3.2. Правовые методы и средства обеспечения информационной безопасности

Блок правовых механизмов призван обеспечить права собственника информации государственных предприятий и органов управления, коммерческих структур (предприятий коллективной и частной форм собственности) и личной информации граждан.

В конце 70-х гг. международным сообществом ООН сформулированы два основных принципа, нашедших впоследствии отражение в национальном законодательстве ряда стран. К ним относятся:

- установление пределов вмешательства в частную жизнь с использованием компьютерных систем;

- введение административных механизмов защиты граждан от такого вмешательства.

Сложившаяся в бывшем СССР государственная система защиты информации соответствовала вполне определенным социально-политическим, экономическим и правовым условиям. К ним прежде всего относились:

- монопольная собственность государства на информационные ресурсы страны;

- строгая централизация международного обмена информацией;

- административно-репрессивный характер управления системой защиты информации;

- возможность ограничения правовых основ защиты информации в основном подзаконными актами;

- пространственно-временная локализация вероятных угроз защищаемой информации.

Если раньше проблемы информационной безопасности были только заботой государственных учреждений, которые производили, потребляли и хранили секретную информацию, то в современных условиях, когда общество становится открытым и демократическим, ни одно из перечисленных условий в правовом государстве с многообразием форм собственности не может иметь места.

Другим моментом является факт, что информация становится не только законным товаром, но также и средством незаконного обогащения, будучи одним из рычагов управления экономическим развитием общества. Исходя из этого, вопросы защиты информации начали обсуждаться всеми заинтересованными сторонами (производители, торговые организации, научно-исследовательские институты и др.). В виду того, что данная проблематика перестала быть “персональной”, вопросы информационной безопасности начали решаться на государственном уровне - начали разрабатываться нормативные акты и законы, которые регламентировали бы отношения производства, потребления, продажи и хранения информации. Например, в Россиikой Федерации основными законами в области с информационной деятельности являются “Закон о коммерческой тайне” [70] и закон “Об информации, информатизации и защите информации” [140].

В основу концепции закона “О коммерческой тайне” была положена идея переориентации существующей системы защиты информации на достижение баланса интересов человека, общества и государства, ее адаптацию к происходящим изменениям в системе управления, в экономической, политической, военной и других сферах жизни общества, создание механизмов реализации правоотношений, способных развиваться в новых условиях [12].

Несмотря на увеличение числа нормативных правовых актов в информационной сфере и рост публикаций на эту тему, пока еще нет единного, согласованнового подхода к решению этой проблемы. Как отмечает автор [3], недостаток принятых законов заключается прежде всего, в локальности применения. А по мнению В.Рубанова “принятые законы очень медленно внедряются в практику и “плохо” работают, а системы защиты информации все еше излишне милитаризованы” [123].

В [77] утверждается, что с помощью правовых норм в области информационной безопасности должны решаться следующие вопросы:

- отнесение информации к категориям открытого и ограниченного доступа;
- определение полномочий по доступу к информации;
- права должностных лиц на установление и изменение полномочий;
- способы и процедуры доступа;
- порядок контроля, документирования и анализа действий персонала;
- ответственность за нарушение установленных требований и правил;
- проблема доказательства вины нарушителя;
- соответствующие карательные санкции.

По мнению автора [14] действующее законодательство и нормативно - методическая база, создающая правовую основу обеспечения информационной безопасности, а также выработка предложений по ее совершенствованию и развитию требуют решения ряда вопросов методологического характера, к которым можно отнести:

- системное представление элементов в сфере информационной безопасности и их связи в инфосфере или информационной среде - ограниченном информационном пространстве;
- определение состава и характеристик предметных областей отношений по субъектно-объектному признаку и их роли в системе безопасности;
- выявление правовой формы установления желаемого порядка в предметной области каждого элемента безопасности;
- системное представление задач правового и организационного обеспечения и фактического состояния нормативного и организационного механизмов регулирования в сфере информационной безопасности.

При решении данных вопросов следует принять во внимание общие положения государственной политики обеспечения информационной безопасности, которые в [28] сводятся к следующим основам:

- ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

- ответственность за сохранность, засекречивание и рассекречивание информации персонифицируется;

- доступ к какой-либо информации, а также вводимые ограниченияя доступа осуществляются с учетом определяемых законом прав собственности на эту информацию;

- государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

- юридические и физичесике лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

- государство законными средствами обеспечивает защиту общества от ложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

- государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

- государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

- государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

- государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

- государство формирует государственную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единной системы информационной безопасности страны;

- государство прилагает усилия для противодействия информационной экспансии США и других развитых стран, поддерживает интернационализацию информационных систем и сетей.

Но основа основных положений государственной политики в области информационной безопасности формируется соответствующее правовое обеспечение.

Правовое обеспечение информационной безопасности включает *законодательное обеспечение* и *правоохранительную практику* [133] (рис.18).

Законодательное обеспечение - это законодательные акты, которые регламентируют правила обработки и использования информации и компьютерной техники, определяют категории открытого и ограниченного доступа, права и обязаности должностных лиц на установление и изменение полномочий, порядок контроля, документирования и анализа работы АИС и устанавливают меры ответственности за нарушение данных правил.

Цель законотворческой работы состоит в комплексном формировании и реализации законодательства по проблемам обеспечения информационной безопасности. Для реализации комплексного подхода к данным работам необходимо проводить следующие мероприятия [88]:

- тщательная организационная и законопроектная подготовка;

- систематическая работа по формирования правосознания в этой области;

Рис. 18. Состав правового обеспечения информационной безопасности АИС

- создание механизмов, которые обеспечивают применение и реализацию принятых законов и иных нормативных документов.

Следует отметить, что в последнее время сформировались следующие направления, требующие законодательной поддержки:

- защита персональных данных;

- борьба с компьютерной преступностью, в первую очередь в финансовой сфере;

- защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;

- защита государственных секретов;

- создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;

- обеспечение безопасности АСУ потенциально опасных производств;

- страхование информации и информационных систем;

- сертификация и лицензирование в области безопасности, контроля безопасности информационных систем;

- организация взаимодействия в сфере защиты данных со странами-членами СНГ и другими государствами.

Согласно [84] законодательное обеспечение объединяет следующие четыре группы законодетельной документации:

Первая группа - блок специальных актов, целиком посвященных проблемам законодательства;

Вторая группа - нормативные правовые акты (отдельные нормы в актах), входящие в состав уже существующих отраслей законодательства (права), посвященные информационным проблемам;

Третья группа - акты, определяющие статус и положение органов государственной власти , юридических лиц, в которые включаются нормы о правах, обязаностях и ответственности субъектов в области информационной деятельности;

Четвертая группа - правовые акты с нормами, регулирующими отношения относительно создания, преобразования и потребления информации.

Правоохранительная практика - представляется мероприятиями по выявлению, исполнению и доказательству компьютерных преступлений. Очевидно, что, в связи со значительной спецификой для практической судебной апробации всех законов, судьи должны получить специальную подготовку.

Следует отметить, что компьютерные преступления в области информационного бизнеса достаточно трудно предотвратить,

обнаружить, расследовать и устранить последствия. Это обусловлено рядом факторов [61,15,84,89], среди которых основными являются следующие:

- трудность выявления объективной стороны преступления;
- сложность АИС;
- значительное количество людей, имеющих прямое или косвенное отношение к подготовке, реализации и последствиям преступления;
- сложность установления субъективной стороны состава преступления с выделением двух аспектов: персонификация деяния и установление факта умышленного или неумышленного совершения воздействия;
- трудность определения предмета преступления;
- неопределенность характеристики системно-географического места совершения преступления и страны юрисдикции которой она подлежит;
- субъективной и объективной сложностью оценки ценности информации, хранимой в АИС, и, следовательно, прямой экономической оценки последствий преступлений.

При разработке и реализации правового обеспечения информационной безопасности АИС необходимо реализовать следующие этапы:

1. *Разработка принципов правового регулирования переработки информации с учетом аспектов обеспечения международной и общественной безопасности и прав человека.* Например, в основу Правового акта 1974г. (США) положены следующие принципы:

- *гласность* - системы, хранящие записи с информацией о частных лицах не должны быть засекречены;

- *индивидуальный доступ* - право человека знакомиться со своим досье;

- *индивидуальное участие* - право человека вносить поправки в информацию о нем;

- *ограничение сбора информации*;

- *ограничение использования информации* - собранная информация должна использоваться только в целях, для которых она собирается.

- *ограничение разглашения информации*;

- *управление информацией* (законность, необходимость, достоверность, полнота);

- *ответственность за деятельность по сбору и использованию информации.*

2. *Разработка правовых норм, устанавливающих ответственность за компьютерные преступления.* С уровнем жесткости санкций тесно связан методологический вопрос оценки ценности информации и определения потенциального ущерба, нанесенного отдельному лицу или обществу в целом.

3. *Защита профессиональных и авторских прав программистов как особой группы лиц, правовая незащищенность или неопределенность которой может существенно влиять на все аспекты обеспечения информационной безопасности.*

4. *Совершенствование уголовного и гражданского законодательства в области информационной безопасности.* Зарубежная практика показывает, что прежде всего законом должен быть установлен порядок санкционированного доступа к АИС. Черезвычайно важным является проблема придания юридической силы документам, формируемым компьютерными средствами.

5. *Совершенствование практики судопроизводства.* Следует отметить, что важной проблемой, которая затрудняет следствие и судопроизводство, является то, что компьютерные преступления (КП) зачастую не рассматриваются общественным мнением как серьезная угроза по сравнению с традиционными видами преступлений. В настоящее время есть все основания для того, чтобы предвидеть пассивность со стороны специальных органов по борьбе с экономическими преступлениями при расследовании случаев совершения КП.

Такая пассивность имеет свое оправдание в силу объективных причин. Низкая техническая оснащенность, недостаточные финансовые возможности и отсутствие высококвалифицированных кадров - это старые проблемы, которые не позволяют эффективно противостоять даже традиционным видам преступлений. Отсутствие должного внимания к криминальным аспектам процесса информатизации и возможности совершения КП может обернуться огромными техническими, экономическими и нравственными потерями. Поэтому необходима проработка комплекса вопросов, связанных с информационной безопасностью компьютерных систем. В их числе можно выделить такие, как:

- совершенствование законодательной базы, поскольку серьезная пустота в правовом отношении сводит к минимуму эффективность превентивных мер противодействия, в основном организационной и технологической направленности;

- разработка стандартов безопасности для всех компонент информационных технологий;

Появление новых видов преступлений связано с использованием вычислительной техники и развитием рыночных механизмов. Отсутствие

внимания к сфере обращения информации может привести, по нашему мнению, к непоправимым потерям и последствиям. Проблема защиты информации и исключения компьютерных преступлений требует подготовки высококвалифицированных кадров с глубокими специализированными знаниями, разработки новых методов расследования и доказательства, новой направленности аудиторской и ревизионной деятельности государственных инспекций и т.д.

6. *Постоянный гласный общественный контроль за разработкой законодательных актов и за разработчиками общедоступных АИС, баз данных и другого программного обеспечения.*

7. *Разработка, принятие, обеспечение международных договоров в области информационной безопасности.* Здесь следует выделить два основных аспекта.

Первый из них сводится к обеспечению правового режима трансграничных пересылок информации, включая:

- отношения *передачи*, разделяющиеся на: отношения поставки, когда передающая сторона формирует передаваемые данные и сама передает их по каналам связи; отношения считывания - когда передающая сторона пассивно допускает пользователя в АИС;

- отношения *коммутации* - возникают у субъектов "отношений передачи" с третьими лицами, содействующие реализации этих отношений. В настоящее время основным правовым актом, регламентирующим оказание услуг при коммутации сообщений по международным каналам автоматизированной связи, является международная конвенция, принятая Международным союзом электросвязи в 1982 году (Найроби). Однако ее положения полностью не обеспечивают правовое регулирование трансграничных пересылок через компьютерные сети с позиций качества и защиты;

- проблемы *международной стандартизации на совместимость ЭВМ, протоколов обмена, средств защиты.*

Второй аспект данного этапа требует уделять особое внимание вопросам реализации правовых ограничений в области компьютерных вооружений, прежде всего ракетно-ядерных.

8. *Правовая охрана стандартов по защите от несанкционированного доступа.* Эти стандарты могут бвть классифицированы на следуюшие разновидности:

- *основные стандарты*, устанавливающие общие функции, необходимые для достижения определенных целей;

- стандарты *функциональной совместимости*, в которых определяются функции и форматы обмена;

- *стандарты взаимодействия*, включающие интерфейс, конструктивные требования, требования к электрическим параметрам и логике;

- *стандарты реализации*, определяющие структуру и метод реализации, гарантирующие уровень вторичных характеристик (быстродействие, надежность, физическую защиту и т.п.).

В [25] рассматриваются следующие правовые методы и средства предотвращения несанкционированного распротранения и использования программного обеспечения:

Патентная защита. Согласно законам об авторском праве, производители программного обеспечения получают на определенное время исключительную лицензию. В обмен на нее патентодержатели в своих патентных заявках должны раскрыть все подробности и детали своих изобретений. Однако патентная защита не получила широкого распространения ввиду наличия следующих недостатков [9]:

- непроизводительные затраты времени, с которыми встречается разработчик программ - оформление патента может занять несколько лет, что может привести к тому, что патент будет получен уже после того, как программа морально устареет;
- большие затраты на получение патента, которые включают затраты на поиск квалифицированного эксперта, проведение исследования на предмет выявления в программе элементов новизны и признаков изобретения, а также составление документации о приоритете;
- возможность несанкционированного распространения патентной заявки; любой пользователь может снять с нее копию без лицензии с низкой вероятностью быть разоблаченным, поскольку нелегальное распространение программ ЭВМ затрудняет обнаружение нарушения права на патент.

Авторское право защищает выражение идеи, а не саму идею и приобретается оно только благодаря авторству. Для использования этого закона производителю программного обеспечения достаточно поместить знак собственности на версию программы, зарегистрировать знак собственности в бюро авторских прав, паредать копии защищенных материалов в библиотеку. Однако практическое применение закона об авторских правах на программное обеспечение связано с трудностями доказательства в суде присвоения авторства кодов программ.

Защита секретов производства - является наиболее популярным видом защиты программного обеспечения. В отличие от патентной защиты и закона об авторских правах, защиту производственных секретов, производитель может осуществлять без их раскрытия. Это достигается заключением лицензионных соглашений между покупателем и продавцом программного обеспечения, по которым покупатель

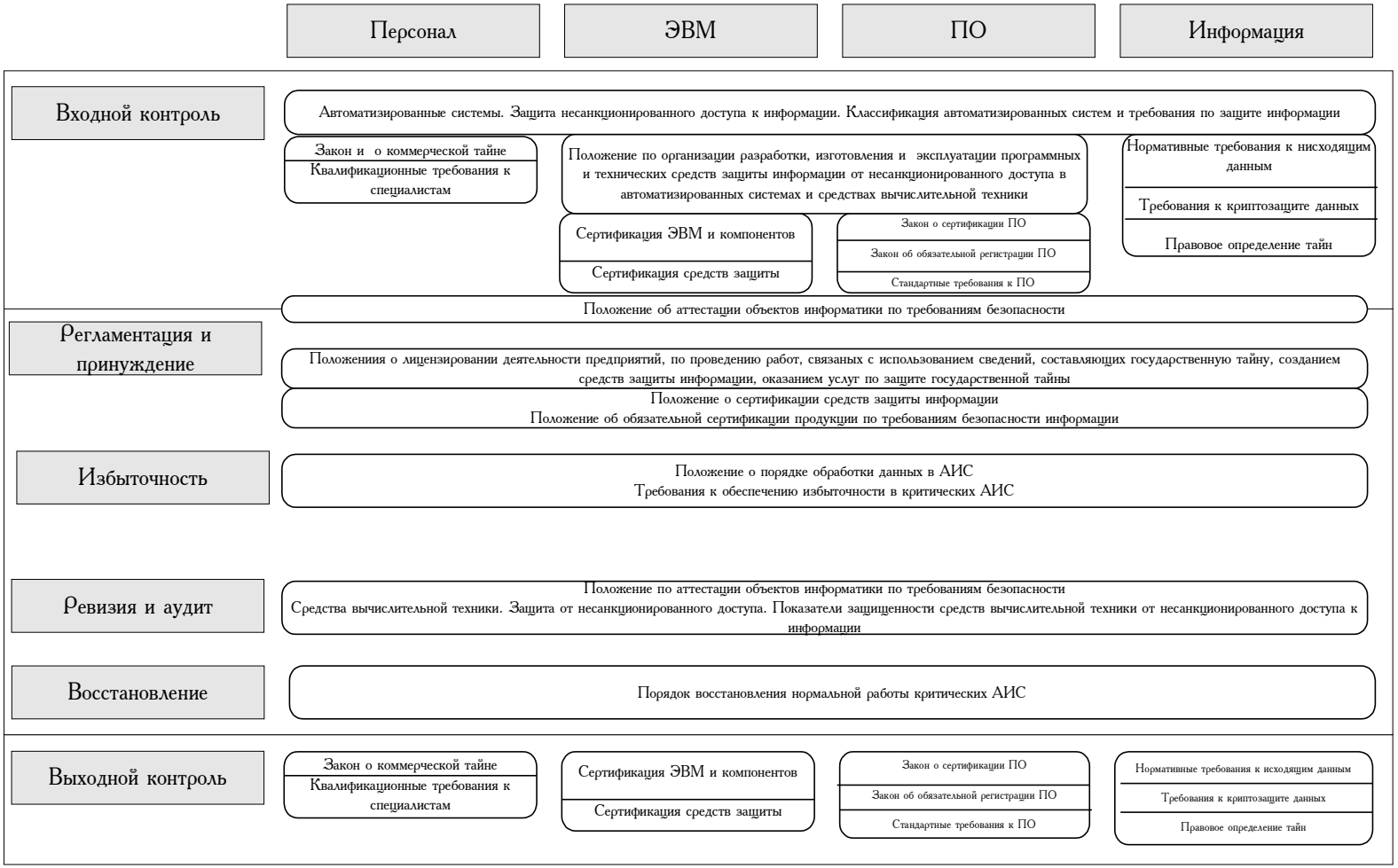
лицензии обязуется не раскрывать секретов производства разработчика программного обеспечения третьим лицам. Данный метод защиты также имеет некоторые недостатки: фирма-производитель программного обеспечения должна ограничить широкое распространение своей продукции, а также ограничить доступ к исходным текстам и к готовым версиям программного обеспечения.

Для того, чтобы повысить эффективность применения юридических мер защиты программного обеспечения от несанкционированного распространения и использования, следует применять комбинированные методы защиты:

- патентов и авторских прав;
- авторских прав и производственных секретов;
- патентов и призводственных секретов.

Важными элементами государственной системы защиты информации являются системы лицензирования деятельности предприятий по оказанию услуг в области защиты информации и сертификации продукции по требованиям безопасности информации [77]. Система лицензирования направлена на создание условий, при которых право заниматься работами по защите информации предоставлено только организациям, имеющим на этот вид деятельности соответствующее разрешение (лицензию). Организации, получившие лицензии, обязаны:

- осуществлять свою деятельность в строгом соотвествии с требованиями нормативных документов по защите информации;
- обеспечивать тайну переписки, телефонных переговоров, документальных и иных сообщений физических и юридических лиц, пользующихся их услугами;
- ежегодно представлять непосредственно в государственный орган по лицензированию сведения о количестве выполненных работ по конкретным видам указанной в лицензии деятельности.



EMBED ShapewareVISIO20

Рис 19. Состав правового обеспечения системы информационной безопасности АИС по объектам и операционным этапам.

Система сертификации технических и программных средств по требованиям безопасности информации направлена на защиту потребителя продукции и услуг от недобросовестной работы исполнителя.

На основе проведенного анализа представляется необходимым объединить правовые методы и средства, регламентирующие проблемы обеспечения информационной безопасности АИС и ее компонентов на всех операционных этапах (рис. 19).