**«Место ИБ в системе национальной безопасности страны»**

*Национальная безопасность Российской Федерации* — состояние защищённости личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации.

*Национальная безопасность* включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Информатизация социально-политической, экономической и военной деятельности страны и, как следствие, бурное развитие информационных систем сопровождаются существенным ростом посягательств на информацию как со стороны иностранных государств, так и со стороны преступных элементов и граждан, не имеющих доступа к ней.

Несомненно, в создавшейся обстановке одной из первоочередных задач, стоящих перед правовым государством, является разрешение глубокого противоречия между реально существующим и необходимым уровнем защищенности информационных потребностей личности, общества и самого государства, обеспечение их ИБ.

При этом **под информационной безопасностью (ИБ) личности, общества, государства и современных автоматизированных и телекоммуникационных систем** понимается состояние защищенности информационной среды, соответствующей интересам (потребностям) личности, общества и государства в информационной сфере, при котором обеспечиваются их формирование, использование и возможности развития независимо от наличия внутренних и внешних угроз*.*

Информационная безопасность определяется способностью государства (общества, личности):

– обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы, и информационные потоки для поддержания своей жизнедеятельности, и жизнеспособности, устойчивого функционирования и развития;

– противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;

– вырабатывать личностные и групповые навыки и умения безопасного поведения;

– поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Национальный информационный ресурс является сегодня одним из главных источников экономической и военной мощи государства. Проникая во все сферы деятельности государства, информация приобретает конкретное политическое, материальное и стоимостное выражение. На этом фоне все более актуальный характер приобретают ***вопросы обеспечения ИБ*** Российской Федерации как неотъемлемого элемента национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

В любой стране ИБ придается особое значение. В своем развитии эта задача проходит множество этапов в зависимости от потребностей государства, возможностей, методов и средств добывания сведений (в частности, разведки), правового режима государства и реальных его усилий по обеспечению защиты информации.

Важным этапом становления и совершенствования такой системы в нашей стране явился период 70–80-х гг. С началом 70-х гг. в разведывательной деятельности ведущих стран мира началось широкомасштабное применение технических средств разведки. 80-е гг., ознаменовавшись бурным научно-техническим прогрессом, особенно в военной области, дали новые импульсы в дальнейшем наращивании возможностей технических средств иностранных разведок: до 70 % разведывательной информации добывалось в то время с помощью технических средств.

Сложившаяся обстановка потребовала совершенствования системы мер противоборства иностранным разведкам. Задачей государственной важности и одной из составных частей в общей системе мер по сохранению государственной и служебной тайны стало противодействие техническим разведкам.

К началу 90-х гг. произошли качественные изменения в военно-политической и научно-технической сфере, заставившие во многом пересмотреть государственную политику в области защиты информации в целом.

Во-первых, информационные технологии принципиально изменили объем и важность информации, обращающейся в технических средствах ее передачи и обработки.

Во-вторых, в России отошла в прошлое фактическая государственная монополия на информационные ресурсы, в частности получило конституционное закрепление право гражданина искать, получать и распространять информацию.

В-третьих, прежний административный механизм управления защитой информации стал неэффективен, в то же время необходимость межведомственной координации в этой сфере объективно возросла.

В-четвертых, в связи с усиливающимся включением России в международное разделение труда, укреплением экономических, культурных, гуманитарных контактов с другими государствами многие режимно-ограничительные меры, облегчающие защиту информации, например, система регионов, закрытых для посещения иностранными гражданами, стали неприемлемы.

В сложившихся условиях с учетом рассмотренных угроз ИБ личности, общества и государства важным является рассмотрение проблем и задач обеспечения ИБ, являющейся неотъемлемой составной частью обеспечения национальной безопасности любого государства мирового сообщества на новом этапе своего развития – этапе формирования информационного общества.

Известными характерными признаками такого общества является явная обусловленность экономического, социального, научного и всего развития страны широким внедрением новых информационных технологий, обеспечивающих эффективную информатизацию общества, которая, в свою очередь, обеспечивает информационную безопасность общества, в том числе обеспечивает его качественной информацией, информационными продуктами, услугами и знаниями, являющимися сегодня важнейшим стратегическим ресурсом страны. Информатизация личности, общества – это важнейшее, стратегическое направление деятельности государства, определяющее стабильное и безопасное социально-экономическое и политическое развитие и приоритеты во всех сферах, в том числе в информационной и видах деятельности в мировом сообществе.

Подтверждением этому являются практические шаги ведущих стран мира и России, что подтверждается принятием ими ряда нормативных правовых актов и иных документов:

– 2000 г. – «Окинавская хартия глобального информационного общества» (от имени России подписана Президентом);

– 2000 г. Концепцией национальной безопасности Российской Федерации (утверждена Указом Президента, в ред. от 10.01.2000);

– 2000 г. – Федеральные целевые программы «Развитие единой образовательной информационной среды (2001–2005 годы)», «Электронная Россия»;

– 25 июля 2007 г. – программа «Стратегия развития информационного общества в России» (принята Советом Безопасности Российской Федерации);

– 2002 г. – Федеральная целевая программа «Электронная Россия на 2002–2010 годы» (утверждена Постановлением Правительства России от 28 января 2002 года № 65);

– 2007 г. «Стратегия развития информационного общества в России» (утверждена 25 июля 2007 года Советом Безопасности Российской Федерации) и другие.

Широкое внедрение современных информационных технологий во все области хозяйственной и духовной жизни приводит к возрастанию значения защиты национальной безопасности РФ в информационной сфере.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

*Интересы личности* в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использовании ее в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

*Интересы общества* в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочения демократии, создании правового социального государства, достижении и поддержании общественного согласия.

Интересы государства заключаются в создании условий для гармонического развития российской информационной инфраструктуры, для реализации конституционных прав и свобод граждан в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности; защиты информационных ресурсов государства от несанкционированного доступа; обеспечения безопасности информационных и телекоммуникационных систем России.

Информационная безопасность является самостоятельной составляющей национальной безопасности и оказывает непосредственное влияние на защищенность интересов РФ в других сферах жизни общества.

Национальная безопасность РФ существенным образом зависит от обеспечения информационной безопасности. Развитие технического прогресса цивилизации приведет к дальнейшему возрастанию этой зависимости. В частности, получает все более широкое распространение мнение, что информационный век станет веком информационного оружия и «бесконтактных» войн.

Жизненно важные интересы Российской Федерации в информационной сфере определяются в Концепции национальной безопасности следующим образом:

— обеспечение конституционных гарантий свободы совести, вероисповедания, мысли и слова, массовой информации, литературного, художественного, научного, технического и других видов творчества, преподавания;

— обеспечение конституционных прав граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды, а также прав на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, защиту своей чести и доброго имени;

— укрепление механизмов правового регулирования отношений собственности на информационные ресурсы, другие продукты интеллектуальной деятельности человека, создание условий для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации, а также к сведениям, составляющим государственную тайну;

— развитие и совершенствование инфраструктуры единого информационного пространства РФ, повышение эффективности его использования в интересах прогрессивного общественного развития, консолидации российского общества, духовного возрождения многонационального народа РФ;

— совершенствование системы формирования, сохранения, рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала РФ;

— развитие отечественного производства конкурентоспособных средств и систем информации и связи, расширение участия РФ в международной кооперации производителей этих средств и систем;

— обеспечение государственной поддержки отечественных фундаментальных и прикладных исследований и разработок в сфере информатизации;

— повышение безопасности информационных систем, включая сети связи, и информационных систем федеральных органов государственной власти, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, экологически опасных и экономически важных производств;

— расширение международного сотрудничества РФ в области развития и безопасности использования информационных ресурсов.

Обеспечение жизненно важных интересов РФ в информационной сфере предполагает достижение четырех основных групп целей.

Первой группой целей является соблюдение конституционных прав и свобод граждан в области духовной жизни и информационной деятельности, обеспечение духовного возрождения России. Это, прежде всего, создание и совершенствование государством правовых гарантий свободы совести, вероисповедания, мысли и слова, творчества, условий реализации прав граждан на участие в культурной жизни, свободный поиск, получение, передачу, производство и распространение информации любым законным способом, получение достоверной информации о состоянии окружающей среды.

Второй группой целей является информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для этого необходимо укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан, интенсифицировать формирование открытых государственных информационных ресурсов, повышать эффективность их хозяйственного использования.

Третьей группой целей является необходимость развития отечественной индустрии средств информатизации, телекоммуникации и связи, обеспечение выхода ее продукции на мировые рынки. В современных условиях только на этой основе можно решить проблему создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертой группой целей является обеспечение безопасности информационных и телекоммуникационных систем как развернутых, так и создаваемых на территории России, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Для этого необходимо повысить безопасность информационных систем, включая сети связи, прежде всего, безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами, обеспечить защиту сведений, составляющих государственную тайну.

В Концепции национальной безопасности выделены в качестве важнейших следующие задачи, решаемые в информационной сфере:

— установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

— совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

— разработка соответствующей правовой базы и координация деятельности федеральных органов государственной власти и других органов, решающих задачи обеспечения информационной безопасности;

— развитие отечественной индустрии телекоммуникационных и информационных средств, их приоритетное по сравнению с зарубежными аналогами распространение на внутреннем рынке;

— защита государственного информационного ресурса, прежде всего, в федеральных органах государственной власти и на предприятиях оборонного комплекса.

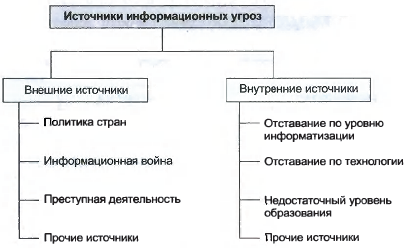
Таким образом, проблема обеспечения информационной безопасности государства стала важнейшей и неотъемлемой частью общей проблемы обеспечения национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач.

Национальная безопасность официально рассматривается в РФ как состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее — граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации[[1]](http://www.eurasian-defence.ru/?q=node/39158" \l "_ftn1" \o ").

Обеспечение национальной безопасности государства (нации) состоит в выполнении двух функций — функции защиты некоего объекта, содержащего важнейшие ценности государства, являющиеся основой жизненно важных интересов личности, общества и государства, а также функции развития этого объекта. Или, употребляя термины Стратегии национальной безопасности — реализуя стратегические национальные приоритеты[[2]](http://www.eurasian-defence.ru/?q=node/39158" \l "_ftn2" \o ").

Существующие в настоящее время представления об объекте национальной безопасности закреплены законодательно: это национальные интересы, объективно значимые потребности личности, общества и государства[[3]](http://www.eurasian-defence.ru/?q=node/39158" \l "_ftn3" \o "). Более подробно совокупность национальных интересов показана на нижеследующем рисунке (

Источниками информационных угроз для человека и общества могут быть внешние и внутренние факторы (рис. 1.1).

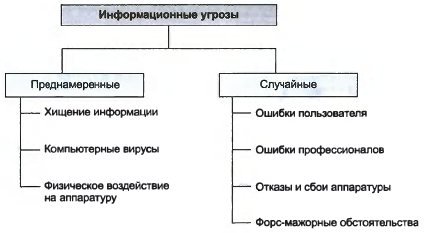


***Рис. 1.1. Источники основных информационных угроз для России***

К источникам основных внешних угроз для России относятся:  
  
♦ политика стран, противодействующая доступу к мировым достижениям в области информационных технологий;  
♦ «информационная война», нарушающая функционирование информационной среды в стране;  
♦ преступная деятельность, направленная против национальных интересов.

К источникам основных внутренних угроз для России относятся:  
  
♦ отставание от ведущих стран мира по уровню информатизации;  
♦ технологическое отставание электронной промышленности в области производства информационной и телекоммуникационной техники;  
♦ снижение уровня образованности граждан, препятствующее работе в информационной среде.

Информационные угрозы безопасности информации можно разделить на преднамеренные (несанкционированный доступ) и случайные (рис. 1.2).



***Рис. 1.2. Основные виды информационных угроз***

Преднамеренные угрозы часто называют несанкционированным доступом, атакой, нападением. Эти угрозы связаны с действиями человека, причинами которых могут быть: самоутверждение своих способностей (хакеры), недовольство своей жизненной ситуацией, материальный интерес, развлечение и т. п. Перечень преднамеренных воздействий на информацию может быть весьма разнообразен и определяется возможностями и фантазией тех, кто собирается их осуществить. Приведем некоторые возможные преднамеренные угрозы, являюиеся типичными для компьютерных систем:  
  
♦ хищение информации: несанкционированный доступ к документам и файлам (просмотр и копирование данных), хищение компьютеров и носителей информации, уничтожение информации;  
♦ распространение компьютерных вирусов;  
♦ физическое воздействие на аппаратуру: внесение изменений в аппаратуру, подключение к каналам связи, порча или уничтожение носителей, преднамеренное воздействие магнитным полем.

Преднамеренные угрозы в компьютерных системах могут осуществляться через каналы доступа к информации:  
  
♦ компьютерное рабочее место служащего;  
♦ компьютерное рабочее место администратора компьютерной системы;  
♦ внешние носители информации (диски, ленты, бумажные носители);  
♦ внешние каналы связи.

Наиболее серьезная угроза исходит от компьютерных вирусов. Каждый день появляется до 300 новых вирусов. Вирусы не признают государственных границ, распространяясь по всему миру за считанные часы. Ущерб от компьютерных вирусов может быть разнообразным, начиная от посторонних надписей, возникающих на экране монитора, и заканчивая хищением и удалением информации, находящейся на зараженном компьютере. Причем это могут быть как системные файлы операционной среды, так и офисные, бухгалтерские и другие документы, представляющие для пользователя определенную ценность. Финансовый ущерб от вирусов в 2003 году, по предварительным оценкам, достиг 12 миллиардов долларов.

Среди вредоносных программ особое место занимают «троянские кони», которые могут быть незаметно для владельца установлены и запущены на его компьютере. Различные варианты «троянских коней» делают возможным просмотр содержимого экрана, перехват вводимых с клавиатуры команд, кражу и изменение паролей и файлов и т. п.



Все чаще причиной информационных «диверсий» называют Интернет. Это связано с расширением спектра услуг и электронных сделок, осуществляемых через Интернет. Все чаще вместе с электронной почтой, бесплатными программами, компьютерными играми приходят и компьютерные вирусы. В 2003 году произошли две глобальные эпидемии, крупнейшие за всю историю Сети. Примечательно, что причиной эпидемий стали не классические почтовые черви, а их сетевые модификации — черви, распространяющиеся в виде сетевых пакетов данных. Они стали лидерами в рейтинге вредоносных программ. Доля «сетевых червей» в общей массе подобных программ, появившихся, например, в 2003 году, превышает 85 %, доля вирусов — 9,84 %, на троянские программы пришлось 4,87 %.

В последнее время среди распространенных компьютерных угроз стали фигурировать сетевые атаки. Атаки злоумышленников имеют целью выведение из строя определенных узлов компьютерной сети. Эти атаки получили название «отказ в обслуживании» («denial of service»). Выведение из строя некоторых узлов сети даже на ограниченное время может привести к очень серьезным последствиям. Например, отказ в обслуживании сервера платежной системы банка приведет к невозможности осуществления платежей и, как следствие, к большим прямым и косвенным финансовым потерям.

Случайные угрозы проявляются в том, что информация в процессе ввода, хранения, обработки, вывода и передачи подвергается различным воздействиям. Случайные факторы, определяющие подобные воздействия, связаны как с непредвиденными ситуациями (форс-мажорные обстоятельства), так и с человеческим фактором (ошибками, халатностью, небрежностью при работе с информацией). Так, например, в компьютерных системах причинами случайных воздействий могут быть:  
  
♦ ошибки пользователя компьютера;  
♦ ошибки профессиональных разработчиков информационных систем: алгоритмические, программные, структурные;  
♦ отказы и сбои аппаратуры, в том числе помехи и искажения сигналов на линиях связи;  
♦ форс-мажорные обстоятельства (авария, пожар, наводнение и другие так называемые воздействия непреодолимой силы).

**Информационная безопасность для различных пользователей компьютерных систем**

Решение проблемы защиты информации во многом определяется теми задачами, которые решает пользователь как специалист в конкретной области. Поясним это на примерах. Определим несколько видов деятельности, например:  
  
♦ решение прикладных задач, где отражается специфика деятельности конкретного пользователя-специалиста;  
♦ решение управленческих задач, что характерно для любой компании;  
♦ оказание информационных услуг в специализированной компании, например информационном центре, библиотеке и т. п.;  
♦ коммерческая деятельность;  
♦ банковская деятельность.

Представим эти области деятельности в виде пирамиды (рис. 1.3). Размер каждого сектора пирамиды отражает степень массовости потребления информации. Он соответствует количеству заинтересованных лиц (потребителей информации), которым потребуется результат соответствующей информационной деятельности. Уменьшение объема сектора по мере продвижения от основания пирамиды к вершине отражает снижение степени значимости информации для компании и всех заинтересованных лиц. Поясним это в процессе рассмотрения каждого из перечисленных видов деятельности.



***Рис. 1.3. Значимость безопасности информации  
для различных специалистов с позиции компании и заинтересованных лиц***

При решении прикладных задач пользователь работает с личной информацией, иногда используя в качестве источника информации ресурсы Интернета. Перед таким пользователем, как правило, стоит задача сохранности его личной информации. Информация, хранящаяся на его персональном компьютере, — это результат его интеллектуальной деятельности, возможно, многолетней, исследовательской или коллекционной. Она имеет существенную степень важности непосредственно для данного пользователя.



При решении управленческих задач важную роль играют информационные системы, реализация которых немыслима без компьютерной базы. При помощи компьютеров осуществляется организационно-распорядительная деятельность, составляется и хранится информация по кадрам, ведется бухгалтерия. Компьютеры в данном случае являются вспомогательным средством, облегчающим работу сотрудников. Для внешней деятельности также используются сетевые технологии, с помощью которых осуществляется обмен необходимой информацией. При этом для обеспечения защиты информации в наиболее важных документах при пересылке пользуются дополнительно обычной почтой. Проблема потери или искажения информации часто касается отдельных сотрудников, что может повлиять на успешность их карьеры. Таким образом, перед управленческими кадрами в такой компании стоит в основном задача обеспечения полноты управленческих документов.



Для компаний, занимающихся оказанием информационных услуг, например провайдеров интернет-услуг или операторов связи, наиважнейшей является задача обеспечения доступности и безотказной работы информационных систем. От этого зависит рейтинг компании, доверие к ней абонентов. Приходится вкладывать средства как в аппаратуру (для обеспечения бесперебойности и устойчивости связи), так и в системы резервного копирования и средства обнаружения атак, нарушающих доступность систем.

Для коммерческой деятельности компаний, работающих в условиях жесткой конкуренции, важнейшей является задача предотвращения утечки информации, сохранение ее конфиденциальности. Это связано с финансовыми рисками компаний в различных сделках. Здесь экономия средств, выделенных на обеспечение безопасности, может привести к большим потерям.



В банковской деятельности приходится решать задачи и сохранности, и конфиденциальности, и безопасности работы, но на первое место встает задача обеспечения целостности информации (например, чтобы было невозможно внести несанкционированные изменения в обрабатываемые платежные поручения).

**Методы защиты информации**

При разработке методов защиты информации в информационной среде следует учесть следующие важные факторы и условия:  
  
♦ расширение областей использования компьютеров и увеличение темпа роста компьютерного парка (то есть проблема защиты информации должна решаться на уровне технических средств);  
♦ высокая степень концентрации информации в центрах ее обработки и, как следствие, появление централизованных баз данных, предназначенных для коллективного пользования;  
♦ расширение доступа пользователя к мировым информационным ресурсам (современные системы обработки данных могут обслуживать неограниченное число абонентов, удаленных на сотни и тысячи километров);  
♦ усложнение программного обеспечения вычислительного процесса на компьютере.

При таких режимах работы в памяти компьютера одновременно могут находиться программы и массивы данных различных пользователей, что делает актуальным сохранение информации от нежелательных воздействий, ее физическую защиту.

К традиционным методам защиты от преднамеренных информационных угроз относятся: ограничение доступа к информации, шифрование (криптография) информации, контроль доступа к аппаратуре, законодательные меры. Рассмотрим эти методы.



Ограничение доступа к информации осуществляется на двух уровнях:  
  
♦ на уровне среды обитания человека, то есть путем создания искусственной преграды вокруг объекта защиты: выдачи допущенным лицам специальных пропусков, установки охранной сигнализации или системы видеонаблюдения;   
♦ на уровне защиты компьютерных систем, например, с помощью разделения информации, циркулирующей в компьютерной системе, на части и организации доступа к ней лиц в соответствии с их функциональными обязанностями. При защите на программном уровне каждый пользователь имеет пароль, позволяющий ему иметь доступ только к той информации, к которой он допущен.

Шифрование (криптография) информации заключается в преобразовании (кодировании) слов, букв, слогов, цифр с помощью специальных алгоритмов. Для ознакомления с шифрованной информацией нужен обратный процесс — декодирование. Шифрование обеспечивает существенное повышение безопасности передачи данных в сети, а также данных, хранящихся на удаленных устройствах.



Контроль доступа к аппаратуре означает, что вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры. Подобные меры позволяют избежать, например, подключения посторонних устройств, изменения режимов работы компьютерной системы, загрузки посторонних программ и т. п.

Законодательные меры заключаются в исполнении существующих в стране законов, постановлений, инструкций, регулирующих юридическую ответственность должностных лиц — пользователей и обслуживающего персонала за утечку, потерю или модификацию доверенной им информации.

При выборе методов защиты информации для конкретной компьютерной сети необходим тщательный анализ всех возможных способов несанкционированного доступа к информации. По результатам анализа проводится планирование мер, обеспечивающих необходимую защиту, то есть осуществляется разработка политики безопасности.

image***Политика безопасности — это совокупность технических, программных и организационных мер, направленных на защиту информации в компьютерной сети.***

Рассмотрим некоторые методы защиты компьютерных систем от преднамеренных информационных угроз, ориентируясь на схему, представленную на рис. 1.2.

Защита от хищения информации обычно осуществляется с помощью специальных программных средств. Несанкционированное копирование и распространение программ и ценной компьютерной информации является кражей интеллектуальной собственности. Защищаемые программы подвергаются предварительной обработке, приводящей исполняемый код программы в состояние, препятствующее его выполнению на «чужих» компьютерах (шифрование файлов, вставка парольной защиты, проверка компьютера по его уникальным характеристикам и т. п.). Другой пример защиты: для предотвращения несанкционированного доступа к информации в локальной сети вводят систему разграничения доступа как на аппаратном, так и на программном уровнях. В качестве аппаратного средства разграничения доступа может использоваться электронный ключ, подключаемый, например, в разъем принтера.

Для защиты от компьютерных вирусов применяются «иммуностойкие» программные средства (программы-анализаторы), предусматривающие разграничение доступа, самоконтроль и самовосстановление. Антивирусные средства являются самыми распространенными средствами защиты информации.



В качестве физической защиты компьютерных систем используется специальная аппаратура, позволяющая выявить устройства промышленного шпионажа, исключить запись или ретрансляцию излучений компьютера, а также речевых и других несущих информацию сигналов. Это позволяет предотвратить утечку информативных электромагнитных сигналов за пределы охраняемой территории. Наиболее эффективным средством защиты информации в каналах связи является применение специальных протоколов и криптографии (шифрования).

Для защиты информации от случайных информационных угрозt например, в компьютерных системах, применяются средства повышения надежности аппаратуры:  
  
♦ повышение надежности работы электронных и механических узлов и элементов;  
♦ структурная избыточность — дублирование или утроение элементов, устройств, подсистем;  
♦ функциональный контроль с диагностикой отказов, то есть обнаружение сбоев, неисправностей и программных ошибок и исключение их влияния на процесс обработки информации, а также указание места отказавшего элемента.



С каждым годом количество угроз информационной безопасности компьютерных систем и способов их peaлизации постоянно увеличивается. Основными причинами здесь являются недостатки современных информационных технологий и постоянно возрастающая сложность аппаратной части. На преодоление этих причин направлены усилия многочисленных разработчиков программных и аппаратных методов защиты информации в компьютерных системах.

**Контрольные вопросы и задания**

**Задания**

1. Опишите информационную среду для перечисленных объектов и укажите для нее возможные информационные угрозы:  
  
а) школа;  
б) библиотека;  
в) ваша семья;  
г) супермаркет;  
д) кинотеатр;  
е) любая другая среда на ваш выбор.

2. Используя Интернет, напишите реферат и сделайте доклад по методам и средствам защиты информации для некомпьютерной среды обитания человека.

3. Перечислите наиболее важные факторы и условия, которые следует учесть при разработке методов по защите информации в информационной среде. Проиллюстрируйте ваш ответ на конкретном примере информационной среды, предложенной в п. 1.

**Контрольные вопросы**

1. Что такое информационная среда?

2. Как проявляется информационная безопасность:  
  
а) человека;  
б) страны;  
в) компьютера;  
г) локальной сети?

3. Каким объектам следует обеспечить информационную безопасность?

4. Что такое информационная угроза?

5. Какие внешние информационные угрозы следует учесть при разработке мер информационной безопасности в России?

6. Какие внутренние информационные угрозы следует учесть при разработке мер информационной безопасности в России?

7. Какие вы знаете преднамеренные информационные угрозы? Приведите примеры.

8. Какие вы знаете случайные информационные угрозы? Приведите примеры.

9. В чем состоит основная цель информационной безопасности при решении прикладных задач пользователя?

10. В чем состоит основная цель информационной безопасности при решении управленческих задач?

11. В чем состоит основная цель информационной безопасности компании, специализирующейся на оказании информационных услуг?

12. В чем состоит основная цель информационной безопасности в коммерческой деятельности?

13. В чем состоит основная цель информационной безопасности в банковской деятельности?

14. Что такое политика безопасности?

15. Какие методы защиты информации от преднамеренных информационных угроз вы знаете?

16. Какие методы защиты информации от случайных информационных угроз вы знаете?