно отнести неконтролируемый доступ сотрудников и обслуживающего персонала к клавиатуре компьютера; низкий профессионализм или отсутствие служб информационной безопасности, отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности компьютерной информации и т.п.

Непродуманная кадровая политика в вопросах приема на работу и увольнения. Здесь показателен пример, имевший место в августе 1983 году на Волжском автомобильном заводе в г. Тольятти. Следственной бригадой прокуратуры РСФСР был изобличен программист, который из мести руководству предприятия умышленно внес изменения в программу для ЭВМ,

обеспечивающую подачу механических узлов на главный сборочный конвейер завода. В результате произошел сбой в работе главного конвейера, и заводу был причинен существенный материальный ущерб: 200 легковых автомобилей не сошло с конвейера, пока программисты не выявили и не устранили источник сбоев. При этом материальные потери составили 1 млн. руб. в ценах 1983 г.

Недостаточный уровень специальной подготовки должностных лиц правоохранительных органов, занятых раскрытием и расследованием компьютерных преступлений.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ.

Стремительный рост количества компьютерных преступлений, совершенных в России за последнее время, а также та общественная опасность, которую они собой представляют, настойчиво требуют принятия целого комплекса действенных мер по обузданию компьютерной преступности.

В настоящее время Межведомственной комиссией Совета Безопасности Российской Федерации по информационной безопасности, Федеральной службой безопасности России и Министерством внутренних дел России предпринимаются значительные усилия по развертыванию борьбы с преступлениями в сфере компьютерной информации. Можно выделит два основных направления борьбы:

Первое – выявление и пресечение компьютерных преступлений. Здесь необходимо отметить, что раскрытие компьютерных преступлений существенно затрудняется их специфичностью и тем, что их совершают люди, хорошо владеющие тонкостями информационных технологий.

Второе – профилактика и предупреждение компьютерных преступлений, которые предусматривают:

создание, сертификацию, лицензирование и внедрение необходимых средств технической и программной защиты информации;

создание специализированных организационных структур, задачей которых является обеспечение надежного функционирования средств защиты,

средств генерации ключей и паролей, их раздачи, контроля за использованием, смены и уничтожения;

подготовка квалифицированных кадров для правоохранительных органов, включая органы дознания и расследования, судов, служб безопасности компьютерных и телекоммуникационных систем и сетей.

Ключевую роль в этой системе мер играют мероприятия по защите информационных систем, в которых осуществляется обработка и хранение компьютерной информации, реализуемые собственниками этой информации или уполномоченными на то лицами.

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК СИСТЕМА ДЕЯТЕЛЬНОСТИ.

Под **защитой информации**, в соответствии с **ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»**, понимается ***деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию***. При этом под несанкционированными воздействиями понимается целенаправленная деятельность людей, направленная на изменение количественных и качественных характеристик информации и/или ее носителей (например, их изменение, уничтожение, утрата и т.п.). Непреднамеренное же воздействие проявляется в виде различного рода природных явлений или ошибок пользователей информационных систем.

Системный анализ любой проблемы начинается с анализа целей. Однако для того чтобы сформулировать основную цель защиты информации в информационных системах и осуществить ее дальнейшую конкретизацию, необходимо конкретизировать возможные угрозы безопасности хранимой, обрабатываемой и передаваемой в информационных системах информации[1].

Проявление этих угроз возможно как вследствие различных возмущающих воздействий, в результате которых происходит уничтожение (модификация)

информации или создаются каналы утечки информации, так и вследствие использования нарушителем каналов утечки информации. В обобщенном виде угрозы безопасности компьютерной информации можно представить так, как это показано на рис. 7.

`

1

Безопасность информации (данных) – состояние защищенности

информации (данных), обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз (ОСТ 45.127-99

«Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения»).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (ГОСТ Р.51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»).


Месть
Денежная выгода
Хулиганство
Терроризм

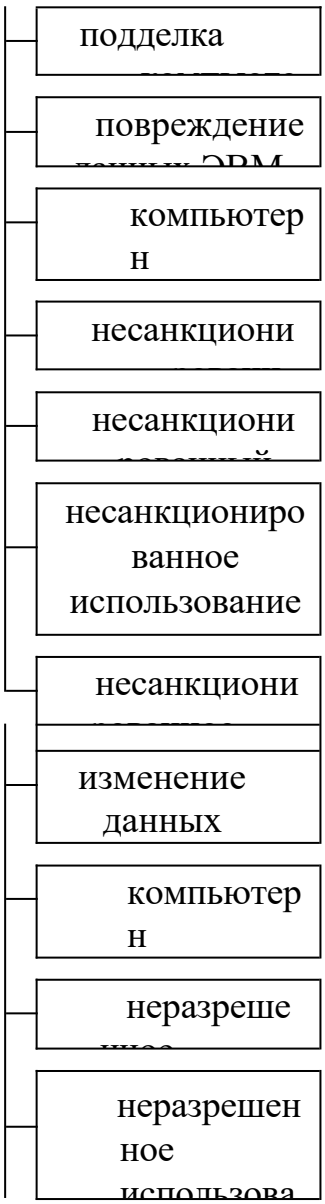


Рис. 7. Классификация угроз безопасности компьютерной информации

Как известно, несанкционированное получение информации реализуется путем доступа злоумышленника или его технических средств к источнику информации. Причем доступ может быть как непосредственный (физический), так и дистанционный. В первом случае речь идет о действиях, предпринимаемых злоумышленником для непосредственного ознакомления с интересующей его информацией. Он может быть реализован, например, путем хищения или несанкционированного

копирования информации и обуславливаться недостатками технических и программных средств защиты, ОС, СУБД, математического и программного обеспечения, а также просчетами в организации технологического процесса работы с информацией. Поскольку такой доступ

является наиболее опасным для злоумышленника (слишком велик риск обнаружения), на практике чаще применяется дистанционный доступ к источнику информации, при котором ее добывание производится в рамках каналов утечки информации.

Каналом утечки информации называют физический путь

несанкционированного переноса информации от источника к

1

злоумышленнику

. Если перенос осуществляется с помощью технических средств, то канал называют ***техническим***.

Каналы утечки возникают, например, вследствие недостаточной изоляции помещений, просчетов в организации работы с информацией и предоставляют нарушителю возможность применения специальных технических средств негласного получения информации, дистанционного фотографирования, перехвата электромагнитных излучений, хищения носителей информации и производственных отходов (дискет, листингов машинных программ и т.п.).

Воздействия, в результате которых может быть нарушена безопасность компьютерной информации, включают в себя:

1. *Внешние возмущающие факторы:*

– случайные воздействия природной среды (ураган, землетрясение, пожар, наводнение и т.п.);

– целенаправленные воздействия нарушителя (шпионаж, разрушение компонентов информационной системы и т.п.);

– техногенные (отказ систем энергообеспечения, общих систем связи и т.п.);

2. *Внутренние возмущающие факторы* (отказы аппаратуры, ошибки в математическом и программном обеспечении, недостаточная профессиональная и морально-психологическая подготовка персонала и т.д.).

`

1 Торокин А.А. К вопросу о понятийном аппарате защиты информации техническими средствами//Безопасность информационных технологий. – 1998. – № 4. – С. 82; Ванчаков Н.Б., Григорьев А.Н. Защита информации. Часть 1: Технические методы и средства. Монография. Изд. 2-е доп. и перераб. / Под ред. д-ра юрид. наук, проф. В.М. Мешкова. – Калининград: Калининградский ЮИ МВД России, 2003. – С.17.

Анализ возможных угроз безопасности компьютерной информации, опыт разработки и эксплуатации различных средств и механизмов защиты информации в информационных вычислительных системах позволяют сформулировать следующие *принципы организации системы защиты компьютерной информации, хранимой, обрабатываемой и передаваемой в информационных вычислительных системах*:

❑ ***принцип системности*** означает, что обеспечение защиты информации представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла информационной вычислительной системы при комплексном использовании всех средств и механизмов защиты данных для предотвращения или компенсации последствий возможных НСД;

❑ ***принцип специализированности*** включает три аспекта:

– надежные механизмы защиты информации могут быть разработаны лишь профессиональными специалистами;

– осуществление непрерывного процесса обеспечения необходимого уровня защиты информации возможно лишь на базе средств и механизмов защиты промышленного производства;

– обеспечивать эффективное функционирование системы защиты компьютерной информации должны специалисты в области защиты информации.

❑ ***принцип неформальности*** означает, что методология проектирования системы защиты информации и отдельных механизмов защиты в своей основе является неформальной.

В то же время на основании изложенного можно сформулировать следующие *основные требования к системе защиты информации, циркулирующей в информационных вычислительных системах*:

1. ***адекватность.*** Система защиты информации должна надежно обеспечить безопасность информации в информационных вычислительных системах;

2. ***экономичность.*** Создание и эксплуатация системы защиты информации

должны осуществляться с минимальным расходом материальных и сетевых ресурсов;

3. ***удобство для пользователей (психологическая приемлемость)***. Механизмы защиты данных не должны создавать дополнительные трудности законным пользователям системы;

4. ***открытость проектирования.*** Механизмы защиты информации должны эффективно функционировать даже в том случае, когда их структуры и алгоритмы работы известны нарушителю;

5. ***минимизация привилегий.*** Каждому пользователю предоставляются только действительно необходимые ему права по доступу к ресурсам (данным) системы;

6. ***полное посредничество (полнота контроля)*** должно осуществляться при каждом обращении к каждому защищаемому ресурсу (данным);

7. ***распределение полномочий.*** Каждая важная операция должна разрешаться при наличии, как минимум, двух условий;

8. ***минимум общего механизма.*** Использование многими пользователями одного механизма защиты может привести к раскрытию механизма;

9. ***наказуемость нарушений.*** В системе защиты информации должны быть предусмотрены «наказания» за нарушения (например, блокировка терминала при вводе пароля больше разрешенного числа раз).

В практическом плане можно выделить четыре основных направлений работ по защите компьютерной информации:

- теоретические исследования;
- детализация действующей нормативно-правовой базы в области защиты информации и совершенствование ее в этом направлении;
- совершенствование форм деятельности и подготовки представителей органов охраны правопорядка, в том числе создание специальных подразделений для выполнения этой работы;
- усиление мер безопасности против возможных злоупотреблений ЭВМ и поиска все более совершенных средств защиты компьютерной техники и информационных сетей.

По своему содержанию эти направления деятельности условно можно подразделить на следующие ***основные меры защиты компьютерной информации:***

- ***правовые;***
- ***организационно-административные;***
- ***инженерно-технические.***

Практическая деятельность показывает, что положительный результат можно получить только при использовании всех этих мер.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Правовое обеспечение безопасности информации *– это совокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых обязательны в системе защиты информации* . Вопрос о правовом обеспечении безопасности информации в настоящее время активно прорабатывается как в практическом, так и в законотворческом плане.

Правовое обеспечение безопасности информации любой страны содержит как международные, так и национальные правовые нормы. В нашей стране правовые или законодательные основы обеспечения безопасности компьютерной информации составляют Конституция РФ, Законы РФ, Кодексы, указы и другие нормативные акты, регулирующие отношения в области информации.

Из общего количества документов в нормативно-правовой базе Российского законодательства выделяют четыре направления защиты информации:

1. защита информации производится в тех случаях, когда наличие информации создает условия для удовлетворения потребностей личности. Уничтожение, хищение или искажение информации мешает возможности удовлетворения потребности в информации (например, ст. 273, 274 УК РФ);
2. защита от информации производится в тех случаях, когда распространение информации причиняет определенный вред гражданам и организациям;

3. защита среды распространения информации (каналов связи) – защита условий для использования информации или возможности обмена информацией;

4. защита технических средств, обеспечивающих обработку информации,

когда вред наносится имуществу и косвенным путем процессу информатизации .

В системе законодательных и нормативно-правовых актов,

регламентирующих вопросы обеспечения защиты компьютерной информации, особое место занимает **Федеральный закон РФ от 20.02.1995 г. № 24-ФЗ**

«Об информации, информатизации и защите информации» Федерального закона от 10.01.2003 г. № 15-ФЗ).

(в ред.

`

См.: Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма.

Справочное пособие. – СПб.: БХВ-Петербург; Арлит 2002, – С.176.

См.: Лисица О.В. Защита и политика безопасности информационных

систем. Общая часть: Учебное пособие/Под ред. д.ю.н., профессора В.Л. Попова и к.ю.н. В.Н. Лопатина. – Калининград: КЮИ МВД России, 1999. – С.20.

Российская газета. – 1995. – 22 февр.

Данный закон без преувеличения сыграл значительную роль в формировании современного информационного законодательства России. Принятие данного закона позволило разрешить целый ряд проблем в области правового регулирования информационных отношений, в том числе:

- закрепил права граждан, организаций и государства на информацию;
- установил правовой режим информации, правила формирования информационных ресурсов и пользования ими;
- права и обязанности граждан, организаций и государства в процессе создания информационных систем страны, создания и развития научно- технической, производственной базы информации, формирования рынка информационной продукции и услуг в этой сфере;
- установил правила и общие требования ответственности в области

защиты информации в системах ее обработки, гарантии субъектов в процессе реализации права на информацию, гарантии безопасности в области информатизации;

- предопределил порядок включения страны в международные информационные системы.

Основная цель закона состоит в создании правовой основы отношений в области формирования и использования информационных ресурсов, в области информатизации с учетом возрастающей роли информации в обновлении производственного, научного, организационного и управленческого потенциалов страны. Сфера действия данного закона охватывает отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

В законе прямо отмечается, что одной из приоритетных целей государственной политики в сфере информатизации является обеспечение как

национальной безопасности, так и реализации прав граждан, а также развитие законодательства в сфере защиты информации.

В соответствии со ст. 21 рассматриваемого закона, защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, – уполномоченными органами на основании Закона Российской Федерации

«О государственной тайне»;

– в отношении конфиденциальной документированной информации

– собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

– в отношении персональных данных – федеральным законом. Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно – технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти в порядке, определяемом Правительством Российской Федерации.

В качестве целей защиты закон определяет (ст. 20):

– предотвращение утечки, хищения, утраты, искажения, подделки информации;

– предотвращение угроз безопасности личности, общества, государства;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных

системах;

– сохранение государственной тайны, конфиденциальности документированной информации, в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Весьма важное значение для целей обеспечения безопасности компьютерной информации представляются положения **Закона Российской Федерации от 9 июля 1993 г. № 5351-1 «Об авторском праве и смежных правах»** (в ред. Федерального закона от 19.07.95 г. № 110-ФЗ). Предметом регулирования данного закона являются отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права).

Согласно ст. 6 Закона, авторское право распространяется как на обнародованные, так и на необнародованные произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения, и существующие в какой-либо объективной форме:

- письменной (рукопись, машинопись, нотная запись и так далее);
- устной (публичное произнесение, публичное исполнение и так далее);
- звукоили видеозаписи (механической, магнитной, цифровой, оптической и так далее);
- изображения (рисунок, эскиз, картина, план, чертеж, кино-, теле-, видеоили фотокадр и так далее);
- объемно-пространственной (скульптура, модель, макет, сооружение и так далее);
- в других формах.

При этом авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.

Объектами авторского права являются, наряду с перечисленными в ст.7 Закона, и программы для ЭВМ, отнесенные законодателем к категории литературных произведений.

Законом установлено, что за нарушение авторских и смежных прав наступает гражданская, уголовная и административная ответственность, в соответствии с законодательством Российской Федерации.

Источником регулирования правоотношений в области охраны авторских и смежных прав являются не только положения данного закона, но и нормы, содержащиеся в других законодательных актах Российской Федерации, прежде всего, – **Законе РФ от 23 сентября 1992 г. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»**, законодательных актах субъектов Российской Федерации, международных договорах, в которых участвует Россия.

Анализ соотношения Закона РФ «Об авторском праве и смежных правах» и Закона РФ «О правовой охране программ для электронных вычислительных машин и баз данных» позволяет сделать вывод о том, что первый из них выполняет роль общего закона по отношению ко второму как закону специальному.

Говоря о правовом обеспечении информационной безопасности в России, нельзя не упомянуть и **Доктрину информационной безопасности Российской Федерации**. Доктрина представляет собой документ, который содержит совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации и служит основой для:

- формирования государственной политики в области обеспечения

информационной безопасности Российской Федерации;

– подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

– разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Особая значимость этого документа заключается в том, что в нем на основе развернутого анализа современного состояния безопасности личности, общества и государства определены цели, задачи и ключевые проблемы обеспечения информационной безопасности. В Доктрине выделяется четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий,

технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории России.

Крайне важным с методологической точки зрения представляется выделение в Доктрине угроз информационной безопасности Российской Федерации. По своей общей направленности эти угрозы подразделены на следующие виды:

- ❑ угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- ❑ угрозы информационному обеспечению государственной

политики Российской Федерации;

- ❑ угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- ❑ угрозы безопасности информационных и телекоммуникационных средств и систем как уже развернутых, так и создаваемых на территории России.

Источники отмеченных выше угроз по своей направленности подразделены Доктриной на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов

Российской Федерации в информационной сфере;

- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

– критическое состояние отечественных отраслей промышленности;

– неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

– недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

– недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

– неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

– недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

– недостаточная экономическая мощь государства;

– снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

– недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

– отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно- финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Помимо отмеченного, в Доктрине определяются общие и специальные методы обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни, основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации, а также организационная основа обеспечения информационной безопасности России.

Доктрина информационной безопасности Российской Федерации недвусмысленным образом указывает, что информационная безопасность является составной частью системы национальной безопасности и относится к

жизненно важным сферам обеспечения интересов личности, общества и государства. В этой связи вполне закономерным представляется установленное действующим законодательством требование

лицензирования различных видов деятельности в области обеспечения информационной безопасности и защиты информации.

В соответствии со ст. 17 **Федерального закона Российской Федерации от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»**, лицензированию в том числе подлежат следующие виды деятельности:

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

- деятельность по технической защите конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи

специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Порядок осуществления лицензирования вышеуказанных видов деятельности определяется соответствующими Положениями, утверждаемыми Постановлениями Правительства Российской Федерации.

Так, **Постановлением Правительства Российской Федерации от 30 апреля 2002 г. № 290** утверждено **Положение о о лицензировании деятельности по технической защите конфиденциальной информации**. Данное Положение определяет порядок лицензирования деятельности юридических лиц и индивидуальных предпринимателей по технической защите конфиденциальной информации, под которой (защитой) понимается *комплекс мероприятий и (или) услуг по защите конфиденциальной информации от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней*.

Лицензирующим органом Положением определена Государственная техническая комиссия при Президенте Российской Федерации.

Положение определяет следующие лицензионные требования и условия при осуществлении деятельности по технической защите конфиденциальной информации:

- осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности

«компьютерная безопасность», «комплексное обеспечение информационной безопасности автоматизированных систем» или «информационная безопасность телекоммуникационных систем», либо специалистами, прошедшими переподготовку по вопросам защиты информации;

– соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации и нормативно-методическими документами по технической защите информации;

– использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

– использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

Для получения лицензии соискатель лицензии должен представить в лицензирующий орган следующие документы:

а) заявление о выдаче лицензии с указанием лицензируемой деятельности; наименования, организационно-правовой формы и места нахождения – для

юридического лица;

фамилии, имени, отчества, места жительства, данных документа, удостоверяющего личность, – для индивидуального предпринимателя;

б) копии учредительных документов и документа, подтверждающего внесение записи о юридическом лице в Единый государственный реестр юридических лиц;

в) копия свидетельства о государственной регистрации соискателя лицензии – для индивидуального предпринимателя;

г) копия свидетельства о постановке соискателя лицензии на учет в налоговом органе с указанием идентификационного номера налогоплательщика;

д) документ, подтверждающий уплату лицензионного сбора за рассмотрение заявления о выдаче лицензии;

е) сведения о квалификации специалистов по защите информации соискателя лицензии.

При этом лицензирующий орган имеет право провести проверку соответствия соискателя лицензии лицензионным требованиям и условиям, а также запросить у соискателя лицензии сведения, подтверждающие возможность соблюдения таких требований и условий.

Решение о выдаче или об отказе в выдаче лицензии принимается в срок, не превышающий шестидесяти дней с даты получения лицензирующим органом всех необходимых документов. В случае положительного решения соискателю выдается лицензия сроком на пять лет. При этом срок действия лицензии может быть продлен по заявлению лицензиата в порядке, предусмотренном для переоформления лицензии.

Вместе с тем, в соответствии с рассматриваемым Положением, лицензирующий орган наделен правом контроля за выполнением лицензиатом лицензионных требований и условий. Он может осуществлять как плановые, так и внеплановые проверки выполнения лицензиатом лицензионных требований и условий.

В области обеспечения безопасности компьютерной информации весьма существенное значение имеют и различные руководящие документы, стандарты в области информационной безопасности. Наиболее значимыми зарубежными стандартами информационной безопасности являются (в хронологическом порядке) «Критерии безопасности компьютерных систем министерства обороны США» («Оранжевая книга»), «Европейские критерии безопасности информационных технологий, «Федеральные критерии безопасности информационных технологий США», «Канадские критерии безопасности компьютерных систем» и «Единые критерии безопасности информационных технологий».

У нас разработкой руководящих документов в области защиты информации занимается Государственная техническая комиссия (далее – Гостехкомиссиия) при Президенте Российской Федерации, к компетенции которой относится:

- проведение единой государственной политики в области технической защиты информации;
- осуществление единой государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществление межотраслевой координации и функционального

регулирования деятельности по обеспечению технической защиты информации в аппаратах органов государственной власти субъектов Российской Федерации и органов государственной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

- прогнозирование развития сил, средств и возможностей

технических разведок, выявление угроз безопасности информации;

– противодействие добыванию информации техническими средствами разведки, предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования;

– контроль в пределах своих полномочий деятельности по технической защите информации в аппаратах федеральных органов государственной власти и органов исполнительной власти субъектов Российской Федерации, федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления, на предприятиях, в учреждениях и организациях;

– осуществление организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны центральным аппаратом Гостехкомиссии России.

К числу основных руководящих документов Гостехкомиссии России, регулирующих вопросы защиты компьютерной информации, относятся следующие:

1. ***Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.*** Данный документ предусматривает два относительно самостоятельных направления в области защиты информации: одно связано со средствами вычислительной техники, а другое – с автоматизированными системами. Отличие между ними обуславливается главным образом тем, что

средства вычислительной техники поставляются на рынок как элементы и, не решая прикладных задач, не содержат пользовательской информации (п. 1.4.). Помимо пользовательской информации, при создании автоматизированных систем появляются такие отсутствующие при

разработке средств вычислительной техники характеристики, как полномочия пользователей, модель нарушителя, технология обработки информации. В связи с этим, если понятия защищенность (защита) информации от несанкционированного доступа в автоматизированных системах и защищенность (защита) автоматизированных систем от несанкционированного доступа к информации эквивалентны, то в случае средств вычислительной техники можно говорить лишь об их защищенности (защите) от несанкционированного доступа к информации, для обработки, хранения и передачи которой эти средства предназначены.

2. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Этим положением устанавливается единый на территории Российской Федерации порядок исследований и разработок в области: – защиты информации, обрабатываемой автоматизированными системами различного уровня и назначения, от несанкционированного доступа;

– создания средств вычислительной техники общего и специального назначения, защищенных от утечки, искажения или уничтожения информации за счет несанкционированного доступа, в том числе программных и технических средств защиты информации от несанкционированного доступа;

– создания программных и технических средств защиты информации от несанкционированного доступа в составе систем защиты секретной информации в создаваемых АС.

3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели

защищенности от несанкционированного доступа к информации. Документ вводит семь классов защищенности. Самый низкий – седьмой, самый высокий – первый.

Требования к показателям защищенности предъявляются к общесистемным программным средствам и операционным системам. В зависимости от реализованных моделей защиты и надежности их проверки классы подразделяются на четыре группы.

Первая группа включает только один седьмой класс (минимальная защищенность).

Вторая группа характеризуется избирательной защитой и включает шестой и пятый классы. Избирательная защита предусматривает контроль доступа поименованных субъектов к поименованным объектам системы. При этом для каждой пары «субъект-объект» должны быть определены разрешенные типы доступа.

Третья группа характеризуется полномочной защитой и включает четвертый, третий и второй классы. Полномочная защита предусматривает присвоение каждому субъекту и объекту системы классификационных меток, указывающих их место в иерархии. Обязательное требование для входящих в эту группу классов – реализация диспетчера доступа (reference monitor). Контроль доступа должен осуществляться применительно ко всем объектам. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и избирательными, и полномочными правилами разграничения доступа.

Четвертый класс характеризуется верифицированной защитой и содержит только первый класс. Для присвоения класса защищенности система должна содержать руководство администратора по системе, руководство пользователя, тестовую и конструкторскую (проектную) документацию.

4. *Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.*

Настоящий документ определяет девять классов защищенности автоматизированных систем от несанкционированного доступа к информации.

Выбор класса производится заказчиком и разработчиком с привлечением

специалистов по защите информации. К числу определяющих признаков относятся:

- наличие в системе информации различного уровня конфиденциальности;
- уровень полномочий субъектов на доступ к конфиденциальной информации;
- режим обработки данных в системе – коллективный или индивидуальный.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в системе. В пределах каждой группы соблюдается иерархия требований к защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности автоматизированных систем.

Третья группа классифицирует системы, в которых работает один пользователь, допущенный ко всей информации системы, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А .

Вторая группа классифицирует системы, в которых пользователи имеют одинаковые права доступа ко всей информации, обрабатываемой и (или)

хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа классифицирует многопользовательские автоматизированные системы, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, и не все пользователи имеют к ней право доступа. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

5. ***Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.*** Этим документом устанавливается классификация межсетевых экранов по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

6. ***Защита информации. Специальные защитные знаки. Классификация и общие требования.*** Устанавливает классификацию по классам защиты специальных защитных знаков, предназначенных для контроля доступа к объектам защиты, а также для защиты документов от подделки.

Данным документом все специальные защитные знаки делятся на 18 классов. При этом классификация знаков осуществляется на основе оцен-ки их основных параметров: возможности подделки, идентифицируемости и стойкости защитных свойств.

7. ***Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.*** Настоящий Руководящий документ устанавливает классификацию программного обеспечения (как отечественного, так и

импортного производства) средств защиты информации, в том числе и встроенных в общесистемное и прикладное программное обеспечение, по уровню контроля отсутствия в нем недекларированных возможностей, т.е. таких функциональных возможностей программного обеспечения, не описанных или не соответствующих описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Уровень контроля определяется выполнением заданного настоящим документом набора требований, предъявляемого:

- к составу и содержанию документации, представляемой заявителем для проведения испытаний программного обеспечения средств защиты информации;
- к содержанию испытаний.

Классификация распространяется на программное обеспечение, предназначенное для защиты информации ограниченного доступа.

Устанавливается четыре уровня контроля отсутствия недекларированных возможностей, каждый из которых характеризуется определенной минимальной

совокупностью требований.

При этом для программного обеспечения, используемого при защите информации, *отнесенной к государственной тайне*, должен быть обеспечен уровень контроля не ниже *третьего*.

Самый высокий уровень контроля – *первый*, достаточен для программного обеспечения, используемого при защите информации с грифом «ОСОБОЙ ВАЖНОСТИ».

Второй уровень контроля достаточен для программного обеспечения, используемого при защите информации с грифом «СОВЕРШЕННО СЕКРЕТНО». *Третий уровень* контроля достаточен для программного обеспечения, используемого при защите информации с грифом «СЕКРЕТНО».

Самый низкий уровень контроля – *четвертый*, достаточен для программного обеспечения, используемого при защите *конфиденциальной информации*.

8.Защита от несанкционированного доступа к информации. Термины и определения. Устанавливает обязательные для применения во всех видах документации термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Безусловно, рассмотренные законодательные и нормативно-правовые акты составляют, пусть и основную, но все-таки часть системы правового обеспечения безопасности информации в Российской Федерации. Кроме того, существует целый ряд проблем в данной сфере, которые требуют своего скорейшего правового урегулирования. Принятие новых законов, безусловно, обеспечит высокую динамику производства информационных продуктов и услуг, поможет формированию и обеспечению безопасности единого информационного комплекса России.

ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ.

Организационные мероприятия всегда по праву занимают крайне важное место в системе обеспечения безопасности компьютерной информации, поскольку зачастую возможности несанкционированного доступа к охраняемой информации обуславливаются главным образом не различными

техническими аспектами, наличием или отсутствием технических каналов утечки информации, а небрежностью, халатностью пользователей или персонала, игнорирующего элементарные правила защиты информации, недостатками организации системы защиты информации в самой организации, учреждении.

Организационное обеспечение безопасности информации *– это регламентация производственной деятельности и взаимоотношений пользователей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий*.

Организационные меры защиты информации и средств компьютерной техники включают в себя совокупность различных по своей направленности организационных мероприятий, к которым можно отнести следующие.

1) ***В отношении персонала*** *– подбор, проверку и инструктаж персонала, участвующего во всех стадиях информационного процесса.*

Прежде всего, речь идет о необходимости реализации в рамках организации ***специальной кадровой политики*** в отношении к персоналу, занятому обработкой конфиденциальной информации. К числу основополагающих принципов работы с персоналом можно отнести следующие.

Во-первых**,** в организации *не должно быть «доверенных лиц»*, для которых ослаблены требования внутреннего контроля. Ни высокое положение, ни стаж работы, ни близость к руководству не могут служить основанием для отмены постоянного и всестороннего контроля.

Во-вторых**,** с момента собеседования с кандидатом особое внимание

обращается не только *на проверку анкетных данных по всевозможным видам учета*, но и на целый ряд более важных моментов. Например, согласие на работу рядовым сотрудником специалиста заведомо более высокой квалификации и опыта уже является тревожным симптомом. Не исключено, что речь идет об одном из законных способов нетрадиционного сбора информации.

***В-третьих*,** одним из основополагающих принципов обеспечения безопасности информации является *«горзионтальная ротация»*. Каждые 2-3 года, а то и чаще, сотрудники должны перемещаться на новые должности и направления, что резко снижает возможность бесконтактных злоупотреблений.

В-четвертых, *жизнь не по средствам*, т.е. приобретение новой дорогой иномарки или переезд в престижный район, приобретение предметов роскоши, частые поездки за границу – все это уже многие годы служит надежным индикатором роста внимания всех контролирующих органов к деятельности данного работника.

Для предупреждения нарушений в сфере информационной безопасности *немаловажное значение имеет работа по изучению лояльности персонала предприятия и его социальной надежности, создание административно- правовой базы для снижения или исключения случаев халатного отношения к сохранности доверенных сведений конфиденциального характера.*

С содержательной точки зрения проводимая в организации специальная кадровая политика может включать в себя:

- ❑ беседы и тестирование при приеме на работу;
- ❑ ознакомление с правилами и процедурами работы с конфиденциальной информацией в данной организации;

- ❑ обучение сотрудников правилам и процедурам работы с конфиденциальной информацией;
- ❑ беседы с увольняемыми.

В результате проведения *беседы* и тестирования кандидата при приеме на работу устанавливается целесообразность приема кандидата на соответствующую вакансию. Главной целью проведения собеседования является выявления у

кандидата необходимых личных качеств. К сожалению, нередки случаи, когда моральный облик человека не соответствует его деловым качествам. В условиях же кризиса это тем более опасно, поскольку социальная и психологическая нестабильность только способствуют росту злоупотреблений служебным положением, в том числе правонарушений в области информационной безопасности.

Отбор кандидата на вакантную должность – сложный и многогранный процесс. Не владея методикой такого отбора, можно наделать массу ошибок в комплектовании штатов, что зачастую приводит к появлению дополнительных каналов утечки информации.

Не секрет, что от того, насколько умело руководитель организации или начальник отдела кадров может построить беседу с кандидатом на вакантную должность, зависит, получит или нет фирма ценного работника. Основные способы оценки кандидата на вакантную должность представлены в Таблице 1.

Способы оценки		
Психологические тесты	***Экспертная оценка деловых и личностных качеств***	***Деловые игры***

Эффективны, когда есть адаптированные тесты и выделены критериальные признаки	Предполагает привлечение группы специалистов (не менее 7 человек)	Требуют значительного времени (несколько часов … несколько дней), высокой методической подготовки ведущего

Одним из основных вопросов, особенно на этапе приема на работу, является проверка кандидата на наркотическую и алкогольную зависимость. Если наркоман лишен по тем или иным причинам очередной дозы, а у него есть доступ к конфиденциальной информации, то такой сотрудник не остановится ни перед чем. То же самое можно сказать и про людей с алкогольной зависимостью.

Необходимые сведения об этом можно получить, затребовав справку из наркологического диспансера. Однако вряд ли можно быть до конца уверенным в подлинности представленного документа, да и сколько наркозависимых лиц в настоящее время не состоят на учете у нарколога. Одним из возможных путей

решения этой проблемы может служить использование методики *иммуноферментной хроматографии,* т.е. использование так называемых «скрин- тестов», в которых реагентом являются моноклональные антитела, очень чутко и с высокой избирательностью реагирующие на вещества, образующиеся в организме человека после приема наркотика.

Важную роль в оценке пригодности кандидата на вакантную должность также играет не только уровень профессиональной подготовки, но и моральные качества работника. Сеть кадровых агентств по подбору персонала, широко развернувшаяся в последнее время, отчасти помогает работодателям. Использование этими службами различных

методик психологического тестирования позволяет отсеивать случайных людей.

Однако оценка моральных качеств, затрагивающая вопросы социальной надежности кандидата, была и остается прерогативой руководителей предприятий. При решении этой задачи обычно используются два пути. *Первый*, наиболее распространенный, характерен для небольших компаний – подбор сотрудников по рекомендациям друзей, знакомых или родственников. *Второй* путь – проведение дополнительного контроля службой безопасности предприятия (банка) или силами правоохранительных органов.

После принятия решения о приеме кандидата на работу необходимо помнить о том, что действующее российское трудовое законодательство позволяет включать в заключаемый с работником трудовой договор условия о неразглашении им охраняемой законом тайны, служебной, коммерческой и иной (ст. 57 Трудового кодекса Российской Федерации). При этом в подтверждение требований сохранения в тайне конфиденциальной информации у поступающего на работу сотрудника целесообразно взять подписку о неразглашении подобного рода информации.

Обучение сотрудников предполагает не только приобретение и систематическое поддержание на высоком уровне производственных навыков, но и психологическое их воспитание в глубокой убежденности, что необходимо выполнять существующие в организации требования секретности,

информационной безопасности и защиты интеллектуальной собственности. Систематическое обучение способствует повышению уровня компетентности руководства и сотрудников в вопросах защиты интересов

(в том числе и производственных, коммерческих) своего предприятия, организации.

Беседы с увольняющимися имеют главной целью предотвратить разглашение конфиденциальной информации или ее неправильное использование. При подготовке к беседе с увольняемым необходимо выяснить:

- характер его взаимоотношений с коллегами;
- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов;
- доступ к конфиденциальной информации и вероятный период ее устаревания;
- предполагаемое в будущем место его работы.

При организации беседы с увольняемым предпочтение отдается служебным помещениям. Руководитель в корректной и тактичной форме должен обсудить все проблемы, связанные с увольнением сотрудника. Увольняемый ни в коем случае не должен ощущать обиду, униженность, оскорбленное достоинство.

Для сохранения контакта с увольняемым необходимо дать ему возможность критично и правдиво изложить ситуацию в организации, предложить рекомендательные документы для дальнейшего трудоустройства. В дальнейшем, используя возможности службы безопасности, рекомендуется не терять уволенного сотрудника из виду, проводить оперативную проверку по новому месту работы.

Увольнение по инициативе администрации имеет свои особенности и проходит обычно в три этапа:

I этап – предварительно под соответствующим предлогом

увольняемого переводят в подразделение, где отсутствует конфиденциальная информация.

II этап – принимают меры к снижению возможного ущерба от разглашения конфиденциальных данных.

III этап – проводят собеседование по поводу увольнения (без ссылок на негативные качества сотрудника).

2) ***В отношении средств вычислительной техники:***

– *приобретение вычислительной техники исредств защиты информации, соответствующих стандартам и удостоверенных сертификатом качества по уровням защищенности,* исключая таким образом использование вычислительной техники сомнительного происхождения и неопределенного качества;

– *организация местного тестирования* для выявления возможных несоответствий, описанных в сертификате и/или заказанной спецификации.

3) ***В отношении используемого программного обеспечения:***

– *приобретение только сертифицированного ПО*, тем самым предотвращая использование заведомо некачественного ПО;

– *реализация местного тестирования ПО* на предмет выявления побочных эффектов, в том числе таких, как «люки», программные закладки и др.;

– *предотвращение использования «пиратских» копий ПО*. Это касается компьютерных игр, которые имеют самый высокий «оборот» нелегальных копий и являются идеальной средой для программных злоупотреблений;

– *организация «вакцинирования» ПО*. Данное мероприятие осуществляется в целях предотвращения «заражения» определенными компьютерным вирусами.

4) ***Организация подразделения, ответственного за обеспечения***

защиты компьютерной информации. Для непосредственной организации (построения) и эффективного функционирования системы защиты компьютерной информации может быть (а при больших объемах защищаемой информации – должна быть) создана специальная штатная служба защиты компьютерной информации, которая представляет собой штатное или нештатное подразделение, создаваемое для организации квалифицированной разработки системы защиты информации и обеспечения ее функционирования.

Основные функции службы заключаются в следующем:

- формирование требований к системе защиты в процессе создания автоматизированной системы;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования автоматизированной системы;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала автоматизированной системы правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом автоматизированной системы установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках несанкционированного доступа к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы защиты определяется следующим образом:

- численность службы защиты должна быть достаточной для выполнения всех перечисленных выше функций;
- служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием автоматизированной системы;
- сотрудники службы защиты должны иметь право доступа во все помещения, где установлена компьютерная техника и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы автоматизированной

системы, если они не отвечают требованиям защиты информации;

- службе защиты информации должны обеспечиваться все условия, необходимые для выполнения своих функций.

Естественно, все эти задачи не под силу одному человеку, особенно если организация (компания, банк и др.) довольно велика. Более того, в службу компьютерной безопасности могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию иерархии):

- ❑ *Сотрудник группы безопасности.* В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления

защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АС имеет своего сотрудника группы безопасности.

- *Администратор безопасности системы.* В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (если в этом возникает необходимость) и за хранением резервных копий.

- *Администратор безопасности данных.* В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

- *Руководитель (начальник) группы по управлению обработкой информации и защитой*. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами (при децентрализованном управлении).

Существуют различные варианты детально разработанного штатного расписания такой группы, включающие перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При

организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы.

ИНЖЕНЕРНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КОМПЮТЕРНОЙ ИНФОРМАЦИИ.

Данный вид обеспечения безопасности компьютерной информации структурно включает следующие средства защиты информации:

- ***физические;***
- ***аппаратные;***
- ***программные;***
- ***комбинированные.***

Физические средства защиты компьютерной информации.

Это, главным образом, различные устройства и сооружения, а также мероприятия, которые создают препятствия для нарушителей на путях к защищаемой информации, например, на территорию, на которой располагаются вычислительные центры, в помещения со средствами компьютерной техники, носителями данных и т.п.

Физические средства защиты выполняют следующие основные функции:

1) охрана территории и зданий;
2) охрана внутренних помещений;
3) охрана оборудования и наблюдение за ним;
4) контроль доступа в защищаемые зоны;
5) нейтрализация излучений и наводок;
6) создание препятствий визуальному наблюдению и подслушиванию;
7) противопожарная защита;
8) блокировка действий нарушителя и т.п.

Для предотвращения проникновения нарушителей на охраняемые объекты применяются следующие технические устройства:

- сверхвысокочастотные (СВЧ), ультразвуковые (УЗ) и инфракрасные (ИК) системы;
- лазерные и оптические системы;

- телевизионные (ТВ) системы;
- кабельные системы;
- системы защиты окон и дверей.

Следует сказать, что физические меры защиты информации часто недооценивают, но они тем не менее являются достаточно эффективными, особенно при обеспечении безопасности кабельных соединений внутри организации. Физическая защита кабельной системы остается главной

«ахиллесовой пятой» большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети, в связи с чем ей должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим образом избавить себя от «головной боли» по поводу неправильной прокладки кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем. К структурированным кабельным системам относятся, например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании Digital, кабельная система корпорации IBM.

Понятие «структурированная» означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и месторасположения компонентов кабельной системы. Например, кабельная система SYSTIMAX SCS состоит из внешней подсистемы (campus subsystem), аппаратных (equipment room), административной подсистемы (administrative subsystem), магистрали (backbone cabling), горизонтальной подсистемы (horizontal subsystem) и рабочих мест (work location subsystem). Внешняя подсистема состоит

из медного оптоволоконного кабеля, устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят устройства сопряжения внешних ка-

бельных линий с внутренними.

Аппаратные служат для размещения различного коммуникационного оборудования, предназначенного для обеспечения работы административной подсистемы.

Административная подсистема предназначена для быстрого и легкого управления кабельной системы SYSTIMAX SCS при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно) , устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т.д.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная система на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

И, наконец, оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает механическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемой.

Наилучшим способом защиты кабеля от физических (а иногда и температурных и химических воздействий, например, в производственных цехах) является прокладка кабелей с использованием в различной степени

защищенных коробов. При прокладке сетевого кабеля вблизи источников электромагнитного излучения необходимо выполнять следующие требования:

- неэкранированная витая пара должна отстоять минимум на 15-30 см от электрического кабеля, розеток, трансформаторов и т.д.;
- требования к коаксиальному кабелю менее жесткие: расстояние до электрической линии или электроприборов должно быть не менее 10-15 см.

Другая важная проблема правильной инсталляции и безотказной работы кабельной системы – соответствие всех ее компонентов требованиям международных стандартов.

Наибольшее распространение в настоящее время получили несколько стандартов кабельных систем.

Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенным среди них является кабель IBM type 1 – экранированная витая пара (STP) для сетей Token Ring.

Система категорий Underwriters Labs (UL) представлена этой лабораторией совместно с корпорацией Anixter. Система включает пять уровней кабелей. В настоящее время система UL приведена в соответствие с системой категорий EIA/TIA. Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standarts Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8.1 для кабельных систем на витой паре (UTP) .

В дополнение к стандарту EIA/TIA 568 существует документ DIS 11801, разработанный International Standard Organization (ISO) и International Electrotechnical Commission (IEC). Данный стандарт использует термин «категория» для отдельных кабелей и термин «класс» для кабельных систем.

Необходимо также отметить, что требования стандарта EIA/TIA 568 относятся только к сетевому кабелю. Но реальные системы, помимо кабеля, включают также соединительные разъемы, розетки, распределительные панели и другие элементы. Использование только кабеля категории 5 не гарантирует создание кабельной системы этой категории. В связи с этим все выше перечисленное оборудование должно быть также сертифицировано на соответствие данной категории кабельной системы.

Аппаратные средства защиты компьютерной информации.

Когда заходит речь об аппаратной защите в целом, недостаточно было бы упомянуть о данных средствах только лишь относительно определенного компьютера или же конкретного программного обеспечения. Помимо этого, термин «аппаратная защита» подразумевает комплексный подход для решения ряда задач и проблем, стоящих перед системным администратором, по правильной настройке достаточно защищенной внутренней локальной сети, имеющей выход в глобальную сеть Интернет. Исходя из этого, аппаратную защиту можно классифицировать на следующие виды:

- аппаратная защита программного обеспечения;
- локальная аппаратная защита (аппаратная защита компьютера и информации);
- аппаратная защита сети (аппаратная защита внутренней локальной сети с одним или несколькими выходами в Интернет).

1. ***Аппаратная защита программного обеспечения.*** На данный момент существует отдельное направление в компьютерной индустрии, занимающееся обеспечением защиты программного обеспечения от несанкционированного использования. Еще на ранних стадиях развития компьютерных технологий применялись довольно разнообразные, но недостаточно гибкие методы такой защиты. Чаще всего она основывалась

на нестандартном использовании носителей информации, которую можно обойти путем использования средств побитового копирования, поэтому после инсталляции дистрибутива «привязка» установленной прикладной программы к аппаратным характеристикам компьютера уже не играет особо важную роль. Серийные номера используются разработчиками программного обеспечения до сих пор, но возможность сделать неограниченное количество копий, если в наличии имеется только один требуемый ключ, сейчас практикуется на рынке «пиратских» компакт-дисков. В связи с этим в последнее время все большую популярность среди производителей программного обеспечения приобретают новые усовершенствованные программно-аппаратные средства защиты, известные как «аппаратные

(электронные) ключи», являющиеся одним из достаточно надежных способов борьбы с нелегальным копированием.

Электронные ключи. Под термином «электронный ключ» предполагается аппаратная реализация системы защиты и соответствующего программного обеспечения. Сам ключ представляет собой плату, защищенную корпусом, в архитектуру которой обязательно входят микросхемы памяти и иногда микропроцессор. Ключ может подключаться в слот расширения материнской платы ISA, или же к LPT, COM, PCMCIA, USB-порту компьютера. В его программное обеспечение входит модуль, который встраивается в защищаемое ПО (таким образом, данное программное обеспечение «привязывается» к ключу, а не к конкретному компьютеру), и драйвера под различные операционные системы. Ключи в большинстве своем основаны на одной из трех моделей существующих аппаратных реализаций: на основе FLASH-памяти, PIC или ASIC- чипов. Помимо этого, в некоторые ключи встраиваются дополнительные возможности в виде энергонезависимой памяти, таймеров, выбора алгоритма кодирования

данных. Что касается аппаратной реализации электронного ключа на основе FLASH-памяти, то следует заметить, что он достаточно прост и является наименее стойким ко взлому (стойкость определяется типом программной части). В архитектуру такого ключа не входит микропроцессор, а в подобных системах критическая информация (таблица переходов и ключ дешифрации) хранится в памяти. Кроме того, такие ключи обладают наименьшей степенью прозрачности для стандартных протоколов обмена. Защита заключается в считывании из ключа определѐнных данных и участков кода на этапе проверки легальности использования. Чтобы дезактивировать такую защиту, в большинстве случаев взломщику потребуется аппаратная часть системы защиты. Методика взлома основана на перехвате диалога между программной и аппаратной частями для доступа к критической информации. Другими словами, определяется алгоритм обмена информацией между ключом и компьютером, считывается информация из

FLASH-памяти и пишется соответствующий эмулятор.

Для PICи ASIC-ключей защита строится по принципиально другому методу.

В их архитектуру уже входит микропроцессор. Помимо этого, данные микросхемы включают небольшое количество оперативной памяти, память команд и память для хранения микропрограммы. В аппаратной части содержится ключ дешифрации и блоки шифрации/дешифрации данных. Ключи на этой основе намного более устойчивы ко взлому и являются более прозрачными для стандартных протоколов обмена. PIC-чипы программируются разработчиками ключей, поэтому PIC-ключи являются более дорогой перспективой для заказчика. Аппаратную копию такого ключа сделать довольно проблематично за счет того, что микропрограмма и внутренняя память защищены от внешнего считывания, но к таким ключам применимы методы криптоанализа. Достаточно сложной является также

задача перехвата ключа (основная обработка производится аппаратной частью). Однако остается возможность сохранения защищенной программы в открытом виде после того, как система защиты отработала.

Отрицательными сторонами аппаратных (электронных) ключей является:

- возможная несовместимость с программным обеспечением или аппаратурой пользователя;
- затруднение разработки и отладки программного обеспечения;
- повышение системных требований для защищаемого программного обеспечения;
- угроза кражи;
- невозможность использования защищенного программного обеспечения в портативных компьютерах;
- затраты на приобретение;
- несовместимость с аппаратными ключами других фирм;
- снижение отказоустойчивости программного обеспечения.

Следует заметить, что достаточно часто возникают конфликты ключа со стандартными устройствами, подключаемыми к портам компьютера, особенно это касается подключения к LPT и COM. Теоретически возможен случай, когда ключ получает данные, не предназначенные ему, и интерпретирует их как команду на чтение/запись FLASH-памяти, что может привести к порче хранимой

информации или нарушению протокола обмена с другим устройством, подключенным к тому же порту компьютера. Кроме того, возможны угрозы перегрузки трафика при конфликтах с сетевым программным или аппаратным обеспечением.

«Ключевые диски». В настоящий момент этот вариант защиты программного обеспечения мало распространен в связи с его устареванием.

Единственным его отличием от электронных ключей является то, что критическая информация содержится на ключевом носителе. Слабой стороной данного варианта является возможность перехвата считывания критической информации и незаконное копирование ключевого носителя.

СМАРТ-карты. В последнее время в качестве электронного ключа широко распространились СМАРТ-карты. Носителем информации в них является микросхема. Условно их можно разделить на микропроцессорные, карты с памятью и криптографические (поддержка алгоритмов DES, RSA и других) карты.

Карты с памятью или memory cards являются самыми простейшими из класса СМАРТ-карт. Объем их памяти составляет величину от 32 байт до 16 килобайт. Такие карты делятся на два типа: с защищенной и незащищенной (полный доступ) памятью. Уровень защиты карт памяти выше, поэтому они могут быть использованы в прикладных системах небольших финансовых оборотов.

Карты с микропроцессором или CPU cards представляют собой микрокомпьютеры и содержат все соответствующие основные компоненты. Часть данных операционной системы микропроцессорной карты доступна только еѐ внутренним программам. Также она содержит встроенные криптографические средства. За счет всего перечисленного подобная карта достаточно защищена и может быть использована в финансовых приложениях.

Подводя итоги всему вышесказанному можно сказать, что, несмотря на кажущуюся универсальность аппаратных ключей, они все-таки подвержены взлому. Разработчики ключей применяют различные способы для сведения вероятности взлома к минимуму: защита от реассемблирования, трассировки,

отладчиков и многое другое. Однако защита от трассировки и отладчиков практически бесполезна, если используется SoftIce.

2. ***Аппаратная защита компьютера и информации.*** Всю совокупность средств защиты информации, относящейся к данной группы можно, в свою очередь, подразделить на:

– средства защиты компьютеров и информации от несанкционированного доступа;

– средства защиты информации от непреднамеренных воздействий как внешних, так и внутренних.

Средства защиты компьютеров и информации от несанкционированного доступа. Данный вопрос в последнее время приобретает все большую популярность. Тенденции роста и развития внутренних ЛВС требуют более новых решений в области программно-аппаратных средств защиты от НСД. Наряду с возможностью удаленного НСД, необходимо рассматривать еще и физический доступ к определенным компьютерам сети. Во многих случаях эта задача решается системами аудиои видеонаблюдения, сигнализациями в помещениях, а также правилами допуска посторонних лиц, за соблюдением которых строго следит служба безопасности и сами сотрудники.

Помимо этого, используются средства разграничения доступа пользователей к ресурсам компьютера, средства шифрования файлов, каталогов, логических дисков, средства защиты от загрузки компьютера с дискеты, парольные защиты BIOS и многое другое. Однако есть способы обойти любое из перечисленных средств в зависимости от ситуации и установленной защиты. Осуществляться это может различными путями перехвата управления компьютера на стадии загрузки BIOS или операционной системы, а также ввода на аппаратном уровне дополнительного BIOS. Следовательно, программно реализовать хорошую

защиту довольно-таки проблематично. Именно поэтому для предотвращения подобных атак предназначена аппаратная защита компьютера. Такая защита базируется на контроле всего цикла загрузки компьютера для предотвращения использования различных загрузочных дискет и реализуется в

виде платы, подключаемой в свободный слот материнской платы компьютера. Ее программная часть проводит аудит и выполняет функции разграничения доступа к определенным ресурсам.

Отрицательные аспекты и возможность обхода. Программная часть: обход парольной защиты BIOS состоит в использовании программ, стирающих установки BIOS, или утилит изъятия паролей. В других случаях существует возможность отключения батарейки, что приводит к стиранию паролей BIOS. Изменить настройки BIOS можно, воспользовавшись программой восстановления.

Аппаратная часть: следует учитывать тот факт, что с точки зрения реализации подобной аппаратной защиты, она сама не всегда защищена от ошибок в процессе обработки поступающей информации. Вероятно, многие системные администраторы сталкивались с ситуацией, когда разным устройствам присваиваются одинаковые адреса, что вызывает конфликт на аппаратном уровне и неработоспособность обоих конфликтующих устройств. В этом и заключается один из аспектов обхода такой защиты, методика которого состоит в эмуляции аппаратного конфликта, при котором отключается аппаратная часть защиты и эмулирующее устройство и появляется возможность несанкционированного доступа к информации. В качестве эмулирующего устройства могут выступать различные сетевые карты, а также многие нестандартные платы.

Возможные решения проблем и предупреждение взлома. Первоочередной задачей в этом случае является создание замкнутой операционной среды

компьютера, отключение в BIOS возможности загрузки компьютера с дискеты, удаление конфигурационных программ и программ декодирования, отладки и трассировки. Следует также произвести разграничение доступа и осуществить контроль запускаемых приложений даже несмотря на то, что этим занимается программная часть аппаратной защиты. *Специальные защитные устройства уничтожения информации*. Решение проблемы безопасности хранения важной конфиденциальной информации было предложено также в виде специальных защитных устройств, назначением которых является удаление информации при

попытке изъятия накопителя – форматирование; первоочередная задача в первый момент действия – уничтожение информации с начала каждого накопителя, где расположены таблицы разделов и размещения файлов. Остальное будет зависеть от времени, которое проработает устройство. По прошествию нескольких минут вся информация будет уничтожена и ее практически невозможно восстановить.

Вид устройств такого принципа действия представляет собой блок, монтируемый в отсек 3,5" дисковода и имеющий автономное питание. Такое устройство применимо к накопителям типа IDE и включается в разрыв шлейфа. Для идентификации хозяина применяются электронные ключи с длиной кода 48 бит (за 10 секунд на предъявление ключа подбор исключается), а датчики, при срабатывании которых происходит уничтожение информации, выбираются хозяином самостоятельно.

Шифрующие платы. Применение средств криптозащиты является еще одним способом обеспечения сохранности информации, содержащейся на локальном компьютере. Невозможно использовать и модифицировать информацию в зашифрованных файлах и каталогах. В таком случае конфиденциальность содержащейся на носителе информации прямо пропорциональна стойкости алгоритма шифрования.

Шифрующая плата вставляется в свободный слот расширения PCI или ISA на материнской плате компьютера и выполняет функцию шифрования данных. Плата позволяет шифровать каталоги и диски. Оптимальным является способ шифрования всего содержимого жесткого диска, включая загрузочные сектора, таблицы разбиения и таблицы размещения файловой системы. Ключи шифрования хранятся на отдельной дискете.

Шифрующие платы гарантируют высокую степень защиты информации, но их применение значительно снижает скорость обработки данных. Существует вероятность аппаратного конфликта с другими устройствами.

Средства защиты информации от непреднамеренных воздействий как внешних, так и внутренних. К данной группе устройств можно отнести, прежде всего, источники бесперебойного питания аппаратуры, а также различные

устройства стабилизации, предохраняющие от резких скачкообразных перепадов напряжения и пиковых нагрузок в сети электропитания.

Следует отметить, что установка источников бесперебойного питания в настоящее время является наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение определенного промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитных носителях. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства – серверы, концентраторы, мосты и т.д. оснащены собственными дублированными системами электропитания.

3. ***Аппаратная защита сети.*** На сегодняшний день многие достаточно развитые компании и организации имеют внутреннюю локальную сеть. Развитие ЛВС (локальной вычислительной сети) прямо пропорционально росту компании, неотъемлемой частью жизненного цикла которой является подключение локальной сети к бескрайним просторам Интернета. Вместе с тем сеть Интернет неподконтрольна (в этом несложно убедиться), поэтому компании должны серьезно позаботиться о безопасности своих внутренних сетей. Подключаемые к Интернету ЛВС в большинстве случаев очень уязвимы к неавторизированному доступу и внешним атакам без должной защиты. Такую защиту обеспечивает межсетевой экран (брандмауэр или firewall).

Брандмауэры существуют двух видов: программные и аппаратные. Однако, помимо этого, их делят еще и на типы: брандмауэр сетевого уровня (фильтры пакетов) и прикладного уровня (шлюзы приложений). Фильтры пакетов более быстрые и гибкие в отличие от брандмауэров прикладного уровня. Последние направляют специальному приложению-обрабочику все приходящие пакеты извне, что замедляет работу.

Для программных брандмауэров необходим отдельный компьютер на базе традиционных операционных систем Unix либо Windows NT. Такой брандмауэр может служить единой точкой входа во внутреннюю сеть. Слабость и ненадежность подобной защиты заключается не столько в возможных нарушениях корректной работы самого программного брандмауэра, сколько в уязвимости используемых операционных систем, на базе которых функционирует межсетевой экран. Аппаратные брандмауэры построены на базе специально разработанных для этой цели собственных операционных систем. Далее приступим к рассмотрению именно аппаратных брандмауэров.

Правильная установка и конфигурация межсетевого экрана – первый шаг на пути к намеченной цели. Чтобы выполнить установку аппаратного брандмауэра, нужно подключить его в сеть и произвести необходимое конфигурирование. *В простейшем случае брандмауэр – это устройство, предотвращающее доступ во внутреннюю сеть пользователей извне*. Он не является отдельной компонентой, а представляет собой целую стратегию защиты ресурсов организации. *Основная функция брандмауэра – централизация управления доступом*. Он решает многие виды задач, но основными являются анализ пакетов, фильтрация и перенаправление трафика, аутентификация подключений, блокирование протоколов или содержимого, шифрование данных.

Методика построения защищенной сети и политика безопасности. В процессе конфигурирования брандмауэра следует пойти на компромиссы между удобством и безопасностью. До определенной степени межсетевые экраны должны быть прозрачными для внутренних пользователей сети и запрещать доступ других пользователей извне. Такая политика обеспечивает достаточно хорошую защиту.

Важной задачей является защита сети изнутри. Для обеспечения хорошей функциональной защиты от внешней и внутренней угрозы следует устанавливать несколько брандмауэров. Именно поэтому на сегодняшний день широкое распространение получили именно аппаратные межсетевые экраны. Довольно часто используется специальный сегмент внутренней сети, защищенный извне и

изолированный от остальных, так называемая демилитаризованная зона (DMZ). Иногда брандмауэры разных типов объединяют. Различная конфигурация брандмауэров на основе нескольких архитектур обеспечит должный уровень безопасности для сети с разной степенью риска. Допустим, последовательное соединение брандмауэров сетевого и

прикладного уровня в сети с высоким риском может оказаться наилучшим решением.

Существует довольно-таки много решений относительно более-менее безопасных схем подключения брандмауэров для проектирования правильной защиты внутренней сети. В данном случае рассмотрены только самые оптимальные в отношении поставленной задачи виды подключений.

Довольно часто подключение осуществляется через внешний маршрутизатор. В таком случае снаружи виден только брандмауэр, именно поэтому подобная схема наиболее предпочтительна с точки зрения безопасности локальной вычислительной сети.

Брандмауэр также может использоваться в качестве внешнего маршрутизатора. Программные брандмауэры создаются на базе последних и интегрируются в них. Это наиболее комплексное и быстрое решение, хотя и довольно дорогостоящее. Такой подход не зависит от типа операционной системы и приложений.

В случае, когда сервера должны быть видимы снаружи, брандмауэром защищается только одна подсеть, подключаемая к маршрутизатору.

Для повышения уровня безопасности интранета больших компаний возможно комбинированное использование брандмауэров и фильтрующих маршрутизаторов для обеспечения строгого управления доступом и проведения должного аудита сети. В подобных случаях используются такие методы, как экранирование хостов и подсетей.

Брандмауэр не является абсолютной гарантией защиты внутренней сети от удаленных атак, несмотря на то, что осуществляет сетевую политику разграничения доступа к определенным ресурсам. Во множестве случаев достаточно вывести из строя лишь один межсетевой экран, защищающий

определенный сегмент, чтобы отключить всю сеть от внешнего мира и при этом нанести достаточный ущерб, вызвав большие сбои в работе организации или компании. Не стоит игнорировать тот факт, что брандмауэры никогда не решали внутренних проблем, связанных с физическим доступом к серверам и рабочим станциям неуполномоченных лиц, слабыми паролями, вирусами с дискет пользователей и многим другим.

Но из всего вышесказанного отнюдь не следует, что их использование абсолютно бессмысленно и неэффективно. Наоборот, применение брандмауэров – необходимое условие обеспечения безопасности сети, однако нужно помнить, что всех проблем они не решат.

В заключении рассмотрения данной группы мер защиты компьютерной информации следует отметить, что в условиях поставленных задач, различных между собой, необходимо рассматривать соответственно различные возможные варианты их решения.

Программные средства защиты компьютерной информации.

Программные средства защиты информации предназначены, во-первых, для непосредственной защиты машинной информации, программных средств, компьютерной техники, а во-вторых, для обеспечения должного контроля за правильностью осуществления процессов ее ввода, вывода, обработки, записи, стирания, чтения и передачи информации по каналам связи.

В своей совокупности программные средства защиты компьютерной информации, в зависимости от направленности, можно подразделить на две основные группы:

- ❑ программные средства защиты информации при ее передаче по каналам

«пользователь-компьютер», «компьютер-компьютер»;

- ❑ программные средства обеспечения доступа только к разрешенным данным, хранящимся в ЭВМ, и выполнение только допустимых операций над ними.

К первой группе программных средств относятся, прежде всего,

программные средства, реализующие различные методы шифрования (криптографические методы защиты информации).

Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования . Криптографический метод защиты информации, безусловно, является одним из самых надежных, так как сохраняется непосредственно сама информация, а не доступ к ней. Данный метод защиты реализуется в виде программ или пакетов программ, расширяющих возможности стандартной операционной системы.

Следует отметить, что шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с изменением потребностей и некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Финансовые службы компаний (прежде всего, в США) представляют важную и большую пользовательскую базу, и часто специфические требования предъявляются к алгоритму, используемому в процессе

шифрования. Опубликованные алгоритмы, например DES (см. ниже) , являются обязательными. В то же время рынок коммерческих систем не всегда требует такой строгой защиты, как правительственные или оборонные ведомства, поэтому возможно применение продуктов и другого типа, например PGP (Pretty Good Privacy) .

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном) . Остановимся подробнее на первом типе, представляющем большой интерес. Наиболее распространены два алгоритма.

Стандарт шифрования данных DES (Data Encryption Standart) был разработан фирмой IBM в начале 70-х годов и в настоящее время является

правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадрилионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

`

Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и

устройства для защиты объектов и информации. Справочное пособие. – СПб.: Лань, 1996. – С.153.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдеманом в 1976 году и представляет собой значительный шаг в криптографии. Этот

алгоритм также был принят в качестве стандарта Национальным Бюро Стандартов.

DES технически является *симметричным* алгоритмом, а RSA – *ассиметричным*, то есть он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрования сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает ненужными секретные соглашения о передаче ключей между корреспондентами. DES определяет длину данных и ключа в битах, а RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но становится длительнее и процесс шифрования и дешифрования)

. Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации ключа RSA десятки секунд. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES разработчики аппаратуры.

Правильный выбор системы шифрования позволяет достичь следующие

цели:

- скрыть содержание документа от посторонних лиц (обеспечение

конфиденциальности документа) путем шифрования его содержимого;

- обеспечить совместное использование документа группой пользователей системы путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, содержание документа является недоступным;
- своевременно обнаружить искажение, подделку документа

(обеспечение целостности документа) путем введения криптографического контрольного признака;

– удостовериться в том, что абонент, с которым происходит взаимодействие в сети, является именно тем, за кого он себя выдает (аутентификация абонента/источника данных).

К этой же группе программных средств защиты компьютерной информации следует отнести и *«антивирусное» программное обеспечение*.

Всю совокупность программ данного класса можно подразделить на пять основных групп :

❑ *программы-детекторы* позволяют обнаружить файлы, зараженные вирусом. Работа детекторов основывается на поиске участка кода, принадлежащего тому или иному вирусу. К сожалению, детекторы не гарантируют обнаружение «свежих» вирусов, хотя в некоторых из них для этого предусмотрены особые средства;

❑ *программы-доктора* «лечат» зараженные программы или диски, уничтожая тело вируса. При этом в ряде случаев информация может быть утеряна, так как некоторые вирусы настолько искажают среду обитания, что ее исходное состояние не может быть восстановлено;

❑ *программы-ревизоры* сначала запоминают сведения о состоянии программ и системных областей дисков, а в дальнейшем сравнивают их состояние с исходным. При выявлении несоответствия выдают сообщение пользователю. Работа этих программ основана на проверке целостности файлов путем подсчета контрольной суммы и ее сравнения с эталонной, вычисленной при первом запуске ревизора; возможно также использование контрольных сумм, включаемых в состав программных файлов изготовителями;

❑ *доктора-ревизоры* – это программы, объединяющие свойства

программ ревизоров и докторов, которые способны обнаружить изменения в файлах и системных областях дисков и при необходимости, в случае патологических изменений, могут автоматически вернуть файл в исходное состояние;

❑ *программы-фильтры* располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые могут использоваться вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Программы-фильтры контролируют действия, характерные

для поведения вируса, такие, как:

`

См.: Андрианов В.И., Бородин В.А., Соколов А.В. «Шпионские штучки» и

устройства для защиты объектов и информации. Справочное пособие. – СПб.: Лань, 1996. – С.165-167.

- обновление программных файлов;
- запись на жесткий диск по физическому адресу (прямая запись);
- форматирование диска;
- резидентное размещение программ в оперативной памяти.

Здесь же необходимо отметить еще одно, важное с практической точки зрения обстоятельство. Защитить компьютер от вирусов может только сам пользователь. Только правильное и своевременное применение

антивирусных средств может гарантировать его от заражения или обеспечить минимальный ущерб, если заражение все-таки произошло. Необходимо правильно организовывать работу на персональном компьютере и избегать бесконтрольной перезаписи программ с других компьютеров, в первую очередь, это касается развлекательных программ и компьютерных игр. Вторую группу программных средств защиты информации образуют средства разграничения и контроля доступа к информационным ресурсам, которые нередко представляют собой систему программно-технических средств защиты информации. Они предусматривает выполнение следую-

щих операций защиты:

а) идентификацию и аутентификацию пользователей, персонала и ресурсов системы. При этом идентификация связана с присвоением каждому объекту и/или субъекту персонального идентификатора.

В настоящее время выделяют четыре основных способа идентификации личности пользователя:

- по предмету, которым владеет человек;
- по паролю, личному идентификационному коду, которые вводятся в ЭВМ с клавиатуры;
- по физическим (антропометрическим) характеристикам личности, присущим индивидуально только ей;
- по электронной цифровой подписи (ЭЦП).

Последние два способа считаются самыми перспективными и надежными в плане достоверности идентификации личности. К ним относятся все

существующие биометрические системы санкционированного доступа, основанные на идентификации личности по таким характеристикам, как голос, размер ладони, отпечатки пальцев рук, сетчатка глаза и др.

б) проверку полномочий, заключающуюся в проверке соответствия временных интервалов разрешения доступа и прав на осуществление тех или иных действий;

в) разрешение и создание условий работы в пределах установленного регламента;

г) реагирование – задержка работ, отказ, отключение, сигнализация и т.д. при попытках несанкционированных действий.

Содержание

ПРЕДИСЛОВИЕ 3

ПОНЯТИЕ ИНФОРМАЦИИ В СОВРЕМЕННОЙ НАУКЕ, ПОНЯТИЕ И СУЩНОСТЬ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 4

ОСНОВНЫЕ СПОСОБЫ ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ С ПОМОЩЬЮ ЭВМ 13

ПОНЯТИЕ И ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ИСТОРИЯ ВОЗНИКНОВЕНИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ В РОССИИ 41

ОСНОВНЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ

ИНФОРМАЦИИ

72