А.В. ТЕРЕХОВ, В.Н. ЧЕРНЫШОВ,
А.В. СЕЛЕЗНЕВ, И.П. РАК

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

• Издательство ТГТУ •

УДК 004.056.5(075)
ББК Х.с51я73
З40

Р е ц е н з е н т ы:

Доктор технических наук, профессор
Д.А. Дмитриев

Кандидат технических наук, доцент
М.Ю. Серегин

Терехов А.В., Чернышов В.Н., Селезнев А.В., Рак И.П.

340 Защита компьютерной информации: Учебное пособие. Тамбов: Изд-во Тамб. гос. техн. ун-та, 2003. 80 с.

ISBN 5-8265-0228-2

В пособии рассмотрены правовые аспекты защиты компьютерной информации, а также программно-технические средства и приемы работы с ними, позволяющие обеспечить защиту на достаточном уровне.

Пособие предназначено для студентов специальности 021100 «Юриспруденция».

УДК 004.056.5(075)
ББК Х.с51я73

ISBN 5-8265-0228-2

Министерство образования Российской Федерации

Тамбовский государственный технический университет

А.В. ТЕРЕХОВ, В.Н. ЧЕРНЫШОВ,
А.В. СЕЛЕЗНЕВ, И.П. РАК

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Утверждено Ученым советом университета
в качестве учебного пособия

Тамбов
• Издательство ТГТУ •
2003

Учебное издание

ТЕРЕХОВ Алексей Васильевич,
ЧЕРНЫШОВ Владимир Николаевич,
СЕЛЕЗНЕВ Андрей Владимирович,
РАК Игорь Петрович

ЗАЩИТА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Учебное пособие

Редактор Т.М. Глинкина

Компьютерное макетирование И.В. Евсеевой

Подписано к печати 23.12.2003
Гарнитура Times New Roman. Формат 60 × 84/16. Бумага офсетная
Печать офсетная. Объем: 4,65 усл. печ. л.; 4,5 уч.-изд. л.
Тираж 150 экз. С. 872

Издательско-полиграфический центр ТГТУ
392000, Тамбов, Советская, 106, к. 14

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3
……..

1 ОБЩИЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ …… 4

2 ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ 9
…….….

2.1 Структура правовой защиты информации 9
……

2.2 Осуществление правовой защиты информации 15
……...

3 АДМИНИСТРАТИВНАЯ ЗАЩИТА ИНФОРМАЦИИ 26
…….....

4 ПРОГРАММНАЯ ЗАЩИТА ДАННЫХ 36
……....

4.1 Структура программной защиты 36
……

4.2 Организация программной защиты 43
……..

5 ФИЗИКО-ТЕХНИЧЕСКАЯ ЗАЩИТА ДАННЫХ 61
……

5.1 Структура физико-технической защиты данных 61
…….

5.2 Процедуры и средства физической защиты данных 64
……

СПИСОК ЛИТЕРАТУРЫ 77
……

ВВЕДЕНИЕ

В настоящее время принято говорить о новом витке в развитии общественной формации – информационном обществе. Информация становится сегодня главным ресурсом мирового сообщества. Практически любая деятельность человека тесно связана с получением, хранением, обработкой и использованием разнообразной информации. Современное общество широко пользуется благами компьютеризации и информатизации. Но пользователям компьютеров и компьютерных сетей следует учитывать, что компьютер может использоваться не только как мощное средство оптимизации и повышения эффективности всех видов юридической деятельности, но и как средство совершения противоправных действий и уголовных преступлений.

При работе с информацией многие просто не подозревают о возможных потерях, модификации, краже информации, а также о том, какой вред все это может принести. Информация во все времена имела свою цену (зачастую весьма высокую). Сбор информации, ее удаление, внесение определенных изменений в состав информации, циркулирующей на объекте конфиденциальных интересов, может привести к дезинформации по определенным сферам деятельности, учетным данным, результатам решения некоторых задач, принятию ошибочных решений. Вероятно, не зря бытует выражение, кто владеет информацией, тот владеет миром.

Шалости программистов с компьютерными вирусами – это лишь часть айсберга компьютерных преступлений. Чрезвычайно высокую опасность для общества и дополнительные проблемы для правоохранительных органов создают усиливающийся криминальный контроль над глобальными компьютерными сетями, телекоммуникациями и использование информационных технологий как для скрытого получения информации, подготовки и осуществления неправомерных действий в отношении организаций и частных лиц, так и для противодействия правоохранительным органам.

Исходя из сказанного выше, следует, что комплексное обеспечение защиты компьютерной информации, а в более широком смысле обеспечение информационной безопасности объектов и субъектов, связанных с информатизацией и использованием информации, является насущной необходимостью.

1 ОБЩИЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Поскольку информатизация связана с осуществлением информационных процессов и реализацией множества информационных отношений, то это означает, что информационная безопасность должна предусматривать безопасность всех процессов информатизации и информационных отношений, а с другой стороны, именно процессы информатизации и соответствующие информационные отношения обязаны обеспечивать информационную безопасность.

Процессы обеспечения информационной безопасности и их материальное обеспечение образуют подсистему безопасности в соответствующей системе информатизации (страны, ведомства, корпорации). Ее формирование и развитие, как и любой другой системы с множеством информационных отношений, регламентируются множеством правовых актов России и регулируются на основе информационного законодательства страны

Поскольку соответствующие требования безопасности относятся ко всем элементам, процессам и отношениям системы информатизации и информационной среды, то система информационной безопасности пересекается практически со всеми остальными информационными подсистемами и тесно связана с решением их задач. Так, в частности, в сферу системы информационной безопасности попадают следующие проблемы: обеспечение безопасности информационной деятельности субъектов информатизации и защита их прав, обеспечение безопасности потребителя информационной продукции, защита информационной собственности, защита содержания и объективной формы информационных объектов, создание объективных форм информации, наилучшим образом обеспечивающих ее сохранение, защита конфиденциальности и коммерческой ценности информации.

Очевидно, первые три проблемы имеют непосредственное отношение к таким системам, как: 1) регулирование отношений изготовителей и потребителей, сертификация; 2) защита интеллектуальной собственности, защита авторских прав; 3) соответствующее множество функциональных систем, осуществляющее информационные процессы и решающее текущие задачи информатизации.

Последние три проблемы целиком относятся к защите информации.

Система информационной безопасности и защиты информации опирается на правовую основу.

Защиту информации следует рассматривать как систему мер по созданию, обеспечению или способствованию обеспечению создания оптимальных условий прохождения всех информационных процессов (хранения, обработки, распространения), связанных с этой информацией. Создание оптимальных условий – это соответствующее совершенствование не только самих информационных процессов, но и других процессов, связанных с производством и использованием информации, т.е. проведением работ по оптимизации окружающей информационной среды в соответствии с требованиями информационной безопасности. Система защиты информации является центральным звеном в решении этой задачи.

Защита информации и данных, хранимых и обрабатываемых на компьютере, предполагает решение следующих задач.

1) Защиту данных от уничтожения, потери и порчи. Эта задача защиты данных заключается в проведении мероприятий по физическому хранению данных в компьютерах и других носителях.

2) Защиту данных от искажений при их обработке, хранении и коммуникации. Эта задача связана с предыдущей, однако имеет свои способы, методы и средства решения.

3) Защиту данных от случайного уничтожения или порчи при ее программной обработке, отображении или коммуникации. Задача заключается в обеспечении наличия в программных средствах обработки данных соответствующих функций.

4) Защиту данных от неправомерного удержания и ограничения доступа к ним. Задача заключается в организации беспрепятственного доступа к информации всем субъектам, имеющим на это право.

5) Защиту информации от несанкционированного доступа к ней. Данная задача заключается в ограждении конфиденциальной, коммерческой и другой информации от лиц, не имеющих права ею пользоваться.

6) Защиту информации от несанкционированной корректировки, изменения, дополнения, уничтожения. Защита предусматривает комплекс мер против попыток пользователей, имеющих право извлекать и использовать эту информацию, но не имеющих право изменения ее.

7) Защиту авторских и имущественных прав на информацию, программы, базы данных, на информационные системы. Поскольку нарушение этих прав влечет незаконное использование информации, то рассмотрение данной защиты в качестве формы правовой защиты данных вполне правомерно. Такая защита решается на основе правовых актов и нормативных документов России и осуществляется процедурами авторской регистрации, сертификации, патентоведения и пр. Правовая защита интеллектуальной собственности должна также быть поддержана средствами программной защиты информации.

8) Защиту содержательной сущности информации, информативности данных. Этот пункт занимает особое место в защите информации. Если все предыдущие относятся в основном к физическому состоянию информации, к проблемам безопасности ее использования, то он – к ее качественному использованию, работе, распространению, развитию. Информация – это живой, развивающийся организм, предполагающий ее активное участие в информатизации, постоянное дополнение и модификацию. Поэтому создание благоприятной среды (производственной, правовой, социальной) по ее максимально эффективному использованию является важнейшей задачей защиты информации. Данная защита выражается в совершенствовании и применении форм представления информации, документирования и правового оформления; в совершенствовании форм распространения информации.

Как и всякая другая подсистема информатизации, система защиты данных действует в интересах субъектов информационной сферы, защиты их прав. Однако эта защита прав действует опосредованно, а непосредственными объектами защиты являются информация, ее объективные формы выражения в виде данных, содержащихся на материальных носителях, а следовательно, и сами эти носители.

Объектами защиты являются:

- информационные ресурсы, хранящиеся в файлах, базах данных и знаний, текстовых и статистических справочниках, сборниках нормативно-правовой документации, переписки;

- системно-управляющее обеспечение компьютера, стандартные и инструментальные средства взаимодействия с ним, подготовки, обработки и передачи данных;
- прикладное программно-информационное обеспечение компьютера, информационные системы и технологии;
- материальные носители информации, все технические средства, на которых хранится, обрабатывается и передается информация, представленная в виде текстовых, табличных, двоично-шестнадцатеричных, графических или иных форм данных.

Для обеспечения защиты информации необходимы специальные организационно-технические системы, создаваемые на уровне страны, государственного органа, предприятия, отрасли и др. Роль этих систем возрастает по мере становления рынка информации и ее коммерциализации, с одной стороны, и развития автоматизации процессов обработки и хранения информации с помощью средств компьютерной техники, с другой стороны, и особенно при коммуникации данных по каналам компьютерных сетей.

По тематике решаемых задач, привлекаемым средствам и ресурсам, а также по множеству исполнителей защита информации подразделяется на несколько типов:

- правовую защиту данных, действующую на уровне научно-производственных структур, разработчиков систем, юридических и нормативных служб, органов и (или) лиц по документированию и правовому описанию информации, сертификации, патентоведению и выполнению других задач, направленных на защиту авторских и имущественных прав собственников, владельцев и пользователей данных;
- административную защиту данных, действующую на уровне управления организации, отрасли, корпорации и т.д. и направленную на организацию и координацию процессов защиты;
- программную защиту данных, действующую на уровне разработчиков системного, прикладного, общего и личного программно-инфор-мационного обеспечения, пользователей компьютерных систем и направленную на обеспечение хранения данных и пресечения попыток несанкционированного доступа к ним и/или их корректировки;
- физико-техническую (физическую) защиту данных, действующую на уровне производственных, технических, хозяйственных и других служб и направленную на обеспечение надежного хранения и коммуникации данных.

Все вышеуказанные типы защиты информации и их элементы тесно взаимосвязаны друг с другом, пересекаются и объединяются, интегрируясь, в единую систему. Только сочетание различных форм и содержащихся в них задач может обеспечить надежность защиты данных. Каждый из этих элементов, составляющих соответствующие подсистемы защиты информации, важен и неотъемлем от всей системы. Однако на современном этапе развития средств и ресурсов информатизации на центральное место в ней выходят правовая и программная системы защиты информации, оставляя за административной и физической системами роль организационного и технического обеспечения защиты.

Тип защиты данных определяется объектом защиты и характером взаимодействия с ним:

- содержанием и формой защиты;
- подходом к защите, обязательным или добровольным;
- целью и назначением защиты;
- уровнем защиты информации.

Содержание и форма защиты определяют ее вид – правовой, административный, программный и физико-технический.

Подход к защите определяется характером средства или продукта информатизации, его свойствами и назначением. Обязательной, как правило, централизованной защите подлежат средства, имеющие важное значение, отношение к вопросам безопасности, государственной тайне. Это относится не только к информационным ресурсам или технологиям, но и к самим средствам обязательной защиты.

Обязательная защита предполагает интеграцию всех форм защиты, однако, особую роль здесь играет программная защита от несанкционированного доступа.

Добровольной защите могут подлежать продукты информатизации ведомств, организаций или личные, если возникает необходимость в их сохранении, защите от неконтролируемого доступа, охране авторского или имущественного права. Организации, разработчики или пользователи са-

ми выбирают объекты и типы защиты, выбирают или создают средства защиты, при необходимости обращаются в специализированные учреждения.

Цели и назначение защиты соответствуют решаемым ею задачам. Здесь можно выделить следующие типы:

- хранение данных, их носителей;
- хранение средств обработки и коммуникации;
- восстановление данных;
- защита от несанкционированного доступа;
- защита авторского и имущественного права.

Уровень защиты информации определяется соответствующей системой информатизации, ее областью и информационной средой. Здесь следует выделить два основных типа – защита на общегосударственном уровне и уровне предприятия, корпорации, ведомства.

На государственном уровне защиты информации решаются задачи:

- правового регулирования защиты в контексте обеспечения информационной безопасности;
- определения стратегии защиты информации, основных направлений и форм защиты;
- определения организационных форм и структур защиты;
- обеспечения защиты информации, имеющей общегосударственное значение;
- создания стандартов документирования информации;
- создания стандартных и других необходимых средств защиты.

На корпоративном уровне, являющемся основным уровнем защиты, решаются текущие, тактические задачи в рамках обеспечения информационной безопасности страны и данной корпорации (предприятия, ведомства). На этом уровне основная роль отводится административной, программной и физической формам защиты информации. Однако на современном этапе развития информатизации здесь также большое значение придается правовой защите информации.

Нормативно-правовая база регулирования отношений пользователей, собственников и других держателей информации основана на законодательных актах России: законах РФ «Об информации и защите информации», «О государственной тайне», «Об авторском праве и смежных правах», «Об участии в международном информационном обмене» и др., указах Президента, постановлениях Правительства и других уполномоченных органов. Отношения, связанные с информационными ресурсами и средствами внутри отрасли, региона и пр., определяются их характером, назначением, свойствами, внутренними правилами и нормами работы с ними.

2 ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ

2.1 СТРУКТУРА ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

***Назначение и аспекты правовой защиты информации*. Правовая защита информации (данных) предполагает наличие регламентации прав на информацию; реализации их; контроля за процедурами реализации прав.**

Регламентация прав на информацию предусматривает регулирование взаимоотношений держателей массивов данных на основе законодательных актов Российской Федерации. На правовой базе информатизации страны создается система норм, определяющих правила пользования информацией, требования к производителям и владельцам, порядок и стандарты документирования, структуру правового оформления (регистрации, депонирования, печати) информации.

Реализация прав на информацию предполагает создание системы, осуществляющей практическую сторону соответствующих правовых взаимоотношений. Множество прав на информацию подразделяется на два основных подмножества: прав авторов, изготовителей, правообладателей; прав пользователей, потребителей информации.

Поскольку права одних из них влекут, как правило, обязанности других, то правильнее говорить о системе реализации прав и обязанностей различных держателей информации. Данная система предполагает наличие:

- множества организационных структур, производящих учет и документирование, правовое оформление информации;
- соответствующих процедур и мероприятий;
- специальных служб, ответственных за ее осуществление в пределах учреждения, ведомства или отрасли.

Контроль за правильностью и соответствием установленным нормам реализации прав на информацию осуществляется уполномоченными органами и организациями, ответственными за ее проведение. Правовой базой контроля являются правовые документы по информатизации, а также положения уголовного и процессуального права.

Контроль на корпоративном уровне предполагает также:

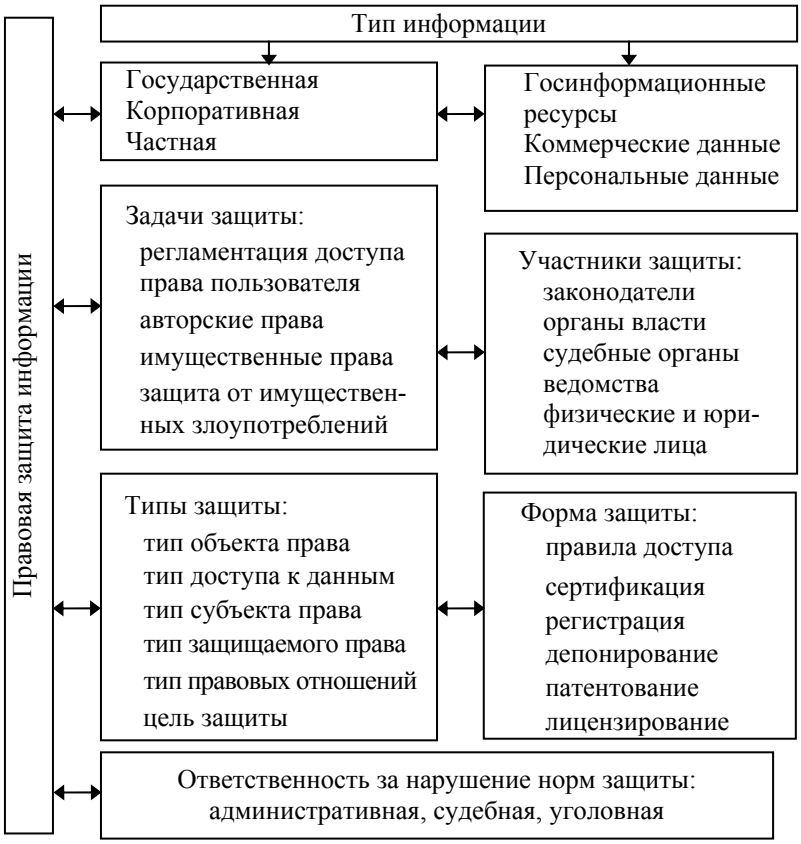
защиту своих авторов, собственников, правообладателей информации от посягательств или ущемления их прав;

защиту прав и проверку соблюдения обязанностей своих потребителей, пользователей информационных продуктов.

Структура правовой защиты данных **представлена ниже.**

Патент или заменяющий его документ обеспечивает защиту авторских и других прав заявителей с обнародованием (выпуском в свет, опубликованием) соответствующего описания разработки, в том числе, идеи разработки и пути решения задачи. В качестве разработок, которые могут быть запатентованы, в «Патентном Законе Российской Федерации» указаны «объекты промышленной собственности» – изобретения, полезные вещи и промышленные образцы.

Право на производство информационных работ или услуг, необходимость получения разрешения на которые предусмотрена правовыми актами России, дает соответствующая лицензия, выдаваемая уполномоченными на это органами.



Если документирование информации является обязательным условием ее правовой охраны, то официальное правовое оформление обычно является добровольным (кроме информационных продуктов, требующих обязательной сертификации или другой процедуры). Официальное правовое оформление не влияет на права автора или собственника информации, однако, дает им дополнительные возможности для реализации и защиты этих прав, а также обеспечивает соответствующие гласность и распространение информационной (программной) продукции.

***Нормативно-правовая база защиты данных*. Базой для построения системы защиты данных в целом и правовой защиты данных в частности являются информационные законы Российской Федерации. Основным из них является закон РФ «Об информации, информатизации и защите информации», большое значение которого состоит в том, что он ставит защиту данных в область юридического права и относит ее к приоритетным сферам заботы и ответственности государства. С принятием этого правового акта вся защита данных становится правовой, а все остальные формы защиты информации становятся лишь средствами реализации правовой защиты. В то же время любая форма и вид защиты данных должны соответствовать правовой, находиться в рамках закона и не противоречить установленным в ней нормам и стандартам.**

Закон отмечает, что правовой (юридической) защите подлежит только документированная информация, оформленная в соответствии с требованиями законодательства РФ. Естественно, недокументированную информацию также можно и нужно защищать всеми доступными средствами, если эта защита не противоречит нормам и правилам ее использования. Правила защиты данных определяются в соответствии с законодательством и разграничением компетенции между различными государственными органами или собственниками этих данных.

Основными целями и направлениями защиты данных провозглашаются предотвращение потери и искажения данных, несанкционированного использования, угрозы безопасности человеку и государству, защита прав субъектов информатизации. Защита должна производиться как в интересах держателей информации (собственников, владельцев, пользователей), так и людей, имеющих непосредственное отношение к ним (авторов, пациентов медицинских учреждений, коммерсантов).

Закон регламентирует отношения различных держателей информации (собственников, владельцев, пользователей), их права и взаимные обязанности по предоставлению и использованию информации.

Закон устанавливает ответственность за нарушение требований и правил защиты информации: административную (наказание, возмещение ущерба), судебную (на уровне арбитражного или третейского суда), уголовную.

Законы РФ «Об авторском праве и смежных правах» и «О правовой охране программ для электронных вычислительных машин и баз данных» определяют:

- субъекты и объекты авторского, имущественного права, а также другого (смежного) права, в том числе, программу, базу данных, авторское право;
- основные положения авторского и смежного с ним права, в том числе, их защиты;
- правила распространения, использования, правовой (официальной) регистрации программ, баз данных.

Данные законы создают правовую базу для официального удостоверения и защиты авторских и имущественных прав на информационные продукты, рассматриваемые как произведения, прав на неприкосновенность программы и базы данных или их частей, защиты «чести и достоинства автора».

Правовая база процессов патентоведения основана в «Патентном Законе Российской Федерации», указах и постановлениях по вопросам патентоведения.

Вопросы лицензирования работ и услуг регламентируются в соответствующих законах, указах президента и постановлениях правительства.

Правовую базу защиты информации составляют также международные документы и соглашения, признаваемые или подписанные Россией. Это, в частности, Всемирная конвенция «Об авторском праве», ратифицированная СССР в 1973 г. (действительная для РФ как правопреемнице СССР), а также Бернская конвенция о защите интеллектуальной собственности зарубежных физических и юридических лиц, ратифицированная нашей страной в 1995 г.

К нормативно-правовым основам информационной безопасности и защиты информации относятся также «Руководящие документы» по защите от несанкционированного доступа, подготовленные Гостехкомиссией при Президенте РФ, а также гармонизированные ею «Критерии оценки безопасности информационных технологий» ITSEC, или «Европейские критерии». Данные документы имеют отношение, в основном, к программной и физической формам защиты, занятым практическим формированием ее систем.

Для организации и создания действенной системы информационной безопасности, как на национальном, так и международном уровнях, необходимы единые системы критериев и оценок. В «Европейских критериях» сформулированы общие требования информационной безопасности и критерии ее оценки. Эти требования и система оценок служат ориентиром при построении эффективной системы защиты данных.

Основу системы оценок и критериев составляют следующие понятия.

Гарантированность информационной безопасности – эффективность и корректность средств безопасности. Гарантированность определяется степенью уверенности в безопасности и защите.

Эффективность безопасности – это степень достоинства и пригодности средств защиты. Эффективность определяется мощностью (качеством и надежностью) механизмов защиты. Выделяются базовая, средняя и высокая мощности.

Корректность безопасности – это степень правильности реализации механизмов защиты при создании и использовании объекта. Выделяются 7 степеней – от Е0 до Е6.

Функциональность системы безопасности – это множество функций и возможностей, которыми обладают применяемые механизмы защиты. В перечень основных функций включены:

- идентификация и аутентификация;
- безопасность обмена данными;
- управление доступом, подотчетность;
- обеспечение точности (целостности) информации;
- надежность обслуживания.

Определяются 10 классов функциональности – от низких потребностей защиты и безопасности до высоких.

В «Руководящих документах Гостехкомиссиии» дается правовое описание защиты от несанкционированного доступа (НСД) к данным, обрабатываемым средствами вычислительной техники (СВТ) и автоматизированными системами (АС). Стратегия и задачи защиты формулируются в «Концепции защиты СВТ и АС от НСД к информации».

Автоматизированная система рассматривается как интеграция самой АС, операционной среды функционирования и соответствующего программно-информационного обеспечения, предусматривающая их активное взаимодействие. Поэтому, если защита данных СВТ относится в основном к физической форме защиты (данные статичны и только хранятся), то защита данных АС – это преимущественно программная форма, включающая следующие функции и процедуры:

проверка полномочий пользователей, регистрация;

построение модели нарушителя;

внедрение и создание средств защиты;

криптография;

обеспечение целостности данных;

установление соответствия технологии обработки и системы информационной безопасности.

Данные в АС переменны, взаимосвязаны и взаимодействуют друг с другом при выполнении различных информационных процессов. Основными требованиями защиты данных в АС в «Руководящих документах» являются:

- обеспеченность всеми необходимыми программно-техническими средствами на всех технологических этапах обработки информации и во всех режимах функционирования;
- отсутствие существенного снижения эффективности работы АС, ухудшения ее основных функциональных характеристик.

Построение системы защиты программной и физической защиты данных предусматривает решение следующих задач:

- создание необходимых средств защиты;
- оценку эффективности средств защиты, учитывающей характеристики объектов и средств защиты;
- контроль эффективности средств защиты – периодический, по мере необходимости, контролирующими органами.

Проверка полномочий пользователя, регистрация и защита от НСД должны осуществляться системой разграничения субъектов и объектов доступа и системой учета информации.

В качестве субъекта доступа рассматривается «лицо или процесс, действия которых регламентируются правилами разграничения доступа», объекта доступа – единицы информационного ресурса АС, доступ к которой регламентируется правилами разграничения доступа. Нарушитель – это субъект доступа, осуществляющий несанкционированный доступ к информации.

2.2 ОСУЩЕСТВЛЕНИЕ ПРАВОВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Документирование информации. Правовая защита информации так же, как и охрана прав лиц, имеющих к ней отношение, требует определенной формализации ее представления. Информационный массив или блок с неопределенными реквизитами назначения, идентификации и принадлежности не может быть предметом правовой защиты. Для осуществления защиты, особенно правовой, необходимо четкое и полное представление о:

- предмете защите (что надо защищать);
- системе защиты (как надо защищать);
- процессах защиты (какие процедуры надо выполнить);
- средствах защиты (с помощью чего надо защищать).

Поэтому в соответствии с законами России защищаемая информация должна быть документирована, что означает:

- указание признаков, однозначно определяющих и выделяющих ее среди других информационных блоков (идентификация информации);
- определение отношений к ней, указание авторов, собственника, других субъектов, а также сведений о них, предусмотренных действующей формой документирования;
- документированное описание, выполняемое в соответствии с требованиями документирования.

Идентификация информационных объектов предполагает не только наличие признаков унификации, индивидуальности и отличия от других объектов, но и их четкую классификацию в соответствии с их назначением, содержанием и формой представления, указание их типов (программы, базы данных, информационные ресурсы или системы и т.д.).

Формализация представления информации предполагает соответствующую формализацию, а значит, и стандартизацию ее документирования, унификацию ее форм и содержания. Эти формы зависят от типа и назначения информации, соответствующих требований, норм и стандартов, устанавливаемых уполномоченными на это государственными и корпоративными органами. Обязательные элементы документирования (правила, порядок, ГОСТы и пр.) определяются государственными или другими органами, ответственными за их разработку или осуществление официального правового оформления. Дополнительно могут указываться другие сведения и реквизиты, устанавливаемые корпоративными органами или администрацией учреждения и требуемые для рационального и эффективного использования и развития (модификации) данной информации.

В соответствии с законодательством Российской Федерации, в частности, с законом «О стандартизации», органом, ответственным за управление стандартизацией технико-информационной документации и координацией работ по ее осуществлению, является Госстандарт РФ. На Госстандарт возложен также контроль за соблюдением обязательных требований государственных стандартов. На основе этих стандартов (ГОСТов) производится документированное описание информационной продукции.

Другие организации и ведомства Российской Федерации, в том числе государственные органы, субъекты хозяйственной деятельности, общественные объединения, организуют и проводят работы по стандартизации информации, в том числе, информационных продуктов в пределах своей компетенции и в соответствии с правовыми актами России.

Как видно из вышесказанного, документирование информации – это не только ее унификация и наделение неким паспортом с некоторым множеством реквизитов. В зависимости от вида информационного продукта требуется подготовка определенных сопроводительных документов, составляющих документированное описание данного продукта, состав которых определяется нормами и порядком этого описания. Документирование информации обеспечивает не только ее однозначное определение, но и, как следствие из этого, длительное хранение в составе соответствующего фонда или банка данных, быстрый поиск, а значит, эффективное и плодотворное использование.

Правовое оформление информации **состоит из двух этапов: 1) документирования информации; 2) ее официального оформления.**

Документирование является первым и необходимым этапом для дальнейшего правового оформления.

Официальное правовое оформление документированной информации производится в соответствии с законодательством России по информатизации и осуществляется в установленных им формах регистрации и депонирования, лицензирования, патентоведения, сертификации.

Это оформление может быть обязательным по отношению к сертификации (для информации с ограниченным доступом) и лицензированию (на право ведения работ или использования информационного продукта).

К обязательной регистрации относится также предоставление обязательного экземпляра документов (программ, отчетов НИОКР и пр.) в государственные информационные фонды.

Решение о добровольном официальном оформлении информации, (добровольной сертификации, регистрации и т.д.) принимается ее собственником (правообладателем) в целях лучшей реализации своих прав и возможностей. Однако во многих случаях эта операция является необходимым условием для успешной рекламы и распространения (продажи) продукции, защиты авторских прав.

Для выявления требуемых типов правового оформления необходимо определение правового статуса информации, информационных продуктов в соответствии с их принадлежностью, категориями доступа и распространения, а также с их информационными типами.

В учреждениях, ведомствах, занимающихся созданием, разработкой информационных продуктов, ресурсов, технологий и систем, практическую работу в этом направлении осуществляет корпоративная служба документирования и ведения научно-технической информации. Процедуры правового оформления требуют определенных знаний, в частности:

- содержания прав и обязанностей субъектов информатизации, структуры охраны прав;
- функциональных и организационных структур соответствующих систем;
- порядка оформления и подготовки необходимых документов и представляемых информационных продуктов;
- форм защиты информационных прав и методов борьбы с их нарушениями.

Поэтому в этой службе должны быть специалисты с соответствующей информационной и правовой подготовкой – эксперты-аудиторы, достаточно хорошо знающие вопросы информатизации и информационных процессов, а также их нормативно-правовую базу.

***Использование информационного товарного знака*. Идентификация информационного продукта осуществляется на уровнях его названия, содержания, отличительных знаков и пр. Одним из таких отличительных знаков может быть товарный знак.**

В законе РФ «О товарных знаках, знаках обслуживания и наименованных мест происхождения товаров» товарные знаки определены как «обозначения, способные отличать соответственно товары и услуги одних юридических или физических лиц от однородных товаров и услуг других юридических или физических лиц». На зарегистрированный в официальном порядке (в Патентном ведомстве) товарный знак выдается свидетельство на имя физического или юридического лица.

По закону «в качестве товарных знаков могут быть зарегистрированы словесные, изобразительные, объемные и другие обозначения или их комбинации... в любом цвете или цветовом сочетании».

Владелец товарного знака (обладатель свидетельства на него) имеет исключительное право пользоваться и распоряжаться им. Нарушением его прав «признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения, в отношении однородных товаров».

Применительно к информации (информационным продуктам) товарным знаком может быть название продукта; аудиовизуальное изображение, кадры на экране.

Форма представления товарного знака зависит от типа информационного продукта, в который он включается, и, конечно, от выбора и фантазии его владельца. В частности знак может быть представлен:

- в символьной форме в виде текста;
- в виде рисунка или эмблемы, соответствующих одному кадру на экране;
- в виде множества кадров, выводимых на экран в режиме анимации – программной заставки.

Пожалуй, оптимальным выбором товарного знака является создание индивидуальной (уникальной) достаточно оригинальной заставки для информационных изделий (программ, информационных технологий, систем), которая однозначно определяет и демонстрирует отличительные признаки и характеристики фирмы, организации или физического лица. Эта заставка, имеющая постоянную зарегистрированную форму, может содержать название изделия, атрибуты изготовителя (автора, собственника), идентифицированные графические изображения, выдаваемые на экран в звуковом или музыкальном сопровождении. Заставка как лицо фирмы-изготовителя может переходить, например, из программы в программу. Изменение названия изделия не обязывает перерегистрировать знак, поскольку другим лицам запрещено использование знаков, «сходного до степени смешения» с зарегистрированным.

Использование товарного знака не является, конечно, решением всех задач защиты информации. Однако это, во-первых, повышает правовую защищенность информационной продукции, а во-вторых, затрудняет возможность их несанкционированного использования. При наличии легко узнаваемого товарного знака, идентифицирующего его владельца, нарушителя очень просто определить и привлечь к ответственности вплоть до уголовной.

***Правовая защита государственных информационных ресурсов*. Все государственные информационные ресурсы объявляются законодательством открытыми для свободного доступа, кроме информационных ресурсов, отнесенных к категории ограниченного доступа – конфиденциальной информации или имеющей отношение к государственной тайне (законом РФ «О государственной тайне»). Отнесение информации к категории ограниченного доступа осуществляется уполномоченными на это органами на основании соответствующих нормативных актов.**

Статус общероссийского национального достояния, как и правовой режим их хранения и использования, получают информационные ресурсы только в законодательном порядке.

К открытым информационным ресурсам относятся, в частности:

- законодательные и другие нормативно-правовые документы, данные, «необходимые для реализации прав, свобод и обязанностей граждан» (согласно Закона о государственной тайне);
- экологические, санитарно-эпидемиологические сведения, информация о чрезвычайных ситуациях и имеющая отношение к обеспечению безопасности людей;
- статистические и справочные данные о состоянии экономики, финансов, деятельности государственных органов.

Открытые информационные ресурсы хранятся в специальных информационных центрах или фондах, библиотеках, архивах или их открытых отделах, предоставляющих возможности их публичного посещения и/или доступа к информации. Вся информация открытого фонда считается открытой.

Фонды из государственных информационных ресурсов формируются специализированными органами, имеющими на это право – лицензию, выдаваемую уполномоченными органами государственной власти.

Открытая информация должна беспрепятственно предоставляться пользователям без объяснения ими целей и назначения работы с ней.

Открытая информация может не только просматриваться, но и использоваться для получения производной информации, в том числе, и в коммерческих целях. Однако при этом обязательны ссылки на источник информации. Согласно Закону РФ «Об информации, информатизации и защите информации» «Источником прибыли в этом случае является результат вложенных труда и средств при создании производной информации, но не исходная информация, полученная из государственных ресурсов».

Отказ владельца государственных или иных информационных ресурсов в доступе субъекта к информации может быть обжалован в судебном порядке.

***Правовая защита персональных данных*. Под персональными понимаются данные об отдельных физических лицах. Персональные данные отнесены законодательством России к конфиденциальным.**

Некоторые категории персональных данных могут быть включены в состав государственных информационных ресурсов (с обязательным предоставлением их уполномоченным государством органам). Это осуществляется только на основании соответствующего закона РФ. По закону РФ «Об информации, информатизации и защите информации» к вышеуказанным категориям не могут быть отнесены:

- данные о частной жизни граждан;
- данные, составляющие личную или семейную тайну;
- предметы переписки, переговоров и других сообщений.

Государственный сбор, документирование, передача и распространение таких данных, согласно названному выше закону, разрешены только по соответствующему решению суда. Законом запрещено любое использование персональных данных «в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации».

Физические (равно как и юридические) лица имеют право знать о целях и употреблении предоставляемой ими информации, а также хранимых данных о них (с правом бесплатного пользования); «ограничения возможны лишь в случаях, предусмотренных законодательством Российской Федерации».

Негосударственные и частные органы, занимающиеся сбором, хранением и обработкой персональных данных, обязаны иметь лицензию на право этой деятельности. Любые органы и лица, в ведении которых находятся эти данные, обязаны обеспечить их физическую и программную защиту, установлен-

ную в соответствии с требованиями соответствующих нормативно-правовых актов Российской Федерации.

Естественно, хранение и защита от несанкционированного доступа к персональным данным, находящимся в личном пользовании соответствующей персоны, возлагается на эту персону.

Правовая защита корпоративных и частных данных. К корпоративным и частным данным относятся все данные, находящиеся в собственности юридических и физических лиц. В качестве собственников информации эти лица обладают в полном объеме (в пределах, определенных законодательством) правами распоряжения и пользования ею. В частности, они отвечают за подготовку, хранение и распространение этих данных, а также за их защиту от несанкционированного доступа. Для того, чтобы указанная информация стала объектом права, она должна быть документирована. Собственник информации (информационных ресурсов, систем, технологий) вместе с уполномоченными им лицами (авторами, исполнителями, владельцами) определяет степень ее конфиденциальности, коммерческой тайны, стоимости, режимы доступа, распространения, определяет меры и средства защиты, осуществляет необходимые мероприятия по их организации и применению.

Гражданский Кодекс РФ дает правовое определение коммерческой информации и права на ее защиту от несанкционированного доступа: «Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности».

Открытой информацией собственник распоряжается по своему усмотрению; информационными ресурсами, отнесенными к государственной тайне, – «только с разрешения соответствующих органов государственной власти».

Корпоративная и частная информация либо отдельные экземпляры соответствующих информационных объектов могут причисляться к государственным информационным ресурсам по желанию собственника либо путем обязательного предоставления ее в государственные органы. В этом случае ее собственник не теряет своих прав и может осуществлять владение ею совместно с государством. Государство имеет также право выкупа информации у ее собственника. Перечень документированных данных, предоставляемых в государственные органы, определяется законодательством и Правительством Российской Федерации.

Собственник информации вправе:

- применять различные средства ее защиты и приостанавливать ее распространение в случае нарушения требований защиты;
- требовать соблюдения конфиденциальности своей информации, предоставляемой им в различные государственные органы.

Нормы международного информационного обмена. Под международным информационным обменом понимается передача и получение (ввоз/вывоз) информационных продуктов через Государственную границу Российской Федерации, а также оказание информационных услуг иностранным субъектам или иностранными субъектами.

Правила и нормы международного информационного обмена регулируются законом РФ «Об участии в международном информационном обмене», а также другими законами России и правовыми актами в области информатизации.

Согласно закону «Об участии в международном информационном обмене» объектами международного информационного обмена являются документированная информация, информационные ресурсы, информационные продукты, средства международного информационного обмена, разрешенные к ввозу в страну или вывозу из нее. Указанные объекты «относятся к объектам имущественных прав собственников и включаются в состав их имущества». Понятие ввоза/вывоза распространяется на передачу информации по сетевым каналам. Как один из видов распространения информации, международный обмен информацией, в частности вывоз ее за границу, зависит от ее принадлежности (имущественных прав на нее) и типа доступа к ней.

Законом не ограничен вывоз из страны открытой информации:

- законов, других нормативно-правовых актов, регулирующих права и обязанности граждан и органов государственной власти;
- информации, необходимой для обеспечения безопасности;
- массовой информации;
- документов из открытых фондов библиотек и различных информационных систем.

Ограничен вывоз из России документированной информации, относящейся:

- к категории ограниченного доступа;
- к общероссийскому национальному достоянию;
- к архивному фонду.

Вывоз государственных информационных ресурсов и других видов информации, которые находятся в государственной собственности или отнесены к категории информации с ограниченным доступом, возможен только с разрешения соответствующих органов или лицами, уполномоченными ими.

Запрещен (без специального разрешения) ввоз в Россию информационных продуктов, которые не имеют сертификата соответствия установленным требованиям или могут быть использованы для совершения противоправных действий. Не разрешается также «распространение недостоверной, ложной иностранной документированной информации, полученной в результате международного обмена».

Конфиденциальная информация, участвующая в международном информационном обмене, охраняется в соответствии с законодательством России. Однако необходимыми условиями защиты являются следующие:

- наличие у работающих с ней физических или юридических лиц лицензии на право этой работы;
- использование сертифицированных средств обмена.

Под средствами международного информационного обмена понимаются все информационные системы, компьютерные сети и сети связи, используемые в этом процессе. Включение последних в состав этих средств осуществляется при наличии международного кода, порядок получения которого устанавливается Правительством РФ.

Для использования средств международного информационного обмена необходимо разрешение их собственников.

Ответственность за нарушения защиты данных. Ответственность за нарушения правил и требований правовой защиты данных, нарушения прав субъектов в сфере формирования и пользования информационными продуктами, а также международных норм предусмотрена законодательством России, в частности, законами РФ «Об информации, информатизации и защите информации « и «Об участии в международном информационном обмене».

За нарушение действующего законодательства предусмотрена административная и судебная ответственность, которая в зависимости от состава правонарушения может осуществляться судом (при нарушении прав субъектов), арбитражным судом (при невыполнении обязательств договора, купли-продажи), третейским судом (при конфликтных ситуациях). На виновных налагается уголовная ответственность или обязанность возмещения ущерба пострадавшим.

Закон предусматривает наложение штрафа или обязанности возмещения ущерба за незаконное использование либо распространение (продажу, воспроизведение) информационной продукции, не принадлежащей нарушителю.

Новый Уголовный Кодекс (УК) России, действующий с 1 января 1997 г., предусматривает уголовное наказание за совершение компьютерных преступлений, в число которых, в частности, входят:

- несанкционированный доступ к защищаемой информации;
- несанкционированное изменение информации;
- неправомерное использование и владение информацией;
- изготовление и сбыт средств для несанкционированного доступа к информации, использования;
- компьютерный саботаж: уничтожение, блокирование, приведение в негодность программ или информации, выведение из строя компьютерного оборудования.

Уголовный Кодекс содержит специальную главу: «Компьютерные преступления». Основными статьями, квалифицирующими уголовные компьютерные преступления и устанавливающими меру наказания за них, являются следующие.

Статья 238 «Выпуск или продажа, выполнение работ либо оказание услуг, не отвечающих требованиям безопасности». Статья предусматривает наказание лиц, совершивших указанные действия, повлекшие:

- причинение вреда здоровью (до 2 лет лишения свободы);
- отягощающие обстоятельства (до 5 лет лишения свободы);
- особо отягощающие обстоятельства (4 – 10 лет лишения свободы).

Статья 272 «Неправомерный доступ к компьютерной информации». Статья предусматривает наказание за несанкционированный доступ к охраняемой законом информации на машинном носителе или в сети, который повлек что-либо из следующего:

- уничтожение, модификацию или копирование информации;
- нарушение работы ЭВМ или сети.

За такие нарушения физическое лицо может быть подвергнуто (в зависимости от состава преступления) либо штрафу в 200 – 500 минимальных зарплат, либо исправительным работам от 6 до 12 месяцев, либо лишению свободы на 1 – 2 года. За преступление групповое или с использованием служебного положения наказание увеличивается от 500 – 800 минимальных зарплат штрафа до 5 лет лишения свободы.

Наказание за несанкционированный доступ к информации и ее использование предусматривают также:

- статья 183 главы 22 «Преступление в сфере экономической деятельности» (коммерческая тайна);
- статья 137 главы 19 «Преступления против конституционных прав и свобод человека и гражданина» (персональные данные);
- статьи 275 и 276 главы 29 «Преступления против основ конституционного строя и безопасности государства» (государственные информационные ресурсы, информационная безопасность);
- статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ». В качестве таких программ имеются ввиду программы-вандалы, «троянские кони», всевозможные вирусы и другие программы, блокирующие ЭВМ, уничтожающие или искажающие информацию. Наказание предусмотрено как за создание, так и за использование или распространение таких программ. В зависимости от тяжести последствий преступления виновный может быть подвергнут штрафу до 500 минимальных зарплат или лишению свободы от 2 месяцев до 7 лет;
- статья 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Наказанию подлежат лица, причинившие своими действиями существенный вред информационным процессам либо повлекшие потерю или искажение информации. Признанный виновным лишается права занимать соответствующие должности, подвергается штрафу или лишается свободы на срок до 4 лет.

Конечно, слово «существенный» придает по отношению к нарушению оттенок субъективности оценки его меры. Видимо, это неизбежно: только экспертиза экспертов – специалистов по информатике может определить величину ущерба.

Пострадавшие в результате компьютерных нарушений и преступлений имеют право также обратиться в гражданский суд, который может:

- обязать нарушителя компенсировать материальный ущерб, причиненный его действиями;
- обязать нарушителя компенсировать моральный ущерб (в материальном или другом выражении).

Причем, суд может обязать нарушителя компенсировать и то, и другое одновременно.

3 АДМИНИСТРАТИВНАЯ ЗАЩИТА ИНФОРМАЦИИ

Административная форма защиты данных. Административная форма защиты информации (данных) – это комплекс мер, направленных на создание системы защиты, организацию всех ее остальных форм, повышение их надежности. Меры административной защиты могут приниматься на различных уровнях, имеющих определенную степень иерархии: страны, республики, региона, отрасли; администрации и служб учреждения, корпорации и т.д.; исполнителя работ, обслуживающей организации; администратора базы данных, сети и других программно-информационных систем.

Административная защита информации, действующая на основе положений правовой защиты, предусматривает:

- определение стратегии, планирование, координацию и руководство процессами представления информации, обработки, хранения и коммуникации данных;
- планирование и организацию системы мероприятий по предотвращению несанкционированного доступа к информации;
- планирование аварийных работ по спасению информации в нештатных ситуациях;
- организацию защиты авторских и имущественных прав на информацию.

Правовая защита определяет защиту информации, административная – создает структуру действующей системы защиты. Предполагается комплексное решение этих задач, реализующееся в перспективном и текущем планировании, в организации проведения повседневных, регулярных и периодических работ по всем типам и формам защиты данных.

В организационном плане административная защита предлагает создание системы защиты соответствующего уровня, включающей:

- структуру задач, процессов и процедур;
- необходимые службы, органы;
- множество взаимосвязей и взаимодействия.

Административная защита, как правило, предполагает логическую замкнутость на определенном участке, производственной и информационной области, т.е. носит корпоративный характер. Следовательно, задачи административной защиты информации и их решение находятся в логической связи с другими информационными и функциональными задачами корпорации и имеют с ними общее планирование.

***Определение задач и средств защиты информации*. Главная проблема, стоящая перед административной защитой информации – это определение ее стратегии, множества задач, а также выбор методов и средств этой защиты.**

Основные проблемы и задачи, как и средства защиты данных, носят стандартизированный характер, т.е. типичны для любой информационной области. Однако в каждом конкретном случае существует своя специфика, обусловленная характером защищаемой информации и производственными условиями ее представления и обработки.

Для определения характера информации требуется достаточно полное и четкое описание информационных потоков, поступающих, формирующихся и передаваемых, обрабатываемых и хранимых; методов и форм их представления в виде данных, позволяющих сделать их идентификацию и классификацию.

Это описание предусматривает учет и паспортизацию всех входных и выходных информационных потоков, программных средств. Паспортизация предполагает анкетированное заполнение специальной таблицы (паспорта, классификатора), содержащей сведения о физических, логических, правовых и прочих свойствах и характеристиках данных.

Производственные условия реализации информационных процессов – это:

- наличие/отсутствие основных технических и программных средств представления информации, хранения, обработки и передачи данных, а также необходимого дополнительного оборудования;
- производственные и правовые отношения с заказчиками, пользователями, собственниками данных, информационных продуктов и комплексов;
- характер обработки и хранения данных;
- множество производственных и деловых связей, технология и объемы коммуникации данных.

***Состав и схема административной защиты информации*. Название данной формы защиты информации определяет ее содержание как действия по планированию мер защиты, координации соответствующих работ и руководству ими.**

Планирование защиты информации – это, прежде всего, предусмотрение всех проблем защиты, путей их решения, а также всех реальных и возможных ситуаций и условий, влияющих на сохранение информации.

В виду этого административная защита информации производится по двум основным направлениям, предусматривающим различные условия работы – нормальные и чрезвычайные.

Под нормальными условиями в информационной среде понимаются условия функционирования компьютерных систем и деятельности их пользователей в обычном рабочем режиме, т.е. в повседневных условиях «трудовых будней». В этих условиях все проблемы обработки и хранения информации (данных) возникают и решаются на основе внутренних факторов информационной среды, т.е. непосредственно в процессах, связанных с созданием и использованием информации, со всеми их позитивными и негативными проявлениями, включая и такие неприятные явления, как пиратство, вандализм и им подобные. Соответствующее планирование предусматривает организацию служб защиты информации, мероприятия по регламентации, руководству и контролю работ этих служб и пользователей ЭВМ по сохранению информации.

Под чрезвычайными условиями в сфере информатизации понимаются так называемые «нештатные ситуации», вызванные внешними факторами по отношению к информационной среде, не имеющими прямой связи с процессами подготовки и использования информации. Такими факторами являются, например, пожары, стихийные бедствия, природные катаклизмы. Эти негативные факторы могут существенно влиять на информационные процессы, нарушая нормальный порядок выполнения процессов информатизации и разрушая устоявшуюся информационную инфраструктуру. Нештатные ситуации, разумеется, не планируются, однако, должны планироваться мероприятия, призванные уменьшить до минимума отрицательные последствия в случае их возникновения; информационная деятельность в условиях их последствий; восстановление утерянных фондов данных.

Схема административной защиты данных представлена на рис. 3.1.

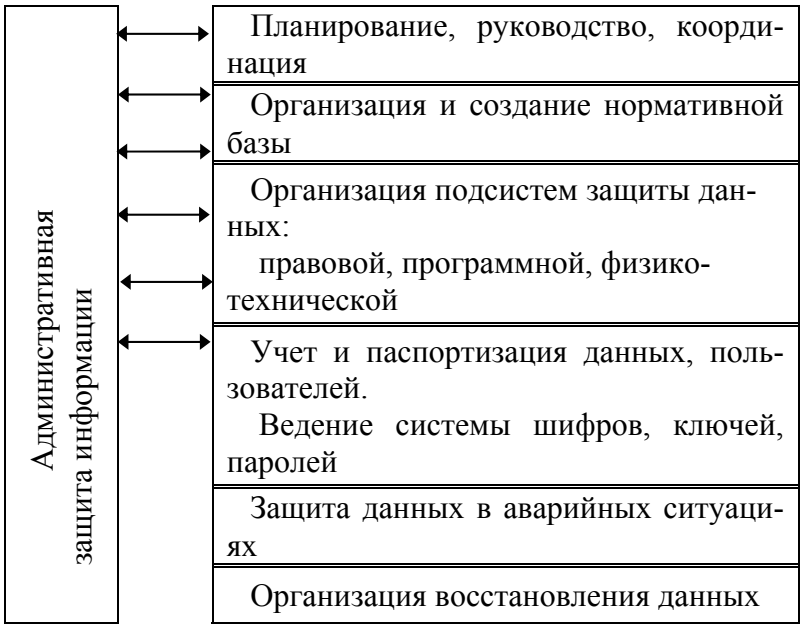


Рис. 3.1 Схема административной защиты данных

***Организация защиты информационных ресурсов государства*. Интересы государства в области информатизации защищаются законодательством, указами и постановлениями. Государственные органы, а также другие учреждения обязаны соблюдать правила и порядок работы с продуктами и средствами информатизации, являющимися предметами национального достояния или содержащими государственную тайну. Центральными исполнительными органами, ответственными за защиту государственных информационных ресурсов, являются Госстандарт РФ, Комитет при Президенте Российской Федерации по политике информатизации – Роскоминформ, Гостехкомиссия РФ, до середины 2003 года Федеральное агентство по правительственной связи при Президенте России – ФАПСИ, а с середины 2003 года ФСБ, и иные уполномоченные органы России.**

Госстандарт разрабатывает стандарты представления и документирования информации, системы защиты данных, криптографии и прочего, решает другие задачи в соответствии со своим статусом.

На Роскоминформ возложены, в частности, задачи формирования и защиты информационных ресурсов государства как национального достояния; обеспечение интересов национальной безопасности в сфере информатизации.

Роскоминформ и/или другие уполномоченные органы власти осуществляют контроль за соблюдением требований к защите информации, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом.

Роскоминформ организует регистрацию всех информационных ресурсов, информационных систем и публикацию сведений о них для обеспечения права граждан на доступ к информации.

ФСБ и Гостехкомиссия РФ ответственны за информационную безопасность страны. Гостехкомиссия РФ разрабатывает системы защиты от несанкционированного доступа к информации.

Организации, обрабатывающие государственные информационные ресурсы с ограниченным доступом, обязаны создать специальные службы для ее защиты. Эти организации (службы) должны получить лицензию у соответствующих органов на право производства средств защиты.

Информационные системы и технологии, предназначенные для обработки государственных информационных ресурсов с ограниченным доступом, а также средства их защиты, подлежат обязательной сертификации на безопасность.

***Организация и регламентация защиты*. Административность данной формы защиты данных предполагает в первую очередь участие в ее создании и функционировании представителей руководства корпорации (учреждения / ведомства). Их роль заключается в выдаче соответствующих циркуляров, планировании и организации работы, руководстве и координации, решении других общих вопросов.**

Другими участниками административной защиты данных являются юридические службы, как наиболее квалифицированные в области законодательства, в области информатики и информатизации, а также в правовых вопросах производственных и информационных отношений. Их задача – приведение ведомственных норм и инструкций по защите данных в полное соответствие с общей нормативно-правовой базой, консультации по правовым вопросам, урегулирование конфликтов.

Третье и, по-видимому, основное звено административной защиты данных образуют математики, специалисты в области информатизации и информационной безопасности. Данные специалисты, хорошо знающие структуру информации, ее представления, обработки, документирования, хранения и передачи, разрабатывают технологию защиты информации, на основе которой и осуществляется планирование, регламентация и реализация соответствующих мероприятий.

Правовые акты, действующие на уровне страны, регламентируют общие отношения, связанные с информацией и ее представлением в виде данных. На уровне предприятия, ведомства, корпорации и т.д. эти отношения также устанавливаются и регулируются на основании многих других факторов и документов:

- типовых классификаторов информации, методик и средств по реализации информационных процессов;
- норм, требований и стандартов работы с данным типом информации, а также ее оформления и документирования;
- инструкций и положений, издаваемых вышестоящими органами;
- договоров и соглашений с другими учреждениями, заказчиками или изготовителями;
- приказов и распоряжений руководства.

На основании этих факторов формируется нормативная база системы защиты информации, действующая на данном локальном участке. Для ее разработки необходимо объединение усилий руководства, юристов и математиков. В числе прочих могут быть следующие руководящие и регламентирующие документы.

Правила и Порядок работы с информационными массивами.

Правила регистрации входной и выходной документации.

Порядок оформления проектов, сопроводительных документов на программы и информационные массивы.

Порядок официального оформления информации.

Положение о разграничении имущественных прав между авторами и заказчиками или администрацией учреждения, вознаграждении и т.д.

Порядок системы сбора, хранения, выдачи информации по различным направлениям деятельности учреждения или ведомства.

Положения об информационных фондах.

Административная защита оборудования **направлена на максимально полное использование техники и аппаратуры для обеспечения информационной безопасности и защиты данных.**

Административная защита данных реализуется в рамках решения следующих стратегических задач:

1 Выбор, комплектация и размещение оборудования. Качество и безопасность хранения, полнота и надежность процессов обработки, отображения и передачи данных зависят от качества и безопасности функционирующего оборудования.

2 Вопросы размещения оборудования должны увязываться с обеспечением пожарной, электрической и электромагнитной безопасности, защитой от природных и других неблагоприятных явлений.

3 Эксплуатация оборудования, использование носителей данных. Вопросы организации и создания оптимального режима функционирования компьютерных систем и машинных носителей данных, технического обслуживания – это и решение проблем защиты данных от потери и искажения.

4 Хранение оборудования, проведение профилактических работ. Проблема хранения оборудования должна решаться таким способом, который гарантирует ее сохранность и работоспособность.

В административную защиту данных входит также организация постоянной, регулярной и периодической профилактической работы с компьютерной техникой, носителями данных, с информационными массивами и архивами, осуществление контроля за ее проведением.

5 Защита и спасение оборудования, носителей данных в аварийных ситуациях.

Планирование должно учитывать и работу в условиях частичной потери информации, а также наличие всех необходимых технических и программных средств по восстановлению утерянной или искаженной информации, а также работоспособности носителей данных.

Организация физической защиты данных **предполагает определение и планирование состава задач, процедур, технических, системных и программных средств хранения данных; создание системы хранения данных, служб, групп, распределение обязанностей и ответственности.**

Система хранения данных включает следующие подсистемы:

- учета данных;
- физического хранения данных;
- профилактики данных;
- безопасности обработки и хранения данных;
- оценки информативности и актуальности данных.

Учет данных предполагает ведение специального реестра поступающей и передаваемой информации с указанием времени перемещения или изменения; источников и адресатов данных; ответственных за хранение и обработку данных; физических характеристик данных; срока хранения.

Учет данных осуществляется на местах и в центрах подготовки и обработки данных по установленным формам.

Ответственность за хранение и обработку данных имеет особое значение.

Создание физической системы хранения информации, корпоративной или иной, в составе соответствующих групп и специалистов определяется структурой и задачами системы хранения.

Административная защита сети**. Компьютерная сеть, особенно глобальная или корпоративная, имеет сложную конфигурацию, основана на множестве технических ресурсов и программных средств. От ее организации, структуры, системы связи, обработки и обмена данными во многом зависят сохранение информации и эффективность ее защиты. Защита данных сети является обязанностью руководства соответствующих учреждений, разработчиков сети, ее администраторов и, конечно, пользователей. Выбор передовой современной аппаратуры, качественных средств коммуникации, системных средств и программных оболочек снижает до минимума риск потери и искажения данных.**

Выбор избыточного способа организации сети делает ее работу менее рациональной, но гарантирует большую надежность хранения данных. При неизбыточном способе, организации типа «клиент-

сервер», достигается гораздо большая производительность сети и рациональность обработки и хранения данных, но снижается надежность хранения: все данные концентрируются в одном месте.

Для повышения надежности сети необходимо дублирование основных средств обработки и хранения данных, особенно, центральных файл-серверов и их носителей данных.

Администратор сети, ее разработчики должны предусмотреть и назначить систему ключей, паролей, шифров, разграничивающую и регулирующую степень и порядок доступа к узлам, компьютерам, информационным системам, файлам, каталогам, возможность их корректировки, копирования или удаления.

Для важной коммерческой или секретной информации, передающейся по каналам сети, необходимо предусмотреть их криптографию.

***Защита данных при аварийных ситуациях*. Необходим четкий и подробный план действий и мероприятий на случай различных аварийных ситуаций. Такой документ должен предусматривать:**

- план мероприятий по предотвращению аварий, защите от стихийных бедствий и по уменьшению их неблагоприятного воздействия;
- план действий в аварийной обстановке: мобилизация персонала, правила поведения людей, их задачи и обязанности, спасение и эвакуация оборудования, носителей данных;
- порядок работы в условиях частичной или полной потери оборудования и/или данных;
- план мероприятий по восстановлению материально-технической базы и утерянных данных, активизации дублирующих и резервных элементов.

Аварийные ситуации могут быть следующих типов.

Сбои и поломки аппаратуры или системы. При этом возможны:

1) Выход из строя компьютерной техники. Необходимо предусмотреть дублирование основных средств, комплектацию запасными частями, квалифицированное обслуживание, обеспечивающее своевременный ремонт или замену неисправных блоков.

2) Выход из строя средств коммуникации, обрыв линий связи. Необходимо предусмотреть альтернативные или запасные линии связи. Для передачи важной информации следует иметь выделенные каналы связи. Требуется также предусмотреть план действий по ремонту средств коммуникации, систему связи с ремонтными и обслуживающими организациями.

3) Частичная или полная потеря работоспособности носителей данных. Может выйти из строя винчестер, не читаться дискета с информацией и пр. Здесь возможна замена дубликатами, исправление с помощью программных средств.

4) Неисправность в операционной системе: уничтожены или не загружаются загрузочные модули, драйверы, утилиты библиотеки ОС и т.д. Необходимо предусмотреть загрузочные дискеты, процедуры восстановления операционной системы и ее библиотек.

5) Отказ в работе программно-информационных средств или их уничтожение. Необходимо предусмотреть оперативную процедуру их восстановления с других носителей данных.

6) Необходимо также наличие службы или группы системного обслуживания и сопровождения эксплуатируемых программно-информационных пакетов и разработок.

Неблагоприятные природные явления. В результате наводнения, землетрясения, урагана и прочих стихий могут частично или полностью пострадать средства обработки, хранения и передачи данных. План мероприятий на случай стихийных бедствий должен предусматривать как действия по сведению к минимуму потери техники и информации, так и процедуру восстановления данных. Необходимы, в частности, постройка сейсмологически устойчивых прочных зданий, заграждений, готовность к эвакуации, план ее оперативного осуществления, система оповещения и сигнализации.

Следует, очевидно, предусмотреть также временную работу в условиях неполноты информации или ее обработку с помощью ЭВМ либо распределение работ на другие центры или места обработки данных.

Пожар, *взрыв*, *диверсия.* Кроме мер, аналогичных приведенным в предыдущем пункте, необходимы:

- система противопожарной безопасности, наличие средств пожаротушения, отлаженная система связи с пожарными подразделениями, аварийными службами, план действий персонала при обнаружения пожара;
- система электротехнической безопасности, наличие безопасной электропроводки, соединений, розеток, защитных коробов и пр., служба обслуживания и профилактики;
- план действий при взрыве или его угрозе, в случае обнаружения мины, бомбы и пр.;
- система защиты и спасения данных от пожаров и разрушений: несгораемые сейфы, защищенные склады и др.;
- система охраны помещений, пропусков, контроля за сохранностью имущества.

Хищение, *умышленная порча информации*, *вандализм.* Хищение может быть произведено путем бесконтрольного выноса техники, носителей данных, копированием данных с компьютера, подключением к сети, перехватом данных при их передаче и пр. Акты порчи и вандализма по отношению к информации могут быть совершены:
- при свободном или недостаточно защищенном доступе к компьютерным терминалам и файлам данных, к архивам и носителям данных;
- при внедрении в ЭВМ различного рода вирусов и программ-вандалов;
- в результате хулиганских или бандитских действий.

Административная защита предполагает организацию надежной охраны и антивирусной борьбы, защиту от несанкционированного доступа.

Организация восстановления данных. Потеря оперативных и архивных данных, выход из строя технических средств, разрушение или уничтожение материальных носителей информации в результате аварий и стихийных бедствий может привести к парализации процессов информатизации и обработки данных. Для снижения уровня негативных последствий необходима организация восстановления данных, планируемая на случай таких аварий:

1 Подготовка к возможным отрицательным последствиям.

2 Восстановление разрушенных фондов.

Подготовка к стихии включает:

1 Классификацию данных по степени важности, первоочередной необходимости, местам хранения, источникам получения;

2 Составление списков держателей информации, разработчиков программно-информационных систем;

3 Создание альтернативных (резервных, дополнительных) архивов на различных носителях данных и в достаточно удаленных друг от друга местах;

4 План мероприятий и процедур, создание организационных структур по восстановлению данных;

5 Наличие средств и источников восстановления или воспроизведения массивов данных.

Имея такие реестры хранимых данных, распределенные архивы и заблаговременно организованные группы специалистов с конкретными заданиями и планами работ, можно надеяться на достаточное быстрое восстановление утерянных фондов.

Для *оперативного восстановления* утерянных или разрушенных данных необходим комплекс следующих мер:
- получение и перезапись файлов или архивов с других компьютеров, узлов сети, архивов, в том числе, альтернативных;
- восстановление работоспособности средств хранения и обработки данных, внедрение, генерация, инсталляция системного и программного обеспечения обработки с резервных, дистрибутивных или эталонных
дисков;
- воспроизведение массивов данных, результатов обработки с помощью соответствующих программных средств.

Система мер по предотвращению отрицательных последствий стихии предполагает самое тесное сотрудничество с физической формой защиты данных, осуществляющей практическую работу по реализации этих мер.

4 ПРОГРАММНАЯ ЗАЩИТА ДАННЫХ

4.1 СТРУКТУРА ПРОГРАММНОЙ ЗАЩИТЫ

***Назначение программной защиты данных*. Программная защита данных – это комплекс мероприятий по разработке, внедрению и организации функционирования специализированного программно-информационного обеспечения, предназначенного для защиты данных. Прежде всего, это средства программной организации доступа к данным, аппаратуре, носителям данных, а также средства восстановления частично или полностью утерянных или искаженных данных.**

Программная защита данных является центральной в системе защиты данных: на этом уровне силами и средствами системного и прикладного программного обеспечения решаются все злободневные проблемы взаимодействия пользователей с информацией и взаимоотношения различных групп пользователей, разработчиков, владельцев информационных массивов и программных средств.

Программная защита данных предполагает решение следующих трех основных задач:

1) Обеспечение целостности, защита от непредусмотренных и несанкционированных изменений данных:

- обеспечение защиты операционной системы, внутренней и внешней памяти компьютера от порчи или потери;
- ведение учета состояния данных и всех его изменений; восстановление данных при нарушении их целостности.

2) Обеспечение доступности**,** защита данных от неправомерного и несанкционированного удержания:

- обеспечение доступа к информации и/или возможности ее изменения всем лицам и организациям, имеющим соответствующее право;
- защита данных при их коммуникации, в том числе, средствами электронной почты, обеспечение доступа к сетевым данным.

3) Обеспечение конфиденциальности, защита данных от несанкционированного доступа и использования:

- классификация данных по степени конфиденциальности и доступа к ним, назначение ключей, паролей, шифров и пр.;
- обеспечение конфиденциальности данных, защита их от несанкционированного доступа.

В систему программной защиты данных могут входить:

- средства защиты операционной системы и ее конфигурации, программного и информационного обеспечения от потерь и несанкционированного доступа;
- системы доступа к информации по ключам и паролям;
- средства архивации данных на машинных носителях, в том числе, под паролями;
- антивирусные и профилактические средства;
- средства кодирования и раскодирования данных;
- средства восстановления данных при их частичной и полной утрате;
- автоматизированная система копирования и дублирования наборов данных на архивные носители;
- система программ и утилит по восстановлению наборов данных с архивных или эталонных носителей.

Разработка программной защиты данных предполагает:

- создание вышеперечисленных средств и обеспечение их бесперебойной и надежной работы;
- распределение данных и системы их обработки в компьютерных сетях, обеспечивающих максимальную надежность их хранения и передачи.

Типы программной защиты. **Программная защита разделяется на несколько типов:**

- тип использования: (уровни пользователя и профессионала-разработчика);
- тип защищаемой информации: память, данные, программа;
- тип защиты: восстановление данных, защита от несанкционированного доступа, изменения, копирования и т.д.;
- тип объекта защиты: операционная система, отдельная программно-информационная система, комплексная защита данных в масштабах учреждения, ведомства, глобальной сети;
- тип средства защиты: программа, утилита, функция и пр.

На профессиональном уровне программная защита данных организуется и создается специальными службами в ходе разработки прикладного программного обеспечения; внедрения и адаптации специализированных системных и стандартных средств.

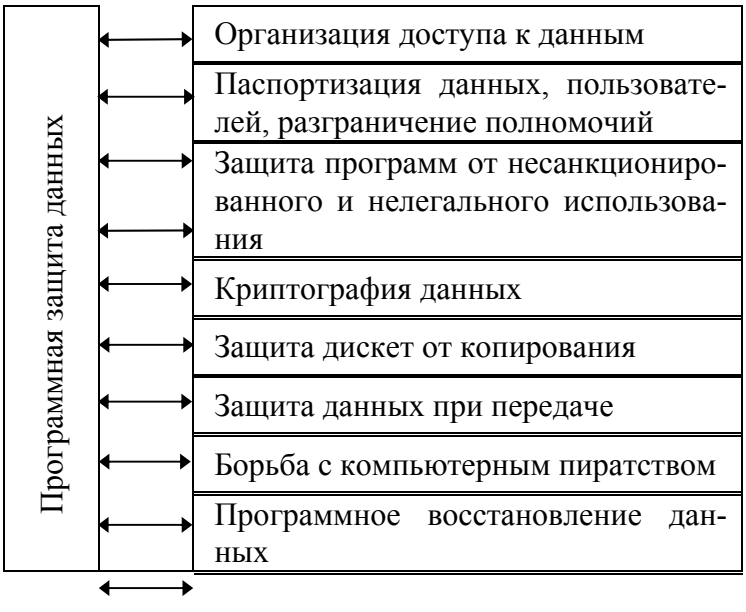
К этому типу относится разработка всех форм и средств защиты – программной, физической, правовой, включая антивирусные программы, архиваторы и пр. На стадии проектирования систем или в ходе их функционирования разработчики предусматривают средства защиты с учетом степени важности и конфиденциальности данных этих систем. В зависимости от объекта защиты, технологии их разработки, а также, разумеется, творческих потенциалов автора выбираются или создаются те или иные средства защиты.

На уровне пользователя осуществляется выбор и применение подходящих средств защиты памяти компьютера, данных или информационной системы, ограничения доступа к ним. Обычно это стандартизированные средства, рассчитанные на массовое применение по отношению к определенному типу информации. Это могут быть программы преобразования (шифрования и дешифрования) или восстановления данных, зашиты программных модулей, система ключей и паролей.

Потребность в защите компьютера или программного и другого информационного продукта может возникнуть в процессе их функционирования или распространения. Комплексная программная защита разрабатывается и осуществляется как часть общей системы защиты данных корпорации, ведомства или учреждения. Для ее реализации требуется создание специализированных служб и групп специалистов разных направлений, от администрации до высококвалифицированных математиков.

Средством защиты могут, в частности, быть специальная программа или утилита, загружаемая в оперативную память по мере необходимости; резидентная программа, проверяющая целостность данных (файлов); функции и процедуры в составе программного обеспечения баз данных, программно-информационных комплексов: преобразование, проверка ключей и паролей, структуры и содержания данных.

Схема системы программной защиты **представлена ниже.**



		Средства программной защиты: личные, стандартные, специальные
		Режим функционирования средств защиты: автономный, автоматизированный

Классификация средств защиты. **Средство защиты может быть встроено в программу разработчика в виде отдельных процедур или функций и вместе с ней скомпилировано и сформировано в единый загрузочный модуль. Обычно такая защита подготавливается самим разработчиком основного продукта. Достоинство ее в своей оригинальности, независимости от внешних факторов, может быть, дешевизне. Однако такой подход вряд ли совершенен, а главное, часто грешит «самодеятельностью» и не обеспечивает полноты и надежности защиты. Чтобы грамотно и профессионально выполнить защиту, автору разработки надо немало изучить и потратить усилий и времени, сравнимых с затраченными на основную работу.**

Второй подход – это подключение стандартизированных средств защиты к продуктам информатизации на стадии их распространения или внедрения в конкретную операционную среду. Как правило, эти средства защиты подготавливаются людьми, специализирующимися на этом поле деятельности, и распространяются в качестве программных продуктов, т.е. рассчитаны на массовое применение. В этом случае программы защиты и загрузочные модули пользователя формируются независимо друг от друга. Этот подход явно удобнее и предпочтительнее, так как:

- выше уровень защиты: она создается профессионалом, знающим, что именно надо защищать и как это осуществить;
- налицо разделение труда, когда каждый занимается своим делом, что, естественно, гарантирует большую эффективность и производительность;
- универсальность средства: однажды созданное оно приложимо к большому классу программно-информационных продуктов;
- осуществимы учет и классификация средств защиты, их выбор для защиты информационных ресурсов (в том числе и государственных) или определение возможности применения.

Кроме того, стандартные средства защиты более удобны в применении. Представленные в виде пакета модулей (программ, рабочих файлов, инструкций) в отдельном каталоге диска или на дискете, они всегда готовы к употреблению и более универсальны. Как только у разработчика программного продукта возникает потребность в его распространении, тиражировании, внедрении, он может к нему обратиться. Обычно такое средство не только защищает продукт от несанкционированного доступа или от копирования, но и формирует соответствующий пакет (из защищенной информационной системы / технологии) на дискете или другом носителе данных, снабжая его программой инсталляции и инструкцией по использованию. При формировании пакета система защиты запрашивает сведения о параметрах защиты, в частности, количестве инсталляций.

Возможно сочетание первого и второго подходов, когда, например, программа защищается стандартным средством защиты, а информация рабочих файлов шифруется/дешифруется криптографическими программами разработчика объекта защиты.

Выделяется также класс специальных средств защиты государственных информационных ресурсов, подготавливаемых специализированными службами по лицензии уполномоченных органов.

Выбор средства защиты. **Степень и надежность защиты данных (файла, программы, дискеты) от копирования зависит от используемого средства защиты. Напрашивается, казалось бы, очевидный вывод: чем лучше средство защиты, тем оно предпочтительнее для применения. Однако это далеко не так.**

Во-первых, любая защита не является абсолютно надежной. Для профессиональных «взломщиков» не составляет большого труда ее преодоление, обход, разрушение. Любые шифры, ключи и пароли устанавливаются и сохраняются лишь на ограниченное время, в течение которого по предположению авторов защиты взломщики не успеют их разгадать и разрушить. Поэтому никогда нельзя исключить вероятность того, что дорогие хлопоты по защите могут оказаться напрасными.

Во-вторых, хорошее и надежное средство защиты может оказаться дороже самого объекта защиты. Удорожание продукта может, в свою очередь, отрицательно повлиять на его реализацию, продажу. Зачем тогда все труды по его созданию и защите?

В этом случае лучше выбрать относительно надежное, но сравнительно недорогое средство защиты. Профессионалам, специализирующимся на присвоении чужих программ, пиратам от информатики выгоднее заниматься дорогими, крупными разработками: затраты их труда по разрушению защиты меньше затрат на создание продукта. Поэтому в этом случае нужна более тщательная защита, хотя и она, как видно, не гарантирует успех.

Средство защиты от копирования файлов или дискеты не должно затруднять инсталляцию и использование программного продукта. Иначе, опять же, дополнительные сложности (необходимость ключевой дискеты, например) снизят реализацию защищаемого продукта.

Функциональные свойства выбираемого средства защиты зависят от цели его применения.

Для защиты информационных объектов на конкретных компьютерных системах необходимы средства по предотвращению несанкционированного доступа и использования.

Для защиты информационной продукции требуются средства, предотвращающие ее неконтролируемое распространение.

***Борьба с пиратством*. Пиратство является одним из нецивилизованных и даже криминальных проявлений в отношениях, устанавливающихся на рынке программно-информационных продуктов. Вместо того, чтобы приобрести ту или иную разработку или информацию на законных основаниях, недобросовестные пользователи зачастую стараются правдами, а больше неправдами, найти обходные пути для их перетаскивания на свой компьютер и последующего незаконного использования. Другие пытаются продать то, что им не принадлежит или то, что они не имеют права распространять. Борьбу с проявлениями пиратства следует вести по всем возможным направлениям и всеми возможными способами, в частности:**

- более четким и полным правовым регулированием отношений в области информатизации;
- запретительными мерами, методами выявления и наказания;
- защитой данных от несанкционированного доступа и копирования;
- экономическими мерами и созданием соответствующих условий;
- повышением культуры отношений и обращения с программными продуктами.

Правовое регулирование должно предусматривать, разумеется, не только сами отношения между субъектами и объектами информатизации, но и отношения к проявлениям недобросовестного обращения с этими объектами. Регулирование должно обеспечить организацию достаточно быстрого и удобного оформления авторских и имущественных прав на продукты информатизации, документирования информации, а также эффективной и действенной правовой защиты документированной, патентованной и зарегистрированной информации, ее правообладателей.

Акты пиратства и злоупотреблений должны не только не приветствоваться, но и преследоваться. Сюда относится запрет продажи программ или баз данных на рынках, приватно или в магазине лицами, не являющимися их правообладателями, авторами или уполномоченными на это; запрет продажи или распространения несертифицированной продукции, для которой предусмотрена обязательная сертификация.

Защита от копирования является относительно эффективным и надежным средством, хотя и не может дать абсолютных гарантий: любую защиту можно при большом желании снять, разрушить.

Системой запретов и преследований, а также защитой от копирования проблему пиратства, конечно, не решить. В условиях насыщенности рынка программно-информационных продуктов пользователь при прочих равных условиях выбирает тот из них, который проще установить, т.е., не защищенный. Поэтому на многих западных программных разработках отсутствует какая-либо защита. Считается, что гораздо более эффективным средством является создание условий, при которых пиратство будет экономически и функционально невыгодным. Для того, чтобы потенциальному пользователю программного продукта было удобнее его приобрести у законного владельца, чем красть или переписывать у товарищей, возможны разнообразные средства и создание соответствующих условий:

- предоставление гарантий качества, безопасности, функциональной полноты, надежности работы и пр.;
- сдача (установка) продукта «под ключ», обучение пользователей;

- возможности обратиться с претензиями по функционированию, с предложениями к изготовителю или жалобами на него;
- возможности получить консультацию или разъяснение по интересующим вопросам, посетить семинары, конференции, посвященные состоянию данного продукта и его использования, вступить в ассоциацию пользователей этого продукта и т.д.;
- предоставление права на приоритетное и льготное приобретение новых версий продукта, полученных в процессе его развития;
- снижение цен, всевозможные скидки для оптовых, повторных покупок продуктов, установление взаимовыгодных отношений, дилерства, дистрибьютерства и пр.

Таким образом, создаются условия для долгосрочных отношений с потребителями, рассчитывающими на приобретение информационных продуктов в их развитии в авторском сопровождении.

Экономические условия выражаются и в следующем. Желая продать свою разработку, автор должен ее документировать, оформить и/или сертифицировать, указав при этом все используемые продукты, которые, разумеется, не могут иметь пиратское происхождение. Другими словами, поскольку конечной целью использования программного обеспечения является создание своего производного продукта, нелегальное приобретение необходимых для работы средств становится бессмысленным и неэффективным.

Повышение культуры пользования программными продуктами выражается в негативном отношении к пиратству, в уважении к чужому труду, чужой собственности и в знании правил и норм документирования и использования средств информатизации, и, разумеется, в необходимости, а затем и потребности их соблюдении. Повышению культуры пользования способствуют все вышеуказанные меры, а также сама атмосфера взаимоотношений на рынке программных продуктов.

Следует иметь, однако, в виду, что пока и поскольку продукция сферы информатизации является товаром, пиратство в той или иной мере будет существовать. Возможно и необходимо только ограничить его масштабы. На вполне цивилизованном информационном рынке США пиратским образом распространяется около 30 % программно-информационных продуктов, у нас – пока значительно больше (свыше 90 %). С нормализацией рыночных отношений и повышением культуры пользования следует ожидать снижение пиратства примерно до того же уровня, что и в США.

4.2 ОРГАНИЗАЦИЯ ПРОГРАММНОЙ ЗАЩИТЫ

Защита операционной системы. Защита операционной системы заключается в обеспечении условий и режимов надежного сохранения и нормального функционирования самой системы, всего программно-информационного обеспечения, работающего под ее управлением, а также средств взаимодействия с ней. Защита системы имеет два уровня – уровень ее разработчика, изготовителя и уровень пользователя.

На уровне пользователя предпринимаются меры по физическому сохранению системы (модулей, драйверов, библиотек) и обеспечению их совместимости между собой, а также с другими модулями. От пользователя зависит степень использования внутренних ресурсов и возможностей системы для защиты данных.

Задачи обеспечения внутренней целостности системы, защиты ее сегментов и блоков памяти от разрушения и искажения системных данных должны решаться самой системой, предусматриваться при ее разработке и при необходимости выполняться соответствующими процедурами. В соответствии с этим операционная система должна удовлетворять определенным требованиям и содержать необходимый сервис процедур, функций и утилит. От пользователя на данном уровне защиты требуется выбор операционной системы, обеспечивающей надлежащий уровень защиты в соответствии с требованиями его задач и процессов хранения, обработки и передачи данных, а также с существующими стандартами уровней защиты информации.

Для обеспечения нормального режима функционирования компьютера и обработки данных операционная система обязана удовлетворять множеству требований, в частности:

1 Соответствовать требованиям безопасности функционирования, выражающимся в соответствующих уровнях ее надежности, отказоустойчивости; в степени обеспечения полноты процессов обработки данных и достоверности результатов.

2 Обладать функциональными, организационными и сервисными средствами защиты данных.

Функциональные средства ядра операционной системы обеспечивают защиту ее целостности и работоспособности, а также содержимого рабочих областей оперативной памяти компьютера и хранение информации на внешних носителях. Операционная система должна обладать возможностями для создания контролируемой системы доступа к данным, исключающей несанкционированное пользование информацией. Организационные и сервисные средства операционной системы – это программы ее библиотеки по физической защите и восстановлению наборов данных и их носителей. Совокупность вышеназванных средств должна обеспечить возможность организации эффективной системы защиты данных (программной, физической).

Современная операционная система должна обладать всеми возможностями для защиты конфиденциальных данных на терминалах пользователей или на файл-серверах компьютерных сетей при их обработке и передаче по каналам связи.

Существует ряд стандартов для операционных систем, на которые ориентируются производители операционных систем, а также производят сертификацию на соответствие им. В частности, стандарт С2, разработанный министерством обороны США, включает следующие требования к ОС:

- Операционная система должна защищать себя от внешнего вмешательства, такого как модификация ее во время работы или файлов системы, хранящихся на диске.
- Операционная система должна защищать находящиеся в памяти компьютера и принадлежащие одному процессу данные от случайного использования другими процессами.
- Каждый пользователь должен быть уникальным образом идентифицированным в системе, а система – иметь возможность применения этой идентификации для отслеживания всей деятельности пользователя.
- Администраторы системы должны иметь возможность аудита всех событий, связанных с защитой системы, а также действий отдельных пользователей. Правами доступа к данным аудита должен обладать ограниченный круг администраторов.
- Система должна обладать возможностями централизованного управления привилегиями и правами, установлением сроков жизни и правил использования паролей.
- Владелец ресурса должен иметь возможность контроля доступа к нему.

Гарантию безопасности и защищенности операционной системы дает сертификат ее соответствия одному из существующих стандартов.

***Ограничение доступа к компьютеру и операционной системе*. Персональный компьютер легко может оказаться доступным не только его законному пользователю, хозяину, но и постороннему человеку, что в большинстве случаев не является желательным.**

Первый способ борьбы с этим явлением – надежная охрана компьютера, исключающая его хищение, проникновение в место его хранения посторонних или случайных лиц. Это необходимая, но недостаточная мера.

Второй способ – это ограничение доступа к памяти компьютера, внутренней и внешней, к модулям операционной системы. Применение его приводит к невозможности осуществления определенной процедуры физической работы устройств ЭВМ; загрузки системы; выхода из режима ожидания.

В целях ограничения доступа к компьютеру используют различные средства.

Вносят в AUTOEXEC. BAT или CONFIG. SYS требование выдачи ключа или пароля при загрузке системы. Такая защита малоэффективна, так как можно, например, загрузиться и с системной дискеты.

Вносят требование выдачи пароля в загрузочный модуль BIOS: при считывании 1-го сектора 0-го цилиндра 0-й дорожки, называемой главной загрузочной записью (Master boot record MBR), инициируется проверка пароля.

Аппаратный уровень: встроенная в процессор плата разрешает доступ к компьютеру только при указании пароля.

Специальным ключом блокируют клавиатуру.

Включают пароль для выхода из программы-заставки, входящей в сервис системы. Кстати, программа-заставка не только защищает пользователя и компьютер, но и скрывает отображаемые на экране данные.

С внешне эффективными методами защиты компьютера надо быть осторожными: можно забыть пароль, потерять ключ, надолго отлучиться, сделав проблематичным доступ к данным машины. К тому же

эффективность и надежность этих средств весьма относительна и не рассчитана на опытного «взломщика». Лучшим, более безопасным и эффективным средством является защита конкретных данных (файлов, программ, каталогов) от несанкционированного доступа.

В целях ограничения доступа к памяти компьютера необходимо обеспечить оперативное обнуление (очистку) областей оперативной памяти после завершения соответствующих процессов обработки данных. Это особенно актуально для компьютерных сетей.

***Программная организация доступа*. В зависимости от решаемых задач, характера обрабатываемой информации и средств ее обработки требуется регулирование области доступа к ним, возможности их модификации, копирования. Для этого требуются различные средства диспетчеризации обращения и взаимодействия с защищаемыми объектами.**

Защита может быть добровольной, когда пользователь или разработчик системы сам решает о ее необходимости, и обязательной, когда решение о защите принимается на основании характера или принадлежности информации к определенному классу либо на основании планов и решений, принятых на уровне корпорации / ведомства. Так, информация, относящаяся к государственным информационным ресурсам и представляющая предмет ограниченного доступа и распространения, подлежит обязательной защите.

Программная организация доступа предусматривает создание системы паспортизации данных; системы управления доступом; системы учета работы с данными и регистрацию изменений.

Паспортизация данных нужна для принятия квалифицированного решения о необходимости и степени защиты информационных массивов. Паспортизация предполагает идентификацию данных и полной структуры взаимоотношений между ее владельцами и различными группами ее пользователей (действительных и потенциальных). В паспорте на информационный блок данных (массив, файл, база данных) должны быть указаны, в частности, следующие сведения:

- идентификационные и физические характеристики данных;
- назначение, места хранения, средства обработки;
- источники и пути движения данных;
- время образования блока данных, срок хранения;
- авторы, владельцы информации, ответственные за хранение;
- тип использования: неизменяемый или подвергающийся обработке и изменению массив;
- тип конфиденциальности, секретности;
- необходимость и тип документирования;
- допустимые пользователи данных с указанием доступных им разделов, возможности изменения, копирования, передачи,
- приоритеты доступа, использования.

Регистрация и учет предусматривают следующее:

- учет процессов обработки и/или передачи данных;
- учет всех изменений данных;
- выдачу и передачу печатных отображений данных;
- взаимодействие программ пользователей с данными, компьютерами (серверами), каналами связи и пр.;
- учет попыток нарушения системы защиты и несанкционированного доступа к данным.

Автоматизация информационных процессов предполагает, что все это должно быть выражено программными средствами и реализовано в соответствующих информационных системах и специализированных средствах защиты данных.

Создание системы доступа предполагает решение множества задач, решаемых как непосредственно силами и средствами программной защиты, так и в процессе взаимодействия с системами правовой и административной защиты, которое выражается, в частности:

- в создании структуры доступа и его средств, программных, криптографических, системы паролей;
- в организации системы доступа, с определением и установлением множества отношений между различными информационными массивами, их собственниками, владельцами и пользователями;
- в создании и/или внедрении программных средств защиты.

Система доступа напрямую зависит от качества соответствующих применяемых средств, их подготовки и функционального содержания, в частности, от их структуры опроса пользователей и порядка ввода ключевых слов. Одними из очевидных требований являются следующие:

- Ключи и пароли должны быть оригинальными, но не громоздкими, легко запоминающимися (не хранящимися на листочках).
- Должна быть предусмотрена периодическая или по мере необходимости смена ключей, паролей и шифров.
- Ввод ключевых слов должен быть невидимым (без воспроизведения на экране). Это, если не помешает, то хотя бы затруднит подглядывание за процессом ввода.
- Введение системы паролей, ключей, разграничения полномочий является относительно надежной, но не гарантирующей предотвращение злоупотреблений с данными: при большом желании всегда можно подсмотреть или подслушать пароль. Поэтому начали применять средства идентификации пользователей на основе средств распознавания образов. Для идентификации пользователя могут использоваться специальная пластиковая карта (смарт-карта), биометрические данные, подпись, отпечатки пальцев и пр.

***Защита информационных систем*. Защиту информационной системы следует рассматривать в двух аспектах: 1) защиту ее содержания и целостности; 2) защиту от несанкционированного доступа и копирования.**

Защита содержания состоит в предотвращении случайного или умышленного его уничтожения или искажения. Об этом должны заботиться и пользователь системы (применяя средства физической защиты данных), и ее разработчик (изготовитель), поскольку именно он отвечает за достоверность и полноту информационных ресурсов системы.

Современные операционные и инструментальные системы предлагают достаточно широкий спектр такой защиты. Можно, например, при подготовке пакета для использования изменить статус файлов на Read-Only, или применять специальные утилиты из библиотеки системы для защиты и восстановления файлов.

Информационная система содержит множество файлов, составляющих ее информационные ресурсы, и программные модули системы управления и обработки этих ресурсов. В соответствии с этим защита информации от несанкционированного доступа подразделяется на два типа защиты программ и рабочих файлов.

Программы – исполнимые файлы, поэтому их защита заключается в создании такого режима, когда они не будут работать без выполнения определенных условий. А в другом качестве они практически бесполезны для обычного пользователя.

Текстовые, табличные или графические файлы можно прочитать, просмотреть, модифицировать, переписать самыми различными способами, с помощью специализированных редакторов и других программ. В сети, информационной системе можно предусмотреть множество ключей и паролей, ограничивающих доступ к узлам сети, каталогам и файлам. Но обычно имеется достаточно возможностей обращения к файлам с помощью вышеперечисленных средств. Поэтому защита файлов заключается в представлении их данных в форме, недоступной для восприятия, зашифрованном, архивированном виде, упакованном формате и т.д. Такое представление позволяет предохранять от ненужных изменений и физическое состояние файлов.

Шифрование файла заключается в разработке некоторой системы замены кодов символов данных на другие; кодировании защищаемых файлов в соответствии с этой системой; выполнении функций кодирования и раскодирования файлов или блоков данных при их обработке и ее завершении.

Некоторые архиваторы (Zip, Rar) позволяют создавать архивы с заданием пароля, который надо указать при разархивировании. Такой файл будет достаточно надежно защищен.

***Система криптографии данных*. Создать и реализовать систему шифрования данных, в принципе, технически несложно. Однако при ее использовании могут возникнуть следующие проблемы, связанные с:**

- уменьшением производительности системы, увеличением времени шифрования и дешифрования данных;
- достижением требуемого уровня секретности;
- надежностью функционирования системы: нечеткость или несовершенство алгоритма могут привести к потере данных, невозможности их восстановления (следует иметь эталонный экземпляр информационных массивов).

Построение хорошей и надежной системы криптографии (шифрования) данных является сложным и дорогостоящим делом, затраты труда на которую сравнимы с созданием большой системы. Поэтому лучше пользоваться средствами, разработанными специализированными службами по алгоритмам, проверенными теорией и практикой. Различают симметричные и асимметричные алгоритмы криптографии.

Симметричный алгоритм использует секретный ключ общей длиной в 64 бита и обеспечивает наличие почти 10^{17} переборов вариантов кодирования. При обмене информации с использованием этого алгоритма криптографии пользователи (источник и адресат) должны иметь общий для них секретный ключ, который они устанавливают заранее. Симметричная система защиты предполагает закрытое применение информации и предназначена, прежде всего, для государственной информации с ограниченным режимом пользования.

Асимметричный алгоритм криптографии использует разные ключи для шифрования и дешифрования. Один открытый ключ используется для шифрования информации. Этот ключ можно дать всем потенциальным корреспондентам пользователя компьютера. Присылаемую ими информацию, зашифрованную данным открытым ключом, может расшифровать только этот пользователь с помощью своего секретного ключа. Длина ключа нефиксирована, чем он длиннее, тем выше уровень шифрования. При этом, однако, увеличиваются процедуры шифрования и дешифрования. Асимметричный способ криптографии предполагает открытый способ взаимодействия, позволяющий создавать собственные системы шифрования. Такие системы применяются при коммуникации коммерческих данных.

***Стандарты криптографии*. Применение систем и средств криптографии требует их унификации и стандартизации. Данная проблема актуальна как на национальном уровне взаимодействия, так и международном. Концепция криптографии изложена в таких документах, как:**

- стандарт ISO/IEC 7498 «Базовая эталонная модель взаимодействия открытых систем. Часть 2. Архитектура безопасности», принятый в 1989 г. Международной организацией по стандартизации IOS (International Organization for Standart);
- стандарт «Рекомендации X.800: Архитектура безопасности, принятый IOS для применения в МККТТ», принятом в 1991 г. Международным консультативным комитетом по телеграфии и телефонии МККТТ.

Одними из наиболее известных стандартов шифрования данных являются системы DES и RSA, разработанные в США. Алгоритм системы DES является симметричным. Алгоритм RSA – асимметричный. Этот алгоритм (RSA) используется в программе PGP – Pretty Good Privacy, широко используемой для шифрования данных в INTERNET. Эта программа обеспечивает не только взаимодействие открытого и секретного ключей, но и их взаимозаменяемость. Пользователь может зашифровать что-либо, например подпись, своим секретным ключом, а расшифровать это сообщение смогут только лица, обладающие соответствующим открытым ключом.

Российское законодательство так же, как и законодательство многих других стран, предусматривает наличие собственной национальной системы криптографии, действующей по общепринятой схеме, но основанной на оригинальных алгоритмах. Данная система должна применяться для защиты государственных информационных ресурсов, а также другой конфиденциальной информации. На базе вышеуказанных алгоритмов были разработаны и введены следующие стандарты шифрования:

ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

ГОСТ 34.11-94 «Криптографическая защита информации. Функция кэширования»;

ГОСТ 34.10-94 «Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

В соответствии с этими стандартами был разработан и сертифицирован целый ряд симметричных систем шифрования секретным ключом. В качестве системы с открытым ключом, предназначенной для негосударственных предприятий, сертифицировано средство криптографии под названием «Верба». Данное средство представляет собой комплекс инструментальных средств шифрования, позволяющих их пользователям или группам пользователей создавать собственные системы криптографии.

***Защита программ от несанкционированного использования*. Защищенная программа может находиться в двух состояниях: состоянии хранения и рабочем состоянии.**

В состоянии хранения она может находиться в одном из каталогов винчестера, компакт-диске или на дискете. При подготовка к хранению программа может быть настроена определенным образом для последующей процедуры защиты, в ней может быть выделена специальная область, записана необходимая информация или запрограммированы (внедрены) специальные команды или функции. В таком виде программа может передаваться другим пользователям для инсталляции в их рабочие каталоги.

Процедура тиражирования и перевод программы в рабочее состояние зависят от типа защиты и формы ее распространения.

При отсутствии защиты копирование и последующее использование программы не требуют, естественно, особых усилий.

Защита может быть условной, относительной. Такая программа свободно распространяется и выполняется при каждой новой инсталляции, однако во время работы постоянно напоминает о ее неузаконенном использовании. Лишь тогда, когда пользователь свяжется по указанным координатам с изготовителем и оформит соответствующим образом отношения с ним – зарегистрирует программу, она «успокаивается» (получив требуемый код) и работает, не причиняя хлопот и моральных неудобств.

На западном рынке условно бесплатное предоставление программных продуктов является довольно распространенным. Такие программы можно получить у знакомых, по каналам компьютерных сетей, глобальной коммуникационной системы INTERNET. Однако у пользователей имеется к таким продуктам некий налет пренебрежительности и недоверия, тем более, что такой вид услуг предлагают в основном малоизвестные фирмы и производители. Возможно, кроме того, и получение программы-вандала или «троянского коня» вместо декларированного полезного продукта. В таком случае приобретение бесплатной или условно бесплатной программы может слишком дорого обойтись их пользователю. Поэтому гораздо в большей мере пользователи предпочитают покупать у солидных фирм за солидные суммы, но с гарантией качества и возможностями консультаций и обслуживания.

Жесткая защита программы предполагает выполнение определенных условий для ее функционирования и переноса на другие компьютеры. Такая защита осуществляется различными способами, в частности:

- соответствием установленным параметрам;
- наличием ключевой дискеты или другого устройства;
- привязкой программы к конкретному компьютеру;
- защитой дискет (с программами) от копирования.

При загрузке программы осуществляется проверка заданных условий. При их невыполнении происходит прерывание работы, которое может сопровождаться:

- сообщениями о защите и несоответствии;
- уничтожением программы с диска (возможно, и не только программы);
- перезагрузкой системы.

Тут уже пользователь, проявляя заботу о своих данных, должен быть осторожным в использовании защищенных, а в общем случае, неизвестного происхождения программ.

Распространение программы с так называемым ключевым устройством (дискетой, разъемом или иным) предполагает работу программы на любом компьютере (без указания количества ин-

сталляций и «привязки»), однако, во время работы или ее начале в указанном дисководе должно находиться указанное ключевое устройство. Такой тип распространения не очень удобен, особенно в случае с ключевой дискетой: дисковод может требоваться для других дискет, и пользоваться программой в данный момент может только один пользователь. Вместо дискеты в качестве ключа могут использоваться, например, разъемы для принтера. Конечно, такой ключ более приемлем, но тоже особым удобством не отличается.

Требования соответствия установленным параметрам предполагают запись определенных команд, операций или функций в тело программы при ее подготовке. Заданные параметры могут быть самых различных типов и видов, в частности:

- Ключ или пароль. Программа при загрузке спрашивает пароль и продолжает нормальную работу при правильном ответе.
- Количество выполненных однородных функций. При достижении заданного числа программа может отказать в дальнейшем функционировании.
- Дата загрузки программы для выполнения. При достижении определенной даты программа перестает работать.
- Список имен (фамилий), разрешенных для доступа к программе и работы с ней. Программа просит назвать имя пользователя и продолжает работу при наличии этого имени в соответствующем списке.

Соответствие заданным параметрам может применяться как при распространении программы, так и для защиты ее на своем компьютере от посторонних людей (нарушителей доступа).

Привязка программы предполагает ее настрой на конкретный компьютер, на который она инсталлирована и с которого она не может быть перенесена на другой.

Система распространения может предусматривать инсталляцию программы с дискет или других носителей данных только самим изготовителем либо уполномоченными им лицами. В этом случае программы подготавливаются соответствующим образом и при инсталляции привязываются к компьютеру. При этом защита дискет от копирования не делается или признается нецелесообразной. Неудобство этого способа распространения – в необходимости постоянных поездок (возможно и на большие расстояния) представителей изготовителя. Для потребителей это также не очень удобная и надежная форма приобретения из-за отсутствия у них резервных копий продукта.

Наиболее совершенна форма защиты, при которой делается «привязка» программы и предотвращается ее копирование с дискеты. Такие программы можно распространять в магазине, по почте, из рук в руки. Приобретая продукт с несколькими его инсталляциями, пользователь всегда может рассчитывать на резервные копии и восстановление программы в случае ее потери или уничтожения на жестком диске.

Защита программы с привязкой ее к компьютеру состоит в:

- выделении специальной области в программе и записи в нее определенной информации, достаточно уникальной для данного компьютера и служащей в дальнейшем эталонной;
- внедрении в нее специального кода проверки (подстановка первой команды заставляет программу считывать и сопоставлять информацию из выделенной области программы с текущей).

Если это сопоставление дало положительные результаты, управление передается основной части программы, в противном случае происходит прерывание работы.

Обычно в выделенную защитой область записывается упорядоченная последовательность динамических и/или статистических показателей, идентифицирующих данный компьютер.

Динамические показатели характеризуют свойства функционирования компьютера. Эти показатели (тактовая частота микропроцессора, скорость вращения диска и пр.) достаточно уникальны и относительно постоянны. Однако они могут незначительно колебаться при изменении напряжения или температуры, что может привести при сравнении эталонных и текущих характеристик к неожиданным результатам.

Часто программа «привязывается» к конкретной конфигурации винчестера, к своему физическому расположению на диске. Это не очень удобно для ее использования: нельзя не только, допустим, переформатировать диск, но и передвинуть (в результате дефрагментации, например) программу на другое место – инсталляция сразу же будет признана незаконной. Для преодоления этих трудностей предусматривают реинсталляцию программы с удалением ее с диска и увеличением числа инсталляций на единицу. Это, однако, существенно снижает эффективность защиты: можно запомнить образ диска, реинсталлировать программу, затем восстановить содержимое диска, разумеется, вместе с этой программой.

Статистические показатели содержат паспортные данные об основных блоках, устройствах, каналах, модуле BIOS (тип, дата регистрации, размер оперативной и расширенной памяти, число портов, накопителей и пр.) и также достаточно хорошо идентифицируют компьютер. Их проверка при выполнении программы обеспечивает, возможно, менее качественную (показатели могут оказаться не уникальными), но более надежную в работе привязку к компьютеру.

***Защита дискет от копирования*. Подготовив ключевую дискету или дискету с заданным количеством инсталляций программного продукта, разработчик хочет надеяться, что эта дискета не может быть воспроизведена, размножена, тиражирована. Для этого дискета защищается от копирования. Существует множество способов и форм этой защиты, многие из них хороши и достаточно надежны, хотя стопроцентную гарантию ни одно из них дать не может.**

Защищаемые дискеты должны удовлетворять следующим основным требованиям:

позволять свободное считывание информационных файлов с дискеты, независимо от типа компьютера;

обладать уникальными характеристиками, исключающими воспроизведение, появление двойника;

быть недоступной для операции копирования содержащейся на ней информации.

Для достижения этих целей применяют, в частности, следующие методы:

- использование нестандартного (отличного от обычного, системного) формата дискеты;
- пропуск дорожки при форматировании: программа копирования встречает неформатированную дорожку и прекращает операцию;
- введение дополнительных секторов, невоспроизводимых стандартными средствами копирования (DiskCopy);
- создание псевдосбойных секторов (с несовпадением контрольных сумм): ошибка не мешает читать данные, но не позволяет осуществить копирование;
- механическое повреждение диска (острым предметом, лазерным лучом) с последующем форматированием его; метод считается надежным, хотя вряд ли является очень удобным.

Существенным недостатком большинства этих методов защиты, а также их конкретных реализаций является то, что они рассчитаны на стандартные средства копирования (вернее, на противодействие им) типа DiskCopy. Однако в настоящее время разработано и выпущено в свет множество других более совершенных программ и утилит, осуществляющих копирование дисков. Эти средства анализируют (Copy II PC, CopyMaster) все дисковое пространство, выполняют побитовое копирование (Disk Explorer) и полностью воспроизводят дискету.

***Программная защита данных при их передаче*. Передача данных по линиям сети, в особенности, на большие расстояния требует принятия дополнительных мер безопасности, в том числе, на уровне разработчиков систем, специалистов по созданию систем коммуникации и удаленной связи.**

Защита данных при их передаче представляется в двух основных аспектах: 1) защита достоверности данных; 2) защита данных от перехвата и нелегального использования.

Защита достоверности данных особенно актуальна при передаче документов по линиям электронной почты. Имеется в виду сохранение юридической значимости документа, предотвращение подделок, появления фиктивных документов. Современная электронная почта предполагает передачу документов посредством факс-модемов через графический интерфейс. Эти средства позволяют передавать и воспроизводить подпись, печать и другие идентифицирующие признаки передающего юридического лица.

По российскому законодательству электронная подпись признается действительной и юридически значимой, разумеется, при наличии специальных программно-технических средств, обеспечивающих идентификацию подписи. На право удостоверять идентичность электронной цифровой подписи требуется лицензия, выдаваемая уполномоченными на это органами.

Для защиты данных сети от несанкционированного использования применяются следующие меры и средства:

- организация доступа и разграничение полномочий;
- криптография, шифрование документов;

- разделение массива передаваемых данных таким образом, что из отдельных частей невозможно понять их смысл и значение, и передача их по двум или более параллельным каналам, линиям связи, станциям, последующее затем слияние фрагментов;
- процедура сжатия и/или шифрования данных при передаче и восстановления исходного вида после приема

Особые проблемы информационной безопасности возникают при использовании таких глобальных информационных магистралей, как INTERNET. Такие сети поддерживают связь с огромным множеством локальных и корпоративных сетей, осуществляют передачу данных по многим каналам, маршрутам и различным протоколам. Здесь необходимо разграничение доступа к различным наборам данных и защита конфиденциальной информации. Однако проконтролировать все системы связи, обеспечить их безопасность и защиту практически невозможно. Многие владельцы информации, потратившие миллионы долларов на защиту информации своих серверов, с ужасом наблюдают, как эта защита обходится, взламывается или рушится прямо у них на глазах. Так называемые брандмауэры, предназначенные для защиты узлов сети (WEB-узлов в INTERNET), нередко сами становятся уязвимыми и легко преодолимыми.

Для обеспечения информации серверов и хост-серверов ее владельцы идут на «ответные меры». Так, сегодня многие WEB-серверы способны собирать информацию о своих пользователях, определяя и запоминая их адреса, фамилии и другие личные реквизиты, в особенности при повторяющихся обращениях к информации определенной тематики или каталога. Это, со своей стороны, вызывает протест пользователей INTERNET, как попытка нарушения частных прав клиентов.

***Программная защита интеллектуальной собственности*. Защита интеллектуальной собственности заключается в защите прав собственников и других держателей информации, авторских и имущественных прав. Программная защита этих прав должна рассматриваться как поддержка их правовой защиты (посредством документирования и официального оформления) и быть направлена на следующее:**

- на защиту информации от несанкционированного использования;
- на использование информации с соблюдением прав собственности.

Первый пункт заключается в ограничении доступа к информации в соответствии с ее конфиденциальностью и коммерческой ценностью, т.е. выражается в предотвращении несанкционированного доступа к ней. Однако имеется множество типов информационных объектов и их физических представлений, предусматривающих относительно свободное использование и потому открытых для доступа. Это и печатные издания, и машинные носители данных, и сетевые информационные фонды. Поэтому не менее, а возможно, и более важен второй пункт этой защиты.

Правовое оформление интеллектуальной собственности юридически обязывает пользователей уважать права ее авторов и собственников. Ее программная защита призвана принудительно заставить возможных нарушителей соблюдать эти права.

Пользователь может на законных основаниях получить доступ к печатному изданию или стать владельцем информационной продукции, приобретая тем самым право на использование их в личных или служебных целях и на получение производной информации. Но он не имеет права на плагиат и распространение (продажу) пиратских копий.

Особенно актуальными эти проблемы становятся для сетевого обмена информацией и в особенности для глобальных сетей типа INTERNET. Размещение информации в открытых для доступа ресурсах INTERNET означает возможность ее копирования и соответствующего использования. Но во многих случаях происходит присвоение интеллектуальной собственности с дальнейшим использованием в качестве собственного продукта. Ограничение доступа к информации INTERNET противоречит ее статусу открытой сети, но по свидетельству специалистов это воровство уже приобрело угрожающие размеры.

Защита условно свободно распространяемых программ осуществляется вставкой текстового фрагмента, постоянно напоминающего о необходимости регистрации. Для защиты информационных ресурсов можно применять специальные реквизиты, товарные знаки, логотипы и пр. Однако нарушитель может их и убрать из текста.

В качестве более действенной защиты текстовой, графической и мультимедийной информации предлагается так называемое электронное тавро, или своего рода система цифровых водяных знаков –

CIPRESS. Вставка электронного тавро заключается во вкраплении в текст «невидимых» битов, убрать которые можно только вместе с самим текстом.

***Защита целостности и точности данных*. Защита целостности данных понимается как система мер, предпринимаемых против несанкционированного и/или непредусмотренного (задачами обработки) изменения информации. Данные изменения могут быть:**

- произведены в результате неправильных (случайных) действий владельцев или пользователей данных в ходе информационных процессов;
- вызваны действиями нарушителей доступа, последствиями преднамеренного хулиганства и вредительства;
- получены в результате сбоев в работе автоматизированных систем.

Защита целостности данных производится на уровне всех форм защиты и, в первую очередь, на уровне физической и программной, в частности, с помощью следующих средств и процедур:

- средствами антивирусологии;
- восстановлением данных;
- систем архивации и хранения данных;
- организацией системы доступа, исключающей нарушения;
- организацией системы пользования данными и их обработки с минимальным риском непредсказуемых последствий;
- созданием распределенных дисковых систем;
- защитой точности данных.

Защита целостности данных должна также предусматривать проведение периодического или по мере надобности тестирования данных (информационных ресурсов, программного обеспечения) на неизменность их состояния. Тестирование может производиться специальными или стандартными (преимущественно) средствами.

Одной из задач защиты целостности является защита точности данных, состоящая из следующих подзадач:

- защиты точности связей, понимаемой как поддержание установленного соответствия между различными частями данных;
- защиты точности коммуникации, понимаемой как сохранение состояния данных при передаче между различными процессами и каналами связи.

***Создание распределенной дисковой системы*. При функционировании распределенных систем данных с большим числом пользователей выявляется неравномерность в обращении к различным блокам данных и участкам дискового пространства – к одним чаще, к другим реже. Причем, источники этой неравномерности также непостоянны (время обращения, решаемые задачи, количество пользователей и т.д.), и определенную закономерность частоты обращений к данным невозможно установить. Образование так называемых «горячих пятен» на диске (с более частым обращением к ним) влечет их ускоренный износ и потерю информации, а с другой стороны, приводит к большим задержкам выдачи соответствующих блоков данных и снижению производительности системы. Одним из способов решения данной проблемы является создание распределенных дисковых систем с определенной избыточностью хранения данных. Стандартом подобной дисковой системы считается RAID -Redundant Arrays of Inexpensive Disks, основные направления которой были сформированы в 1987 г. в Калифорнийском университете. Для обеспечения системы записи и хранения данных в корпоративной среде используется группа из двух и более дисков, информация между которыми распределяется в соответствии с некоторым алгоритмом. В зависимости от выбранного алгоритма (простое распределение массивов, использование зеркальных дисков, формирование областей с избыточным хранением данных и пр.) различают несколько уровней RAID (от RAID 0 до RAID 7). Достигаемая здесь избыточность при хранении массивов данных позволяет увеличить ее надежность (за счет дублирования), а также разгрузить «горячие пятна» за счет переадресации данных на их дублеров и другие диски. С точки зрения защиты данных, система RAID 0 наименее надежна (хотя и максимально производительна), так как здесь осуществляется простое распределение блоков данных по различным дискам без резервирования и дублирования, а также без вычисления контрольных сумм и записи кодов исправления ошибок. При вы-**

ходе из строя одного из дисков информация теряется. При использовании системы RAID 1 с зеркальной записью данных на два диска достигается максимальная надежность хранения (при большом снижении производительности), поскольку данные с поврежденного диска всегда можно скопировать с дубликата. Пожалуй, наиболее предпочтительной и популярной является дисковая система RAID 5. В этой системе каждый блок данных записывается на один из дисков – каждый последующий блок на альтернативном предыдущему диске, а его контрольные суммы, вычисляемые по методу Exclusive OR, заносятся на другой диск. При выходе из строя одного из дисков или его отдельных участков информация с них восстанавливается с помощью других дисков и соответствующих контрольных сумм. При достаточно большом количестве используемых дисков данная система показывает высокую производительность и эффективность при сравнительно низкой себестоимости, а также высокую степень защищенности данных.

Возможно, технологией будущего является система RAID 7, разработанная американской фирмой Storage Computer Corporation и выполненная на принципиально новом асинхронном принципе доступа.

***Программное восстановление данных*. Защита данных заключается не только в ограждении их от актов пиратства, хулиганства или несанкционированного доступа. Не менее важной задачей является защита полноты и достоверности информации. При потере или искажении части информационного потока при его хранении на материальном носителе или при передаче невозможны достоверное исследование статистических данных и оперативная обработка блоков информации. Помимо усилий по модернизации и замене физически и морально устаревшей техники, необходимо следующее:**

- отлаженная система оценки количества и качества принятых к обработке данных;
- система оперативной связи с источником коммуникации для замены или повторной передачи данных;
- средства восстановления данных.

Под программным восстановлением массивов данных понимается приведение их отдельных компонентов (чисел, символов, блоков) к значениям, выражающим первоначальные значения или смысл с определенной степенью точности и достоверности. В результате сбоя в обработке, в ее алгоритме, при коммуникации данных часть значений данных может исказиться, что приведет к неверным результатам и заключениям при их обработке. Задача программного восстановления состоит в том, чтобы по контексту, окрестности утерянных / искаженных данных определить их относительно верное значение.

К этому типу относятся и задачи очистки программ и прочих файлов от всевозможных наслоений, паразитических элементов, кодов, символов. Борьба с этими проявлениями ведется путем защиты целостности и неприкосновенности файлов (проверки объемов, подсчета контрольных сумм), обнаружения и удаления внедрившихся и/или внедренных в них дополнений. К этому типу относится и создание средств антивирусологии, борьба с вирусами и другими программами-вандалами.

5 ФИЗИКО-ТЕХНИЧЕСКАЯ ЗАЩИТА ДАННЫХ

5.1 СТРУКТУРА ФИЗИКО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

Физико-техническая (физическая) защита данных – это комплекс таких производственных профилактических мероприятий по сохранению информации и средств, предназначенных для хранения и передачи данных. Эти мероприятия не связаны непосредственно с процессами программирования, компьютерной обработки и коммуникации, относятся, в основном, к функциям технико-операторского обслуживания и профилактики, осуществляемым на уровне пользователей и специальных групп людей.

К защищаемым физической формой защиты средствам следует отнести все технические устройства, применяемые для защиты данных, а также системные и стандартные программные средства, используемые для увеличения надежности хранения данных.

Надежность хранения данных – это исключение любой возможности потери данных, в том числе случайной, умышленной или непредвиденной, обеспечение разрешенного доступа и конфиденциальности информации. Физическая защита данных обязана предусматривать и предот-

вращать все объективные, природные и субъективные факторы, влияющие на систему хранения. Система должна быть оснащена всеми необходимыми средствами физического хранения данных и средствами их ограждения от недобросовестного обращения с ними, злоупотреблений и пр.

Сфера действия физико-технической формы защиты информации распространяется на ее физическое представление в компьютерных системах, т.е. на данные, поэтому данная форма и является защитой данных. Подлежащие защите данные имеют определенную организацию, сформированы в виде неких информационных объектов (файлов, модулей и т.д.), содержатся в памяти компьютера или других материальных (машинных) носителях. Поэтому физико-техническая защита данных является системой двух взаимосвязанных составляющих: 1) защиты самих данных (физической защиты); 2) защиты аппаратуры (технической защиты).

По методике функционирования физико-техническая защита бывает двух типов:

- осуществляемая внутри сферы информационных процессов и выражаемая действиями по реализации данных процессов или непосредственным продолжением этих действий (копированием, архивированием, профилактикой и т.д.);
- осуществляемая вне сферы информационных процессов (охрана, установка дополнительного оборудования и т.д.).

Назначение и цели физико-технической (физической) системы защиты определяются ее формой и выражаются во множествах ее составляющих задач (защите самих данных и защите их материальных носителей) и типов (защита внутри и вне информационных процессов).

Физическая защита данных обязана обеспечивать:

- надежность и безопасность средств обработки данных;
- надежность и достаточность технических средств для хранения и передачи данных, в том числе, на большие расстояния;
- надежность физических и технических систем хранения, обработки и коммутирования данных, исключающую потерю их целостности, полноты и достоверности;
- аппаратную защиту данных от несанкционированного доступа к ней, использования, перехвата при коммуникации;
- защиту данных от стихийных бедствий, пожаров и прочих аварийных ситуаций.

В физическую систему хранения и защиты входят:

- все информационные ресурсы компьютерной системы;
- используемые программные средства хранения и защиты данных;
- архивы данных и система архивации;
- система антивирусологии.

В техническую систему хранения и защиты входят:

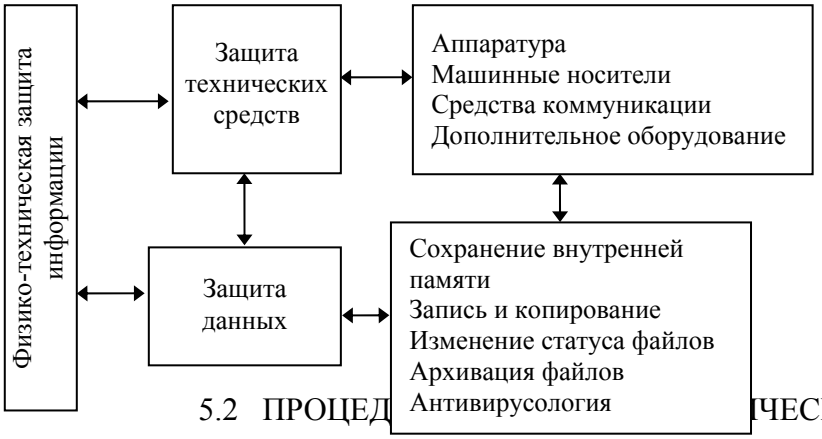
- машинные носители данных;
- техническое обеспечение компьютерных систем;
- технические средства коммуникации данных;
- дополнительное оборудование, средства размещения и хранения аппаратуры.

Физическая защита данных выражается в повседневной, часто рутинной работе по их физическому сохранению с применением средств физической и технической систем хранения, а также необходимых системных или прикладных программных средств. В этом выражается связь физической защиты с административной и программной формами защиты информации и ее зависимость от них. Физическая защита требует определенной организации и планирования; технология физической защиты формируется программной защитой.

Защита информации при ее обработке средствами вычислительной техники, безусловно, должна начинаться с выбора этой техники. Вся аппаратура должна не только соответствовать решаемым задачам с полным учетом необходимых им ресурсов, установленным стандартам и требованиям безопасности, но и требуемым показателям качества, надежности и устойчивости.

Все технические устройства и приборы должны иметь сертификаты относительно электрической и электромагнитной безопасности.

Схема физико-технической защиты данных представлена ниже.



5.2 ПРОЦЕД ЧЕСКОЙ ЗАЩИТЫ ДАННЫХ

***Защита машинных носителей данных*. Машинные носители данных – винчестеры, дискеты, бумага и пр. Надежность хранения предусматривает:**

- выбор носителей с достаточно большим объемом памяти и обладающих хорошим качеством: записав данные на ненадежную или непроверенную дискету можно не считать их с нее, возможно, лишившись вообще;
- обеспечение надежности и качества хранения носителей данных: необходимо содержать их в местах, исключающих возможности физического воздействия на них, физической порчи, а также достаточно недоступных для злоупотреблений и несанкционированного доступа (в сейфах, коробках и т.д.).

Дискеты с течением времени могут портиться, размагничиваться, что привести к потере хранящейся на них информации. Для повышения гарантии сохранения данных необходимо разумное дублирование их носителей, а также их периодическая или по мере необходимости проверка, тестирование и замена.

Жесткий диск также нуждается в защите от повреждений (ударов во время работы). Для жесткого диска характерен еще и моральный износ. Появляются все новые диски с более надежной и большой мощностью памяти. Замена устаревшего диска (после двух-трех лет работы) повысит и надежность хранения (как на более новом), и возможности оперативного и архивного сохранения данных.

Защита носителей информации предполагает также их достаточно хорошо организованное хранение: строгий учет, систематизацию и идентификацию, удобное обращение и предотвращение несанкционированного доступа, а также меры по безопасности их хранения.

В настоящее время имеется довольно надежное средство сохранения информации жесткого диска с помощью стриммера – специальной постоянной кассеты с цифровой записью информации и объемом памяти до 30 Гб либо набора сменных картриджей емкостью от 100 Мб до 1 Гб. Стриммер замечателен тем, что на него в достаточно оперативном режиме можно сбросить содержимое всего жесткого диска и восстановить его в случае аварии или другой надобности.

***Защита технического обеспечения компьютерных* систем К техническому обеспечению компьютерных систем относятся системный блок (процессор), периферия, оргтехника. Работа на аппаратуре, не удовлетворяющей необходимым требованиям безопасности и качества, может привести к аварийной ситуации, непредсказуемым последствиям, искажению или потере информации. Надежность технического обеспечения предусматривает также необходимое дублирование устройств и блоков на случай непредвиденного сбоя одного из них.**

Защита оборудования компьютерной системы как средства хранения и обработки данных (процессора, винчестера и др.) заключается в:

- защите от злоупотреблений с ним, разрушений, хищений и пр. (в том числе помещений);
- защите от несанкционированного доступа к ним, вернее, к их функциональным блокам: использование специальных встроенных плат, системных средств, блокирование устройств специальными ключами и т.д.;
- соблюдении требований безопасности работ на компьютере и правил его использования;

- предотвращении и устранении аварийных ситуаций: организация технической поддержки, своевременного и квалифицированного ремонта аппаратуры, обслуживания и т.д.;
- в соответствующем техническом обслуживании и систематическом проведении профилактических работ;
- модернизации и обновлении оборудования, замене морально и физически устаревших блоков компьютерных систем на новые и более совершенные, мощные и производительные.

***Выбор и защита средств коммуникации*. Надежность и безопасность средств коммуникации зависят от их выбора и системы функционирования.**

К средствам коммуникации и сетевого обмена информацией относятся аппаратура, устройства и приборы, используемые для удаленной передачи данных: сетевые адаптеры, коммутаторы, модемы, факс-модемы, сотовые телефоны, линии передач и пр.

Выбор модема, факс-модема зависит как от его качества (функционирования, изготовления), так и его параметров, режимов работы. Так, при скорости передачи выше 28 000 битов в секунду (максимальной скорости передачи по телефонным линиям) качество передачи снижается, что может привести к потере информации.

Выбор линий передачи данных в компьютерной сети зависит от ряда факторов и в том числе:

- важности передаваемой информации и уровня ее секретности;
- необходимой степени надежности ее коммуникации;
- качества и надежности этой линии.

Обычные рабочие данные можно передавать по телефонным линиям, для более важной, строго конфиденциальный или содержащей государственную тайну, могут потребоваться выделенные каналы и линии связи. Качество передачи можно повысить за счет использования волоконно-оптических проводов или беспроводной передачи.

При соединении компьютеров локальной сети внутри одного помещения, здания, комплекса зданий требуется соблюдение необходимых требований: стандартов, безопасности, заземления и пр. Соединительный кабель (медный, волоконно-оптический) должен быть в защищенной оболочке и желательно в специальных коробках.

***Дополнительные технические средства защиты данных*. Для надежности компьютерной системы, локальной или глобальной сети, системы информатизации необходимы дополнительные устройства и приборы для обеспечения:**

- защиты компьютерных систем от несанкционированного доступа, целостности системы данных, памяти и файлов;
- защиты от естественного или умышленно посылаемого излучения в целях искажения или уничтожения данных при их обработке и коммуникации;
- предотвращения попыток перехвата данных при их передаче, разрушения системы связи или системы доступа к данным.

Эта аппаратура используется как дополнение к основной компьютерной технике, повышающей степень ее сохранности и надежности функционирования. К этому типу оборудования следует также отнести:

- здания, помещения, где размещается вычислительная техника, средства ее охраны, сигнализации и пр.;
- средства хранения, транспортировки носителей информации;
- сейфы, шкафы, склады, контейнеры и пр.;
- оборудование для создания оптимального режима работы техники и персонала: кондиционеры, приборы и средства освещения, профилактики, уборки помещений и пр.;
- оборудование для обеспечения безопасности вычислительных работ и хранения данных.

Конечно, вопросы приобретения и организации работы вычислительной техники и дополнительного оборудования находятся в ведении административной защиты информации. Однако большинство вопросов по практическому применению этих средств в целях защиты данных относится к физической защите. По существу, речь в данном случае идет о защите материальной собственности с помощью физических (материальных) средств.

Одним из средств защиты данных может служить защитный фильтр для экрана монитора. Выполняя свои прямые обязанности по защите пользователя компьютера от электромагнитных и других вредных излучений, фильтр способен скрывать информацию экрана от посторонних глаз (подглядывание в чужие экраны также может служить источником несанкционированного доступа). Изображение хорошо видно близко сидящему человеку, но недоступно человеку, находящемуся в удалении или под другим углом к экрану.

Используемое программное обеспечение. **Хранение данных на внешних носителях данных неминуемо должно предполагать работу с различным программным обеспечением – системным и прикладным, общим и личным. В этой работе могут выполняться следующие функции и процедуры:**

- сохранение внутренней памяти;
- защита операционной системы и программ;
- записи и копирования;
- изменение состояния, статуса файлов и дисков;
- восстановление данных;
- архивация данных и работа с архивами;
- антивирусология.

Выполнение этих функций и процедур относится в определенной степени к программной защите файлов. Однако в отличие от прочего программного обеспечения защиты данных, эти программные средства носят, во-первых, универсальный характер (независимы от конкретных данных) и предназначены для массового применения, а во-вторых, они используются в рамках профилактики системы хранения данных. Профилактические работы должны проводиться в следующем порядке:

- постоянно, регулярно, периодически – в зависимости от вида ее процедур;
- в автономном режиме – в виде выполнения соответствующих заданий;
- в автоматизированном режиме – в виде выполнения определенных процедур и функций прикладных программ.

Автоматизация запуска программ профилактики системы данных персонального компьютера может быть организована также посредством включения соответствующих операторов в командные файлы, в том числе, системные (AUTOEXEC. EXE) или рабочие файлы операционной системы или управляющей оболочки (NORTON, WINDOWS и пр.).

Профилактические работы по защите данных. **Профилактика на уровне физической защиты данных заключается в текущих мероприятиях пользователя по сохранению нужной ему информации, обеспечению нормального функционирования операционной системы, системы хранения, поиска и передачи данных.**

Сохранение операционной системы заключается в следующем.

Необходимо особо бережное отношение к ресурсам системы: загрузочным модулям, драйверам, системным библиотекам, а также к таблицам конфигурации системы. Загрузочные модули нельзя произвольно менять или переписывать в другое место на диске. Необходимо иметь резервную копию операционной системы на дискете для аварийной загрузки в случае невозможности загрузиться с винчестера, а также для ее восстановления на нем. Необходимо также сохранение текущей конфигурации операционной системы.

Защита программ и файлов данных заключается в их резервном копировании, архивировании, операциях восстановления, а также мерах антивирусной защиты. Такие операции необходимо проводить регулярно или обеспечить их автоматическое выполнение.

Рациональное использование ресурсов внешней памяти также требует определенных мер по ее защите. Помимо операций по сохранению данных пользователь должен позаботиться об очистке памяти от всякого рода «мусора» – ненужной, необязательной или устаревшей информации. Многие программы, редакторы текстовых и других файлов могут создавать параллельные файлы, куда заносится предыдущее (до его изменения) состояние основного файла. В WINDOWS используются системы файлов подкачки и автоматического сохранения документов, куда заносится временная информация. При ограниченных ресурсах памяти целесообразно удалять их по окончании работы или время от времени. Кроме того, в файлах подкачки может оказаться конфиденциальная информация без должной ее защиты.

*Сохранение внутренней памяти***.** Сохранение внутренней памяти компьютера производится во время работы с информационными массивами, файлами, блоками данных. Для того, чтобы обрабатываемые данные, корректировки, изменения, дополнения не пропали после работы, необходимо своевременно запомнить их во внешней памяти. Здесь необходимо сочетание двух факторов:

- наличие средств, функций, процедур и пр. в программах обработки данных (редакторах, утилитах, прикладных программах) для организации сохранения текущей информации;
- знаний и усилий пользователя по использованию этих функций.

Для оптимального сохранения информации и внутренней памяти ПК средства обработки могут содержать следующее:

- Вызываемые функции по сохранению данных. Во время работы с файлами данных с помощью текстовых редакторов, других программ надо не забывать периодически сохранять изменения (в результате какого-либо сбоя информация может пропасть).
- Дублирование рабочих файлов. Для предотвращения случайного или экспериментального искажения, разрушения редактируемого файла, программа работает с его копией. В конце работы пользователь может решить сохранять новое состояние файла или нет.
- Сохранение старого состояния файла. Программа копирует «старый» файл в файл с другим расширением, например, bak. При желании можно восстановить прежнее состояние файла или найти и переписать нужный блок данных.
- Автоматизация режима сохранения. Многие редакторы данных (WORD и др.) имеют режимы по автоматическому периодическому сохранению текущих данных. Пользователю необходимо лишь настроить редактор соответствующим образом: задать режим, установить период сохранения.

*Изменение статуса данных***. Хранение данных в файлах и дисках во многом зависит от состояния этих носителей данных, их режимов, назначенных им при их создании, форматировании или во время работы с ними.**

Тип и статус файла (системный, невидимый, чтение/запись, только чтение) зависят от природы, функции файла. Системные файлы имеют статус SYS. Такие файлы «невидимы» для некоторых команд DOS (DIR) и имеют также статус Read-only (R/O) – «только чтение». Обычно пользовательские файлы имеют тип «архивный», и им присваивается статус Read/write, их можно читать и редактировать. Можно, однако, изменить статус файла, присвоив ему Read-only. Такой файл можно только читать, но не изменять. Эту процедуру можно осуществить, используя меню свойства при нажатии на требуемом файле правой клавиши мышки. Разумеется, такая защита относительна: эти файлы можно переписать, удалить. Кроме того, невидимые файлы и каталоги в одной операционной системе могут оказаться вполне видимыми в другой.

Можно менять также режим модификации дискеты – заклеиванием прорези слева (5,25») или передвижением вверх/вниз специального язычка (3,5»). Защищенная дискета не подлежит никаким изменениям, данные с нее можно только читать.

*Копирование данных***.** Копирование данных, файлов, блоков, каталогов, дисков, операционной системы производится для гарантии сохранения информа**ции,** для передачи информации, обмена данными.

Копирование файлов производится либо в автономном режиме в рамках профилактических работ с системой информации, либо в автоматизированном режиме под управлением программ обработки данных.

Командами и утилитами копирования можно не только сделать копию одного файла, но и многих, выделенных с помощью INSERT или по шаблону, либо всех файлов каталога.

Копирование дисков, дискет осуществляется утилитами библиотеки DOS; средствами управляющих оболочек: DISKCOPY, NCDD (Norton Commander), DUPDISK (Norton Utilites); с помощью функциональных средств и графического интерфейса WINDOWS.

Важная информация должна храниться на защищенной эталонной дискете с, возможно, периодическим обновлением.

Операционная система должна тщательно оберегаться. Обязательно надо иметь загрузочную дискету. Конфигурацию системы, ее основные модули можно отобразить на загрузочную дискету (аварийный диск) с помощью утилиты RESCUE из пакета Norton Utilites. Возможен и более надежный способ со-

хранения и операционной системы, и всего содержимого винчестера: сбросить образ диска на стриммер и при необходимости восстановить его.

Копирование файлов и каталогов, дублирование дисков желательно организовать во время или после их обработки прикладными программами. Такая работа осуществляется в автоматизированном режиме, относительно независимо от пользователя. Программа лишь напоминает ему в необходимых случаях поставить дискету для записи в нее данных или их обновления. Для создания этих возможностей надо либо на стадии разработки программ внести в них соответствующие функции и операторы, либо сформировать командный файл с наличием команд копирования.

Для большей гарантии сохранения данных на дискете, ее можно форматировать непосредственно перед записью. Дефектные дорожки будут изъяты из употребления. Со временем дискета размагничивается, поэтому архивы на них надо периодически тестировать и обновлять.

Восстановление данных и носителей данных. **Здесь восстановление данных понимается как совокупность профилактических мер по восстановлению утраченных или испорченных блоков данных, файлов, дисков или их отдельных участков. Имеется в виду не восстановление самой информации в соответствии с ее логическим смыслом и обозначением, а возможности ее достаточно правильно считать с носителя данных, куда она была помещена для хранения, т.е. считать с наименьшими потерями. Это осуществляется различными системными и стандартными прикладными средствами.**

Восстановление блоков файла на сбойном участке диска можно осуществить внешней командой DOS RECOVER. При этом возможна, однако, потеря части данных.

Удаленные файлы обычно не восстанавливаются. В библиотеке NU имеется, однако, утилита UNERASE из пакета NU, с помощью которой это можно сделать. При этом необходимо, чтобы между удалением файлов и их восстановлением дисковое пространство не изменялось. Иначе разрушение файла необратимо.

Наличие в системе WINDOWS 3.* системы файлов подкачки и временных рабочих файлов делает почти невозможным восстановление случайно удаленных файлов: состояние системного и рабочих дисков постоянно меняется. Но уже начиная с операционной системы WINDOWS 95, имеется специальная «корзина» для временного хранения удаленных файлов и каталогов. По горячим следам и даже в течение определенного времени (пока корзина не переполнится) можно вытащить из нее удаленный набор данных и восстановить его первоначальное состояние.

Восстановление операционной системы (модулей, конфигурации) осуществляется с загрузочной дискеты (командой SYS), а лучше с аварийного диска, полученного с помощью RESCUE.

Восстановление участков жесткого диска, дискеты, их нулевых дорожек можно произвести утилитой NDD из пакета Norton Utilites.

Системы архивации данных. Архивы. **Использование внешних носителей памяти предполагает их сменяемость и множественность, а значит, и определенную систематизацию, упорядочение, накапливание. Упорядоченное множество информационных массивов, расположенных на множестве различных носителей данных, образует архивы.**

Архив понимается как организованная система хранения следующих элементов:

- документов и соответствующей ретроспективной информации о них (каталогов, информационных файлов и пр.);
- материальных носителей информации.

Архивы нужны для удобного хранения и/или передачи блоков данных, экономии памяти. Архив информации может быть расположен как на жестком рабочем диске, так и на других носителях: дискетах, магнитных лентах, компакт-дисках и пр.

Выделяются следующие организационные типы архивов.

Государственные центральные или специализированные архивы в виде централизованных информационных центров обладают статусом юридического лица, имеют определенный состав сотрудников,

хранилища и систематизированное множество однородной или разнородной информации, используемой широкой аудиторией для получения производной информации.

Корпоративные архивы, имеющие статус подразделения или управления с соответствующим административным подчинением. В таких архивах сосредотачивается научно-техническая информация определенной тематики на некотором множестве машинных и других материальных носителей информации.

Сетевые архивы, организуемые на центральных или узловых серверах сети, в его дисковых устройствах, базах данных, каталогах и файлах. Организованная определенным образом и наделенная соответствующими параметрами доступа информация сетевого архива передается на рабочие станции сети или поступает с них.

Личные архивы, организуемые на уровне физического лица, отдельного пользователя. Эти архивы сосредоточены на жестком диске персонального компьютера, множестве дискет, упорядоченных и хранимых некоторым образом, возможно, стриммере и других машинных носителях данных.

Поименованные архивы в виде архивных файлов или пакетов. В архивном файле и пакете может быть сосредоточена информация какого-либо раздела данных, объединяющего выделенную группу файлов и каталогов. Архивный файл может храниться на жестком диске, компакт-дисках, дискетах и служить объектом хранения и распространения.

Государственные и корпоративные архивы относятся к интеллектуальным, сетевые, личные и поименованные – к физическим.

В интеллектуальных архивах информация упорядочена по содержанию, в физических – по форме.

При формировании и использовании архива приходится решать задачи:

- выбора системы, структуры и формы записи информации;
- выбора средства представления данных;
- выбора средства хранения, носителя данных;
- идентификации и систематизации объектов хранения;
- обеспечения надежного, доступного и защищенного хранения архива;
- обеспечения простого, удобного и быстрого нахождения данных в архиве, представлениях в исходной форме.

Дискета может содержать архив или часть архива, сформированного для длительного хранения информации, либо содержать файлы, представляющие копии рабочих файлов, отдельных блоков БД, программных модулей. Данные копии могут быть получены в автономном режиме или в процессе работы программно-информационных комплексов. Создание архива предполагает не только идентификацию и классификацию архивных файлов и их носителей, но и рациональное использование памяти. Для достижения этих целей используются специальные архиваторы, сжимающие информацию и представляющую ее в удобной для хранения и восстановления форме.

Архиватор – это одна комплексная программа или совокупность двух (архивирующей и разархивирующей) программ, выполняющих следующее:

- сжатие файла, каталога (всех его файлов), многоуровневого каталога (каталога вместе с его подкаталогами);
- представление сжатой информации в виде одного файла с соответствующим расширением и указанным именем;
- модификацию, дополнение архива новыми файлами или новыми версиями имеющихся;
- восстановление информации в исходном виде в указанном пользователем месте;
- извлечение или удаление из архива указанных файлов (по названию или шаблону);
- предоставление необходимой справочной информации о хранимых в архиве данных.

Наиболее популярные архиваторы (ZIP, Rar) предоставляют возможность задать пароль при формировании архива, что создает его защиту от несанкционированного доступа.

Обычно используемый архиватор создает файл с унифицированным для него (архиватора) расширением. Большинство из них позволяют, кроме того, создать саморазворачивающийся (SFX) архив с расширением EXE.

Классификация архивов данных. **Архивы могут храниться на самом рабочем винчестере или, что предпочтительнее и надежнее, на альтернативных носителях информации – на дискетах, стриммере и пр. По сроку хранения можно выделить:**

- временные архивы, получаемые как множество копий, дубликатов файлов при их обработке и модификации;
- архивы длительного хранения, содержащие множество простых или сжатых файлов и каталогов и периодически пополняемые или обновляемые новыми версиями объектов хранения;
- постоянные архивы, содержащие неподлежащую модификации информацию (эталонные файлы, модули системы, утилиты и пр.).

Дискеты с постоянным архивом и, возможно, с архивом длительного хранения, должны быть защищены от записи.

По характеру хранимой информации и структуре ее организации выделяются такие типы, как:

- рабочие (текущие) архивы, постоянно изменяющиеся по составу и содержанию в соответствии с процессами обработки данных;
- эталонные архивы, которые содержат оригиналы файлов, массивов, блоков данных, содержащихся в операционных, управляющих или информационных системах; такие архивы создаются для исключения потери или искажения данных, для оперативной замены или сравнения недостоверной или сомнительной информации, содержащейся на жестком диске; в соответствии с требованиями обработки данных эталонный архив может периодически изменяться;
- инсталляционные архивы, представляющие библиотеки программ, информационных и рабочих файлов на дискетах, сформированные в соответствии с требованиями инсталляционной программы (также содержащейся в архиве) и ею же переносимые на винчестер; файлы инсталляционного архива могут быть в обычной форме, в сжатом, зашифрованном или другом виде; такой архив обычно предназначен для передачи и распространения;
- дистрибутивные архивы, составляющие особый тип инсталляционных архивов, независимых от жесткого диска: дискета с архивом является системной;
- системные архивы, образуемые при формировании загрузочных дискет, содержащих основные модули, рабочие файлы, драйверы операционной и управляющей систем, а также другую информацию, которая необходима для начала работы на компьютере.

Антивирусология. **Одной из постоянных проблем работы на компьютере является борьба с вирусами и программами-вандалами. Эти программы, «вандалы», «паразиты», «троянские кони» и т.д., резидентные и нерезидентные структуры внедряются в программы и другие файлы пользователя компьютера, магнитные диски и оперативную память, искажают и разрушают информацию, делают средства ЭВМ неработоспособными.**

«Троянские кони» рядятся под полезные программы, а в определенный момент совершают «диверсию». Поэтому в целях защиты информации пользоваться незнакомыми программными средствами надо очень осторожно.

Риск подвергнуться акциям вандализма, диверсии, влекущим потерю или искажение информации или даже прерывание нормального течения всех информационных процессов – это одна из теневых сторон несанкционированного использования программно-информационных продуктов или систем: пользователь не знает с уверенностью, что делает приобретенная нелегальным путем программа, а ее собственник, естественно, не отвечает за последствия, поскольку копия приобреталась не у него.

Бутовые (загрузочные) вирусы поражают начальные дорожки дискет, которые сами затем становятся разносчиками заразы. Поэтому лучше «не забывать» дискету в дисководе.

Для борьбы с вирусами применяются следующие меры и средства.

Аппаратные: специальные платы в процессоре проверяют целостность файлов, чистоту памяти и пр., не дают проникнуть вирусам.

Программные: полифаги, ревизоры, вакцины, сторожа и другие обнаруживают и/или уничтожают вирусы, не дают им проникнуть в память и данные, сигнализируют о нежелательных изменениях.

Соблюдение правил работы с данными, а также проведение профилактических, работ.

Более подробную информацию о вирусах, их природе и классификации, методах и средствах борьбы с ними можно получить в сети Интернет (сайты AVP Касперского, Доктор Веб и др.).

Антивирусная профилактика. **Кроме средств непосредственной антивирусологии существует определенный набор правил, которым желательно следовать в целях защиты от вирусов и программ-вандалов.**

1. Нельзя загружать в ОП программу, не зная всех последствий ее работы. Опасно приобретать программы «контрабандным» путем.
2. Форматировать (тем более с записью системы) дискеты лучше на своей машине.
3. Приобретая где-то программу, перед копированием ее в свой ПК следует всеми доступными средствами убедиться в ее чистоте от вирусов.
4. Дискеты, содержащие информацию, не подлежащую модификации (временно или постоянно), должны быть защищены (заклеены) от записи.
5. Необходимо иметь в одном из каталогов жесткого диска или дискеты копии загрузочных модулей, а также других программ (NORTON, текстовые и табличные редакторы и т.д.), иметь так называемую аварийную дискету. В случае утери или порчи загрузочных модулей можно попытаться заменить их копиями. Копии, разумеется, должны быть эталонными (не участвующими в рабочем процессе и/или находящимися на защищенных дискетах). Загрузочные модули далеко не всегда можно просто поменять на копии, не достаточно опытному пользователю не следует этим заниматься.
6. Надо приобретать новые версии фагов (встать на абонементное обслуживание), регулярно пользоваться ими. Можно команду вызова антивирусной программы поместить в AUTOEXEC.BAT для автоматического ее вызова при загрузке системы.
7. Необходимо, по возможности, автоматизировать запуск антивирусных программ:

- Сгруппировать программы в один каталог, возможно, с подкаталогами.
- Указать программы в расширенной области поиска командой PATH, поместив ее в файл AUTOEXEC.BAT.
- Создать командный файл вызова программ и/или поместить этот вызов в автоматическое меню системной надстройки.

8 Следует иметь копии антивирусных программ на защищенной дискете.

Эти, а также другие профилактические мероприятия, относящиеся к процедурам защиты данных, позволят надеяться на относительную вирусозащищенность персонального компьютера.

СПИСОК ЛИТЕРАТУРЫ

1 Анин Б.Ю. Защита компьютерной информации. СПб.: БХВ – Петербург, 2002. 384 с.

2 Барсуков В.С., Водолазкий В.В. Современные технологии безопасности. М.: Нолидж, 2000. 496 с.

3 Байкова И., Кулагин М. Современные дисковые системы // Открытые системы. 1995. № 3.

4 Беляев В.И. Безопасность в распределенных системах // Открытые системы. 1995. № 3.

5 Веденеев Г.И., Коротенков Ю.Г. Основы взаимодействия с ЮМ РС. М.: Недра. 1996.

6 Вольф М. Электронное тавро защитит // PC WEEK. 1998. № 45.

7 Галатенко В. Информационная безопасность // Открытые системы. 1995. № 5.

8 Гражданский Кодекс Российской Федерации. Ч. 1. № 52-ФЗ. 30.11.1994 // Российская газета. 1994. 8 дек. № 238-239.

9 Информатика для юристов и экономистов: Учебник для вузов / С. В. Симонович и др. СПб.: Питер, 2001. 688 с.

10 Информатика. Математика. Правовая информатика / Т.М. Беляева. М.: МЦУПЛ, 2000. 214 с.

11 Леонтьев В.П. Новейшая энциклопедия персонального компьютера 2002. М.: ОЛМА-ПРЕСС, 2002. 920 с.

12 Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. М.: Горячая линия-Телеком, 2001. 148 с.

13 Симоян Р.Е, Симоян С.Л. Компьютер для юриста: Практ. пособие для начинающих. М.: ФЕНИКС, 1998. 352 с.

14 Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма: Справочное пособие. СПб.: БХВ – Петербург; Арлит, 2002. 496 с.

15 Об информации, информатизации и защите информации: Закон РФ // Российская газета. 1995. 22 февраля.

16 Об участии в международном информационном обмене: Закон РФ. № 85-ФЗ. 04.07.1996 // Российская газета. 1996. 11 июля.

17 Уголовный Кодекс Российской Федерации. № 63-ФЗ. 13.06.96 // СЗ РФ. 1996. 17 июня. № 25. Ст. 2954.

18 Об основах государственной политики в сфере информатизации: Указ Президента РФ. № 170. 20.01.1994 // Российская газета. 1994. 29 января.