1.2. Основы и современные проблемы информационной безопасности

Вопросы информационной безопасности стали актуальными одновременно с появлением первых ЭВМ и совершенствовались совместно с развитием технической базы. Рассмотрим кратко эволюцию концепции безопасности и защиты вычислительной техники, программного обеспечения и информации.

Первоначально, в качестве основного объекта защиты, рассматривались только ЭВМ [172,100,147,150,33], вследствие сосредоточения в них значительных информационных и вычислительных ресурсов. Весьма показательной, в данном плане, является монография Б.Дж.Уолкера и Я.Ф.Блейка "Безопасность ЭВМ и организация их защиты" [137], в которой необходимость в непосредственной защите обосновывается развитием коллективных методов доступа пользователей и концентрацией информации в вычислительных центрах коллективного пользования.

Д.Сяо, Д.Керр и С.Мэдник в [135] расширяют концепцию защиты ЭВМ за счет включения правовых вопросов, криптографических преобразований и защиты информации в базах данных.

Совершенствование технологической базы систем обработки информации обеспечило дальнейшее развитие концепции безопасности, в рамках которой стали выделять защиту технических средств, программного обеспечения и информации.

Массовое применение персональных компьютеров и локальных сетей в ряде областей человеческой деятельности, среди которых следует выделить такие, как производственная, административная, технологическая, финансовая, патентная и др., информационное наполнение которых в большей степени не должно быть общедоступной, порождает новые проблемы защиты и определяет возросшую актуальность.

Следует согласиться с точкой зрения А.Д. Урсула [138, с.10 -11], в соответствии с которой информационная безопасность не сводится только к компьютерной. Информационная безопасность объединяет компьютерную безопасность, безопасность информационных систем и процессов в обществе, а также специальную среду для гуманистической ориентации информационных процессов.

Автор [84] определяет безопасность информационной сферы как состояние, которое обеспечивает нормальную жизнедеятельность гражданина, общества, государства.

Но приведенное содержание информационной безопасности нуждается в детализации и углублении. В определении компьютерной безопасности, как системы охраны информации, технических и программных средств от нанесения им ущерба в результате сознательных либо случайных противоправных действий, совершенно не учитываются активы, присущие всем информационным системам. Речь должна идти не только об информации, как основном активе, но и ресурсах и отношениях партнеров. Доступность и стабильность вычислительных и информационных услуг, а также отношения партнерства являются активами системы и должны быть защищены от неверных манипуляций.

Термин "безопасность" определяется как минимизация уязвимости активов системы (ресурсы, информация и отношения партнеров), а "угроза" - как потенциальное нарушение безопасности. С развитием систем обработки данных возрастает значение непреднамеренных (ошибки в управлении) и преднамеренных (несанкционированное получение и манипуляция данными) угроз.

Пользователи персональных ЭВМ и информационных систем во многом осознают актуальность и необходимость защиты информации и ресурсов от несанкционированного доступа и использования. Особую остроту данная проблема приобретает по отношению к коммерческим информационным системам, поскольку информация превращается в

товар, который обменивается и продается. Кроме того, несанкционированный доступ, даже если он является случайным и непреднамеренным, приводит к раскрытию и возможному удалению содержания информации, что нарушает ее целостность, и становится причиной утаивания полученной информации, а также соответствующих услуг и ресурсов.

Таким образом, на сегодняшний день, несмотря на большое количество публикаций и повышенный интерес к данной тематике, остаются непроработанными следующие основные вопросы:

1. Отсутствие единого подхода в определении целей системы обеспечения информационной безопасности АИС.

2. Неоднозначность интерпретирования терминологии.

3. Отсутствие единого подхода к классификации факторов, оказывающих влияние на информационную безопасность с выделением преднамеренных и потенциальных угроз.

4. Отсутствие единого подхода к разработке концепции безопасности.

5. Отсутствие единого подхода к оценке защищенности ресурсов АИС;

6. Отсутствие единого подхода измерения ущерба от реализации программных злоупотреблений;

7. Отуствие единых показателей измерения риска и эффективности системы информационной безопасности.

Рассмотрим существующие подходы к определению таких категорий как информационная безопасность, защита информации, безопасность АИС и других терминов, связанных с данной тематикой.

В посвященных данной проблеме публикациях, термин информационная безопасность трактуется с разной функциональной и смысловой наполненностью. Так, все определения можно объединить в следующие группы: 1. сформулированные с точки зрения информационной безопасности общества и государства; 2.

информационной безопасности объектов управления и АИС как их составной части; 3. безопасности информации и др.

Рассмотрим существующие подходы.

В.А. Копылов в [84] рассматривает *безопасность информационной сферы* и определяет ее состояние, которое обеспечивает нормальную жизнедеятельность гражданина, общества, государства.

Обеспечение *безопасности информации* в АИС представляет собой решение четырех взаимосвязанных задач: обеспечение конфиденциальности информации, защита информации от искажений или модификации, защита информации от уничтожения и исключение “захвата” вычислительных ресурсов в монопольное использование [149].

Защита информации от несанкционированных действий - это комплекс организационно-административных, технических и программных мероприятий, направленных на противодействие посторонним лицам доступа к массивам информации с целью изъятия отдельных сведений, разрушения или искажения хранимых и обрабатываемых данных [97].

Автор [123] подразумевает под *защищенностью системы* способность самостоятельно осуществлять контроль себя и окружающей среды в процессе своего функционирования на предмет выявления и предотвращения ситуаций из некоторого наперед заданного множества ситуаций.

Безопасность информации - степень ее зашишенности от раскрытия содержания, определения самого факта ее передачи (демаскирования), изменения, преднамеренного или непреднамеренного искажения и уничтожения лицами, не имеющими на это право, а также утечки по побочным каналам [142].

Авторы [29] определяют категорию *безопасность информации* как защищенность информации, находящейся в организованных системах,

от дестабилизирующего воздействия внешней среды и внутренних угроз.

Под *безопасностью программного обеспечения* понимают отсутствие в коде программного обеспечения элементов разрушающих программных средств (РПС), т.е. вирусов, закладок, троянских коней и т.д [73].

Безопасность системы обработки данных - это показатель или система показателей, характеризующих уровень защищенности информации при обработке в АСОД [85].

Информационная безопасность - это защита общества от отрицательных последствий информатизации, обеспечение ответственности нарушителей и соблюдение интересов личности, организаций, государства; правопорядок отношений в области информатизации, использования техники и технологий в этой сфере [88].

В работе [45] А.С.Голубков определяет *информационную безопасность* как составную часть проблемы информационного обеспечения человека, государства и общества, ориентированную на защиту информационных ресурсов и, на основе этого, - на защиту их законных интересов во всех сферах деятельности.

Под *защитой информации* понимается совокупность мероприятий, методов и средств, обеспечивающих решение следующих основных задач: проверка целостности информации; исключение несанкционированного доступа к ресурсам ЭВМ и хранящимся в ней программам и данным; исключение несанкционированного использования хранящихся в ЭВМ программ (т.е. защиты программ от копирования) [130].

Защита информации в вычислительных системах означает способы и методы функционирования этих систем в заданых режимах при невозможности как преднамереного, так и случайного раскрытия, изменения и искажения данных.

Защита информации в информационных системах означает сохранение заданного уровня конфиденциальности, целостности и доступности информации в заданном промежутке времени при заданных режимах эксплуатации информационных систем.

Под нарушением конфиденциальности данных принято понимать ознакомление с данными лиц, которые к этим данным не допущены, либо создание предпосылок для доступа к данным неопределенного круга лиц [83]. Нарушения конфиденциальности информации могут быть систематизированы с различных позиций (рис.2).

Под нарушением целостности данных понимать сохранение их [illegible] их защищенность от [illegible] намеренной модификации ил[illegible]

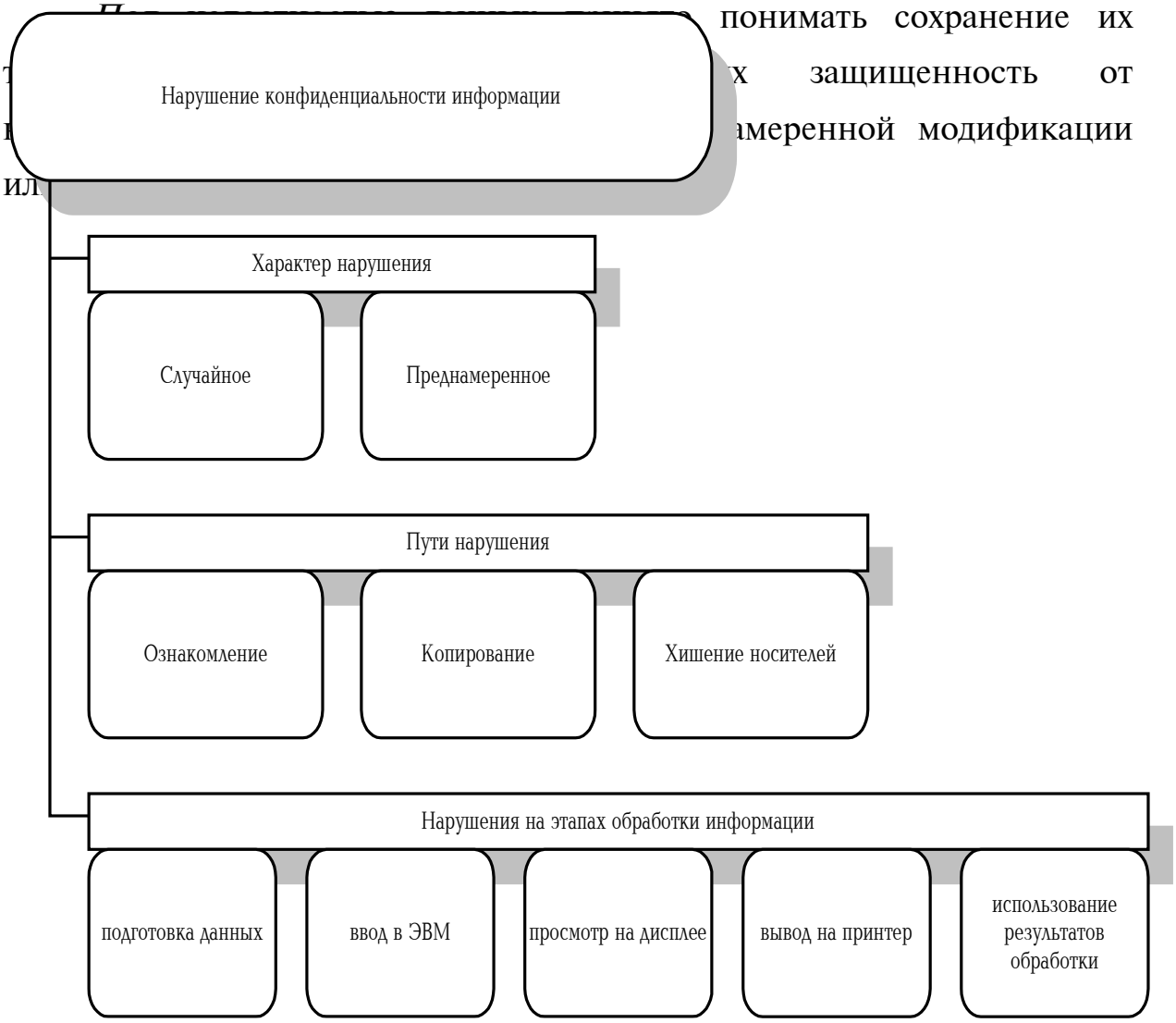

Рис. 2. Состав основных видов нарушений конфиденциальности информации.

Доступность данных - возможность использования лицами, которым это разрешено.

В ранее упомянутом законе Российской Федераци “Об информации, информатизации и защите информации” цели защиты имеют следующее определение [140]:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации: предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- обеспечение прав субъектов в информационных процессах при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Отличительная черта обеспечения безопасности информационных систем государственного сектора - необходимость строго детерминированной и централизованной системы, реализирующей принцип директивного управления и контроля. В данном случае необходимый уровень информационной безопасности определяется прежде всего государственными интересами, и только потом величиной затрат на обеспечение безопасности.

И, наоборот, в коммерческих информационных системах, право выбора мероприятий по обеспечению информационной безопасности принадлежит ее собственнику. При этом действующая в стране система правовых норм защиты информации должна оказывать методологическую помощь и правовую поддержку организации защитных мероприятий.

В литературе существуют разные подходы в определении информационной безопасности АИС коммерческого назначения. Так, Ю.А. Стрельченко определяет информационную безопасность как множество элементов: система защиты информации банка; деловая разведка; анализ необходимой для эффективного функционирования банка информации; целенаправленное распространение информации о банке для повышения эффективности его функционирования, а структура целей рассматривается как *защита ресурсов* и *комплексные усилия по снижению риска* [131].

Автор монографии [161] проводит исследование системы обеспечения информационной безопасности АИС с точки зрения несанкционированного ее получения и как само собою разумеющееся, предполагается защита информации от уничтожения или искажения. Вне поля зрения, однако, остается защита от несанкционированной модификации и несанкционированного размножения. Автор рассматривает основную направленность системы защиты как системное использование всех имеющихся средств и методов и экстраполяцию имеющихся достижений. В то же время концепция защиты вычислительных систем и сетей рассматривается в монографии без органической взаимосвязи с концепцией построения систем и сетей.

В. А. Герасименко в [35,34] расширяет подход и разрабатывает постановку задачи комплексной защиты информации в АИС и рассматривает следующие аспекты:

- *комплексность целевая* - защита по всей совокупности показателей защищенности информации и всей совокупности факторов, влияющих на защищенность;
- *комплексность временная* - непрерывная защита во все время и на всех этапах жизненного цикла АИС;
- *комплексность концептуальная* - изучение и реализация проблем защиты в общей совокупности всех проблем развития, построения и использования АИС.

Представляется возможным расширить предложенное содержание целевой комплексности, которая рассматривается как обеспечение физической и логической целостности АИС и предупреждение несанкционированного получения, модификации и распространения информации.

По нашему мнению цели комплексной защиты следует дополнить и расширить следующими компонентами:

- обеспечение [45]:

- физической и логической целостности системы формирования информационных ресурсов и достижение их достаточной для соответствующего применения полноты, достоверности, непротиворечивости, актуальности и юридической состоятельности;

- физической и логической целостности применяемых технологий обработки информации и, прежде всего, использующих современные системы и средства информатизации;

- обеспечение гарантий конституционных прав и свобод граждан в информационной сфере;

- предотвращение использования информационных ресурсов в ущерб правам и свободам граждан, законным интересам юридических лиц, государства и общества (предупреждение несанкционированного получения, модификации и распространения информации, а также отказа от своих действий);

- восстановление физической, логической, организационно-технологической целостности и устранение экономических потерь;
- наказание нарушителей.

Таким образом, целями системы информационной безопасности АИС являются не только предупреждение и обеспечение защиты активов, но и восстановление нормальной работы, а также установление и изучение причин и наказание виновных (рис. 3.).

Функция восстановления является одной из самых главных, которая должна обеспечить нормальное функционирование АИС и при ее проектировании это должно учитываться.

На структуру целей влияет множество факторов, которые представляют собой не что иное как угрозы безопасности АИС.

В свою очередь, цели комплексной защиты достигаются только при взаимодействии множества средств защиты, представляющих собой единное логическое целое, призванное обеспечить работу АИС в заданных режимах.

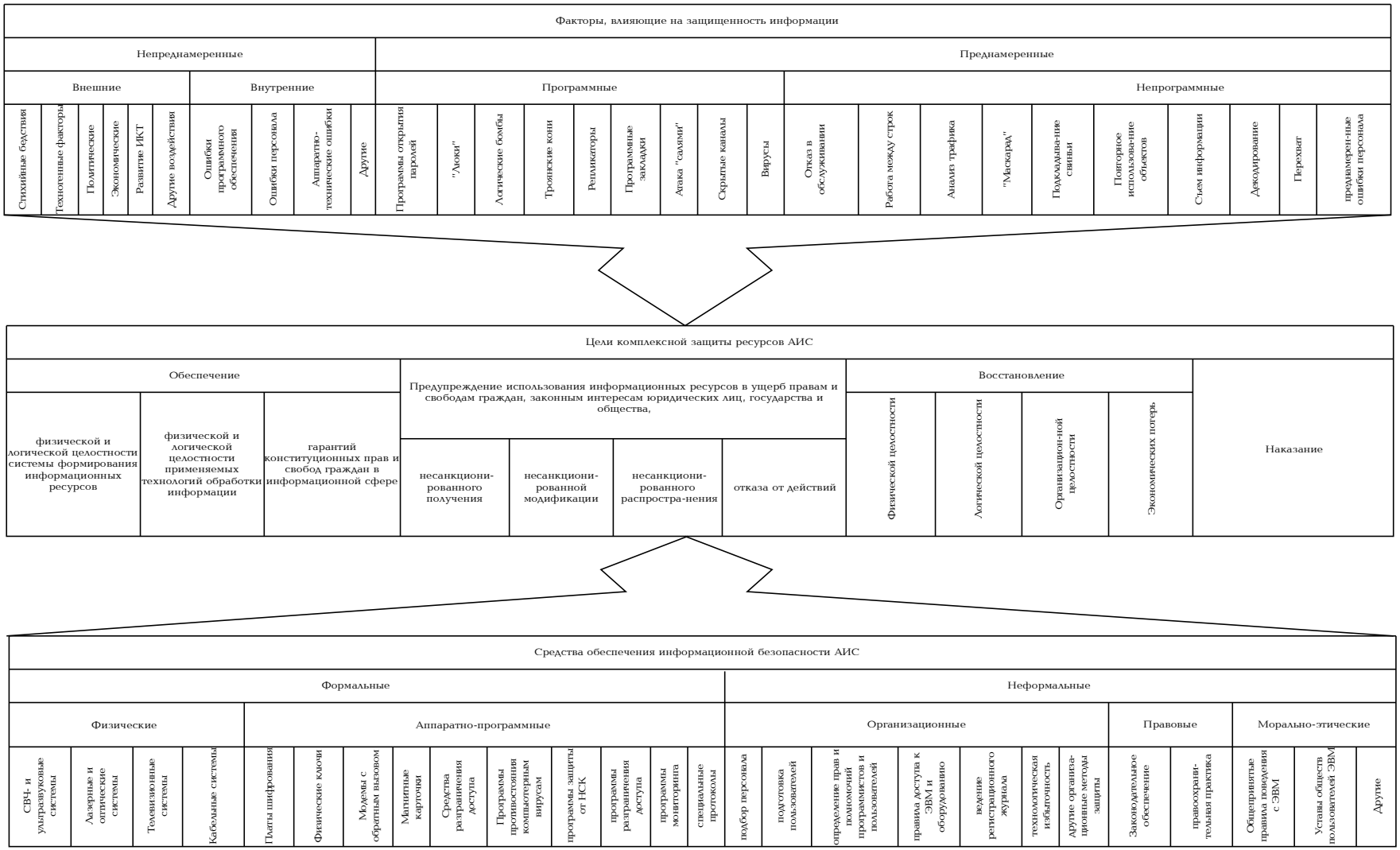

Рис.3. Структура и общее содержание целей комплексной защиты АИС

Из содержания рис. 3 видно, что множество средств защиты можно разделить на две большие группы: формальные и неформальные. Группа формальных средств защиты объединяет методы и средства, действие которых происходит по заранее заданному алгоритму. В свою очередь группа неформальных методов объединяет средства и методы рекомендательного и законодательного характера, которые определяют поведение людей в целях обеспечения безопасности АИС.

На современном этапе, когда общество становится все более информатизированным и открытым, когда пользователи получают в личное пользование компьютеры, модемы, факсы, радиотелефоны и другие телекоммуникационные средства с помощью которых можно реализовать связь со всем миром, проблема информационной безопасности встает особенно остро и не сводится только к компьютерной, а приобретает новые аспекты. К ним следует отнести:

- правовые;
- организационные;
- информационная безопасность программно-технического комплекса;
- экономические.

Рассмотрим основные аспекты информационной безопасности, выполняемые функции и используемые средства.

Правовые средства препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей. В качестве основы служат действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией ограниченного использования и ответственность за их нарушения.

Организационно-административные средства регламентируют процессы функционирования системы обработки информации, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой. Основными средствами

реализации служат: правила обработки информации в АИС; пропускной режим; организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией; распределение реквизитов доступа; организация подготовки и скрытого контроля за работой пользователей и персонала АИС.

Технические (аппаратно-программные) средства выполняют самостоятельно или в комплексе с другими средствами следующие функции защиты: создание препятствий на возможных путях проникновения и доступа потенциальных нарушителей к системе и защищаемой информации; идентификацию и аутентификацию пользователей; разграничение доступа к ресурсам; регистрацию событий; криптографическую защиту информации. Основными средствами являются специальные аппаратные и аппаратно-программные средства.

Морально-этические нормы регламентируют действия, несоблюдение которых приводит к падению авторитета, престижа человека, группы лиц и/или организации. Они представляются в виде определенных норм поведения, которые сложились или складываются по мере распространения ЭВМ в стране или в обществе. Морально-этические нормы бывают неписанные и писанные. Первые воспринимаются как общепризнанные правила поведения, а вторые как правила и предписания, оформленные в некий свод (например, “Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США”).

В составе каждой АИС должна быть построена собственная система информационной безопасности (СИБ), которая реализует операции по обнаружению, противостоянию угрозам безопасности и восстановлению ее нормальной работы.

Разработка такой системы является многоитерационным процессом, который реализуется на протяжении всего жизненного цикла АИС и включает все вышеописанные аспекты.

Рассматривая подходы к обеспечению информационной безопасности АИС, следует делать упор на системность процесса. При этом имеется ввиду не просто создание соответствующих механизмов, а регулярный процесс, осуществляемый на всех этапах жизненного цикла АИС при комплексном использовании всех имеющихся средств защиты [36]. Средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рациональным образом взаимосвязаны и составляют единый целостный механизм - систему обеспечения информационной безопасности (СИБ) АИС, которая должна обеспечить безопасность информации на всех уровнях не только от злоумышленников, но и некомпетентных или недостаточно подготовленных пользователей и персонала АИС.

Важно при реализации СИБ обеспечить разумный компромис между, с одной стороны, эффективностью защиты от злоупотреблений, сбоев и т.д., а с другой стороны - улучшением временных и стоимостных характеристик эксплуатации, сложностью доступа, увеличением времени обработки и т.д.