ЧАСТЬ II

Основы построения систем защиты информации

В этой части

- *Законодательная, нормативно-методическая и научная база функционирования систем защиты информации*
- *Математические модели систем и процессов защиты информации*
- *Структура и задачи органов, осуществляющих комплексную защиту информации*
- *Политика информационной безопасности (организационно-технические и режимные меры)*
- *Программно-технические методы и средства защиты информации*

Законодательная, нормативно-методическая и научная база функционирования систем защиты информации

5

В этой главе

- *Подсистема организационно-правовой защиты*
- *Промышленный шпионаж и законодательство*
- *Защита программного обеспечения авторским правом*
- *Требования к содержанию нормативно-методических документов по ЗИ*
- *Нормативные документы, определяющие порядок защиты ИС*
- *Разработка нормативно-методической основы ЗИ*
- *Научно-методологический базис защиты информации*
- *Стратегическая направленность защиты информации*
- *Инструментальный базис защиты информации*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИН				Управление системой защиты			
	Основы >>>	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154
200	Выявление угроз и каналов утечки информации	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
300	Проведение оценки уязвимости и рисков	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
400	Определение требований к СЗИ	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
500	Осуществление выбора средств защиты	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
600	Внедрение и использование выбранных мер и средств	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
700	Контроль целостности и управление защитой	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Существуют различные представления о системах защиты информации с точки зрения их назначения, состава и выполняемых функций. Предлагаемый подход к рассмотрению совокупности проблем защиты информации не является строго научным, а представляет мнение автора по этим вопросам.

Итак, для формирования полного представления о системах защиты информации целесообразно рассмотреть их основные составляющие, а именно:

1. Законодательная, нормативно-методическая и научная база
2. Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации
3. Организационно-технические и режимные меры
4. Программно-технические методы и средства защиты информации

ОСНОВЫ СЗИ представлены на рисунках 5.1 и 5.2.

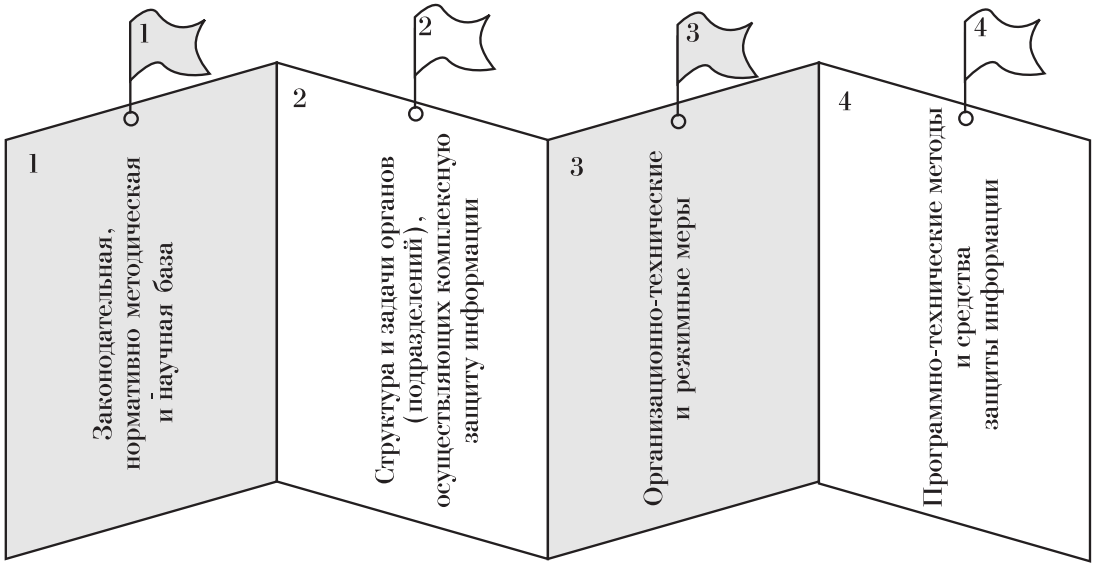


РИС. 5.2

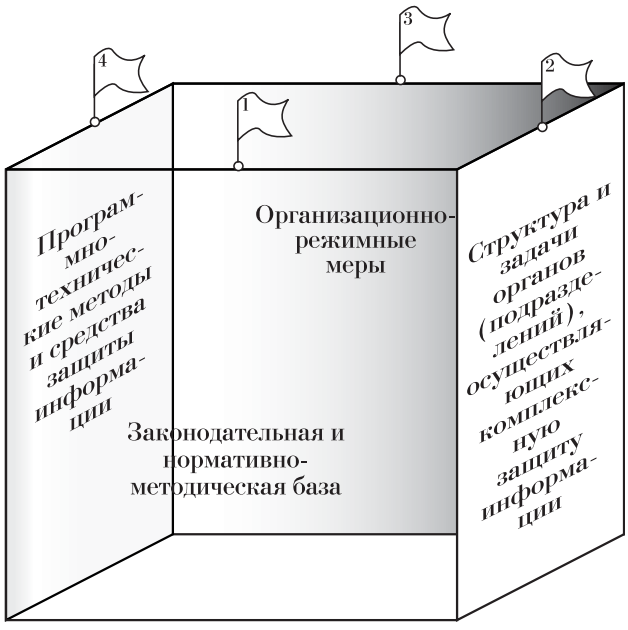


РИС. 5.1

Учитывая предложенный подход к систематизации материалов книги, напомним, что нормативно-методическая БАЗА (001) является одной из основных составляющих СЗИ. В содержании документов нормативно-методической базы целесообразно отразить следующие группы вопросов:

ОСНОВЫ:

- 002 Структура и задачи органов (подразделений), обеспечивающих защиту информации;
- 003 Организационно-технические и режимные меры и методы (политика информационной безопасности);
- 004 Программно-технические способы и средства.

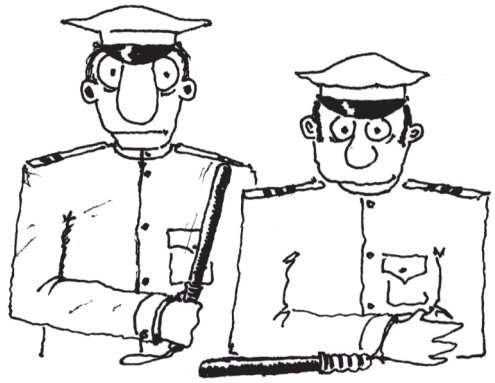
НАПРАВЛЕНИЯ:

- 010 Защита объектов корпоративных систем;
- 020 Защита процессов, процедур и программ обработки информации;
- 030 Защита каналов связи;
- 040 Подавление побочных электромагнитных излучений;
- 050 Управление системой защиты.

ЭТАПЫ:

- 100 Определение информационных и технических ресурсов, подлежащих защите;
- 200 Выявление полного множества потенциально возможных угроз и каналов утечки информации;
- 300 Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;
- 400 Определение требований к системе защиты;
- 500 Осуществление выбора средств защиты информации и их характеристики;
- 600 Внедрение и организация использования выбранных мер, способов и средств защиты;
- 700 Осуществление контроля целостности и управление системой защиты.

К сожалению, законодательная база еще отстает от потребностей практики. Имеющиеся законы и указы носят в основном запретительный характер. Ряд нормативных положений по защите информации в информационных системах, разработанных ранее, не соответствует уровню развития современных информационных технологий. Работы в этом направлении заметно отстают от потребностей и носят однобокий характер (в основном сведены к защите информации от утечки по техническим каналам).



"Имеющиеся законы и указы носят в основном запретительный характер..."

В литературе справедливо уделяют внимание ***правовым аспектам защиты информации***, которые могут возникнуть при недостаточно продуманном или злонамеренном использовании ИС. К ним относятся:

1. Правовые вопросы защиты информации и установления юридической ответственности за обеспечение ее сохранности.

2. Юридические и технические вопросы защиты информации от несанкционированного доступа, исключающие возможность неправомерного ее использования.

3. Установление юридически закрепленных норм и методов защиты авторских прав и приоритетов разработчиков программного продукта.

4. Разработка мероприятий по приданию юридической силы электронным документам и формирование юридических норм, определяющих ответственность за качество таких документов.

5. Правовая защита интересов экспертов, передающих свои знания в фонды банков данных.

6. Установление правовых норм и юридической ответственности за использование ИС в личных интересах, противоречащих интересам других личностей и общества.

В настоящее время пока еще отсутствует полная нормативно-правовая и методическая база для построения информационных и вычислительных систем в защищенном исполнении, пригодных для обработки секретной информации в государственных учреждениях и коммерческих структурах.

При разработке средств защиты ***возникает ряд проблем правового характера:***

1. Лицензирование деятельности по разработке средств защиты информации. (Система лицензирования направлена на создание условий, при которых право заниматься защитой информации предоставлено только организациям, имеющим на этот вид деятельности соответствующее разрешение).

2. Сертификация средств защиты. (Система сертификации направлена на защиту потребителя от недобросовестного исполнителя).

3. Соответствие разрабатываемых средств защиты концептуальным требованиям к защите, стандартам и другим нормативным документам.

4. Отсутствие нормативно-правового обеспечения для решения спорных ситуаций с использованием цифровой подписи в арбитражном суде.

5. Оценка информации в стоимостном выражении крайне проблематична и часто напрямую не может быть решена, например при возникновении угроз информационным системам, обрабатывающим секретную информацию. В этом случае ответственность устанавливается по аналогии с действующими нормами уголовного права.

Анализ показывает, что в целом можно выделить следующие ***критерии состава злоупотреблений*** в сфере обработки информации:

1. Нарушение правил регистрации информационных систем и перечней обрабатываемой информации.

2. Нарушение правил сбора информации, а именно: получение информации без разрешения и сбор ее сверх разрешенного перечня.

3. Хранение персональной информации сверх установленного срока.

4. Нарушение правил хранения информации.

5. Передача третьим лицам сведений, составляющих коммерческую тайну или персональных сведений.

6. Несвоевременное информирование о событиях, явлениях и фактах, могущих причинить вред здоровью или нанести материальный ущерб.

7. Превышение пределов компетенции учетной деятельности, допущение неполных учетных записей и фальсификации данных.

8. Предоставление заинтересованным лицам заведомо неточной информации.

9. Нарушение установленного порядка обеспечения безопасности информации.

10. Нарушение правил и технологии безопасной обработки информации.

11. Нарушение норм защищенности информации, установленных Законом.

12. Нарушение правил доступа к информации или к техническим средствам.

13. Нарушение механизма защиты информации и проникновение в систему.

14. Обход средств защиты и проникновение в систему.

15. Хищение информации.

16. Несанкционированное уничтожение данных в информационных системах.

17. Несанкционированная модификация данных в информационных системах.

18. Искажение (модификация) программного обеспечения.

19. Перехват электромагнитных, акустических или оптических излучений.

20. Перехват информации, передаваемой по линиям связи.

21. Изготовление и распространение заведомо непригодного ПО.

22. Распространение компьютерных вирусов.

23. Разглашение парольно-ключевой информации.

24. Несанкционированное ознакомление (попытка) с защищаемыми данными.

25. Несанкционированное копирование.

26. Внесение в ПО не оговоренных изменений, в том числе и вирусного характера.

Подсистема организационно-правовой защиты (001)

Такая подсистема предназначена для регламентации деятельности пользователей ИС и представляет собой упорядоченную совокупность организационных решений, нормативов, законов и правил, определяющих общую организацию работ по защите информации в ИС.

Организационно-правовую защиту структурно можно представить так:

Организационно-правовые вопросы:

а) органы, подразделения и лица, ответственные за защиту;

б) нормативно-правовые, методические и другие материалы;

в) меры ответственности за нарушение правил защиты;

г) порядок разрешения спорных ситуаций.

Регистрационные аспекты:

а) фиксация “подписи” под документом;

б) фиксация фактов ознакомление с информацией;

в) фиксация фактов изменения данных;

г) фиксация фактов копирования содержания.

Юридические аспекты.

Утверждение в качестве законов:

а) правил защиты информации;

б) мер ответственности за нарушение правил защиты;

в) регистрационных решений;

г) процессуальных норм и правил.

Морально-психологические аспекты:

а) подбор и расстановка кадров;

б) обучение персонала;

в) система моральных и материальных стимулов;

г) контроль за соблюдением правил.

Информационное право (001)

Насущная потребность информационного общества в построении его правового фундамента требует активного содействия становлению информационного права.

Морально-психологические аспекты...

Информационное право — это система охраняемых государством социальных норм и отношений, возникающих в информационной сфере — сфере производства, преобразования и потребления информации.

Определение

Информационное право — совокупность юридических норм и институтов, регулирующих информационные отношения в информационной сфере.

Основные объекты правового регулирования — это информационные отношения, т.е. отношения, возникающие при осуществлении информационных процессов — создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Таким образом, информационное право можно определить как комплексную отрасль права, представляемую системой охраняемых государством социальных норм и отношений (информационных отношений), возникающих в информационной сфере (производство, преобразования и потребление информации).

Основные субъекты информационного права (001)

К основным субъектам информационного права относятся лица, участвующие в создании, преобразовании, передаче и распространении, получении и потреблении информации. Это прежде всего создатели или производители информации, обладатели информации (или информаторы), потребители информации.

Создатели или производители информации — это лица, в результате интеллектуальной деятельности которых появляется информация. К ним относятся и авторы, создающие творческую продукцию, и лица (в том числе органы государственной власти, местного самоуправления, юридические лица), не претендующие на авторство по поводу созданной ими информации.

Обладатели информации (информаторы) — это посредники между создателями и потребителями информации; лица, приобретающие исключительное право на передачу и распространение информации и обеспечивающие доведение созданной информации до потребителя.

Потребители информации — это лица, нуждающиеся в информации, выполняющие поиск и получающие ее для удовлетворения своих потребностей (повышение знаний, образование, принятие решений и т.п.).

К субъектам информационного права относятся также и те лица, которые участвуют в создании и применении средств и механизмов программно-технического обеспечения информационных процессов — информационных систем, сетей, информационных технологий и средств их обеспечения (информационных, лингвистических, технических, программных и иных).

Информация как объект информационного права (001)

Под информацией как объектом права подразумеваются создаваемые в процессе интеллектуальной деятельности сведения (данные) об окружающем мире и протекающих в нем процессах или сообщения, осведомляющие о положении дел.

Информация — объект многофункциональный, она создается, обращается и применяется во всех сферах деятельности и как бы обеспечивает выполнение многочисленных функций и задач, стоящих перед разными субъектами — органами государственной власти, местного самоуправления, перед физическими и юридическими лицами.

При обращении информации в государстве и обществе она может выступать:

- как товар в процессах ее создания, хранения и использования, передачи и распространения;
- как средство, с помощью которого осуществляются правовые координация и управление поведением субъектов (через официальные документы и судебные решения);
- как источник для принятия решений;
- как источник знаний при образовании и воспитании в процессах осуществления конституционного права на образование;

- как средство извещения общества о происходящих событиях и явлениях (через СМИ) в порядке осуществления конституционного права на информацию;
- как средство отчетности о деятельности юридических и физических лиц (налоговая, бухгалтерская, статистическая отчетность и т.п.);
- как средство реализации прав и свобод личности через предоставление сведений о личности разным структурам (право на жизнь, право на жилище, право на медицинское образование; право на воспитание, право на труд и т.п.).

Следует обратить внимание на то, что информация одновременно может выступать и в качестве источника, несущего определенную функциональную нагрузку, и как товар. Например, нормативные правовые акты, выполняя основную функцию — распространение правовых норм и доведения их до каждого, — одновременно выступают и в качестве товара при продаже информационных продуктов и предоставлении информационных услуг, построенных на их основе.

То же самое можно сказать и о персональных данных, которые за рубежом продаются и сдаются в аренду для реализации прямого маркетинга. Продаются также различные информационные ресурсы, содержащие сведения о полезных ископаемых, о научном и техническом развитии общества, о его творческом потенциале и т.п.

Особенности и юридическими свойства информации (001)

В отличие от известных, традиционных для права объектов, информация обладает специфическими особенностями и юридическими свойствами, которые во многом определяют и отношения, возникающие при ее обращении между субъектами, и характер их поведения.

К таким особенностям и свойствам можно отнести следующие:

- Информация при включении в оборот обособляется от ее создателя или обладателя, овеществляется в виде символов или знаков и вследствие этого существует отдельно и независимо от создателя или обладателя. Отсюда возникает юридическое свойство информации — ***возможность выступать в качестве объекта***, передаваемого от одного субъекта к другому и требующего юридического закрепления факта ее принадлежности субъектам, участвующим в таком ее обращении;
- Информация, передаваемая от одного субъекта к другому, одновременно принадлежит двум участникам информационных отношений. Это основное отличие информации от вещи. Юридическое свойство информации в связи с этим — ее ***физическая неотчуждаемость от создателя***, обладателя и потребителя. Такое свойство требует разработки и применения к информации при ее обращении особых правовых механизмов, заменяющих механизм отчуждения вещи.
- Информация при включении в оборот документируется и отображается на материальном носителе. Существуют две группы носителей: жесткие — к которым информация привязана жестко (бумага, нестирающиеся лазерные диски и т.п.), и виртуальные, к которым информацию нельзя привязать жестко, по которым она как бы скользит (дискеты с перезаписью, оперативная память ПК и т.п.). Юридическое свойство, вытекающее из этой особенности, заключается в ***двуединстве информации и материального носителя***, на котором эта информация закрепляется.

Информация представляется в определенных организационных формах — отдельные данные (сведение), документ, массив (база) данных (документов), библиотека, фонд документов, архив и т.п. Отсюда юридическое свойство — ***возможность относить к информационным данным как отдельные исходные документы, так и сложные организационные структуры***, содержащие информацию. Это информационные системы, банки данных, информационные сети, библиотеки, архивы и т.п.

Основные принципы информационного права (001)

Под принципами информационного права будем понимать основные исходные положения, юридически закрепляющие объективные закономерности общественной жизни, проявляющиеся в информационной сфере. Принципы информационного права позволяют формировать это право как самостоятельную отрасль, вследствие чего являются системообразующими.

Можно выделить следующие основные принципы информационного права:

- **Принцип информационных отношений** как отношений, образующих комплексную отрасль информационного права, означает, что информационные отношения, возникающие, исходя из особенностей и юридических свойств информации и ее многофункциональности как основного объекта информационного права, обладают на этом основании спецификой, отличающей их от других общественных отношений, и составляют основу общественных отношений в информационной сфере;
- **Принцип информационной собственности** означает, что при передаче и распространении информации как основного объекта информационного права, объективно существуют особые категории субъектов информационного права (создатели, обладатели и потребители информации) и их поведение реализуется на основании информационных правомочий — права знать, обладать и применять информацию;
- **Принцип неотчуждаемости информации** от ее создателя, обладателя и потребителя (невозможность лишить субъекта полученных знаний) означает, что механизм отчуждения информации должен заменяться механизмом добровольного отказа от определенных информационных правомочий через установление по договору прав, обязанностей и ответственности по использованию этой информации после ее передачи указанными субъектами;
- **Принцип комплексного регулирования** отношений информационной собственности (в смысле признания информации своей собственной), означающий, что такие отношения могут регулироваться и авторским правом, и правом имущественной собственности, и правом инвестиционной собственности, в зависимости от конкретных условий;
- **Принцип инвестиционной собственности**, означающий, что механизм авторского права может быть распространен на создание любой открытой информации, представляющей для ее создателя интерес, в том числе и не относящейся к результату творчества. При этом защищаются только личные имущественные права создателя информации;
- **Принцип информационной вещи**, основанный на двуединстве материального носителя и информации, отображенной в нем, означает, что при обращении информационных вещей объективно существуют особые категории собственников информационных вещей (собственники-создатели, собственники-обладатели и собственники-потребители информационных вещей), которые реализуют традиционные правомочия собственников, однако при обязательном соблюдении ими информационных правомочий;
- **Принцип типовых информационно-правовых норм** означает, что такие нормы, вне зависимости от отрасли правового регулирования, обладают определенной спецификой, основанной на особенностях и юридических свойствах информации. Эта специфика выражается в том, что любая информационно-правовая норма обеспечивает регулирование отношений по поводу создания, обладания, передачи, распространения и применения информации через информационные правомочия субъектов, исходя из особенностей и функционального назначения конкретной информации.

Многофункциональность информации приводит к необходимости применять в информационном праве различные методы правового регулирования информационных отношений, в зависимости от вида информации и ее назначения в информационных процессах: создания, сбора, накопления и хранения информации, поиска, передачи, распространения и потребления информации.

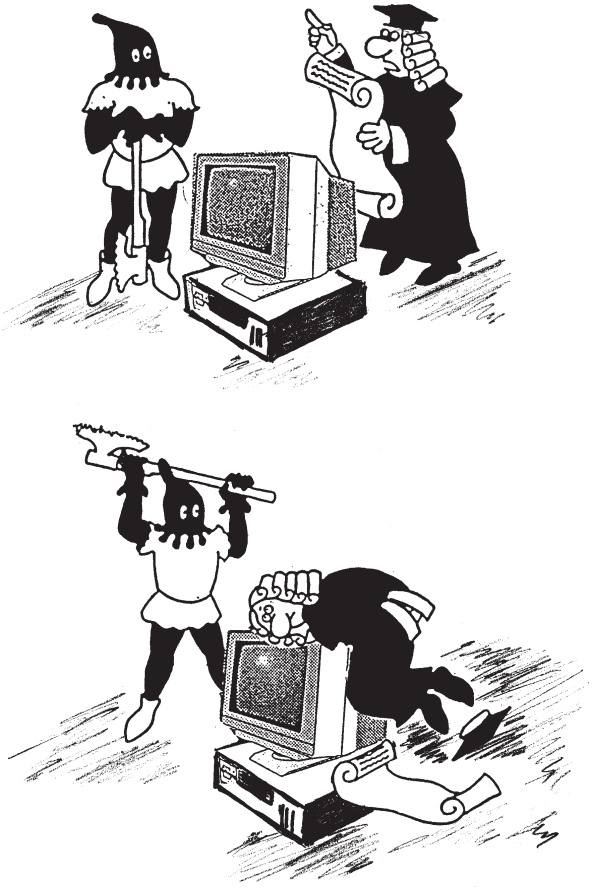
В частности, при регулировании отношений по поводу ответственности за допущенные правонарушения в информационной сфере должны использоваться методы законодательства об административных нарушениях и уголовного права.

Законодательство и промышленный шпионаж (011)

Многие специалисты отмечают слабость юриспруденции развитых стран в отношении защиты предприятий от промышленного шпионажа. Американский специалист по этому поводу высказался так: “Нет еще законов, обеспечивающих надлежащую защиту от похитителей секретных знаний и данных. Те, кто крадет эту ценную информацию, находятся в выгодном положении по сравнению с теми, кто крадет материальное имущество, так как первые не подпадают под действие закона о хищении имущества. Кроме того, промышленный шпион, как правило, рискует получить шесть месяцев тюрьмы за то, за что военный шпион был бы расстрелян, а вознаграждение промышленного шпиона в случае удачи было бы в несколько раз больше вознаграждения военного шпиона”.

Похищение промышленного секрета трудно доказуемо. Неадекватные законы — по словам американского юриста — ограничивают суды и дают им мало шансов в преследовании преступников, занимающихся промышленным шпионажем. Так, в США для того чтобы потребовать законодательной защиты ***в случае разглашения торгового секрета требуется доказать***:

1. Что предмет, рассматриваемый как торговый секрет, является таковым фактически;



Слабость юриспруденции в отношении защиты информации...

2. Право собственности на него;

3. Что действия лица, раскрывающего торговый секрет, относятся к одной из следующих категорий:

а) торговый секрет получен нечестным путем;

б) разглашение или использование торгового секрета представляет собой нарушение доверительных отношений между лицами;

в) лицо узнало секрет (в том числе и от третьего лица) и знало о том, что это секрет.

Лучше защищена запатентованная информация, хотя и здесь много слабых мест. Так, закон США предусматривает запрет на публикацию сведений в печати в течение года до подачи заявки на патентование. В других странах, (кроме Франции и Голландии), простого запрета на разглашение информации хватает для того, чтобы доказать, что она секретная. Однако и здесь законодательство несовершенно.

Но ни в какое сравнение с законами развитых стран не могут идти законы (а точнее, их полное отсутствие) на территории стран СНГ. Такое положение шокирует западных бизнесменов и вызывает у них боязнь инвестирования новых технологий в совместные предприятия, действующих на территории СНГ.

Коммерческой тайной не являются следующие документы и сведения:

- учредительные документы, документы, позволяющие заниматься предпринимательской или хозяйственной деятельностью или ее отдельными видами;
- информация по всем установленным формам государственной отчетности;
- данные, необходимые для проверки начисления и уплаты налогов и других обязательных платежей, сведения о численности и составе работающих, их заработной плате в целом, по профессиям и должностям, а также о наличии вакансий;
- документы об уплате налогов и обязательных платежей;
- информация о загрязнении окружающей природной среды, необеспечении безопасности условий труда, реализации продукции, которая приносит вред здоровью, а также о других нарушениях законодательства и размерах нанесенного при этом ущерба;
- документы о платежеспособности;
- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, союзах, объединениях и других организациях, которые занимаются предпринимательской деятельностью;
- сведения, которые в соответствии с действующим законодательством подлежат оглашению.

Указанные сведения предприятия обязаны предоставлять контролирующим органам государственной власти и правоохранительным органам, а также другим юридическим лицам по их требованию, согласно действующему законодательству.

Говорят, что успешно проведенные акции промышленного шпионажа ведут к получению незаконных преимуществ над конкурентами. Однако следует ли считать промышленный шпионаж таким серьезным преступлением в мире рыночных отношений, где правит конкуренция и где каждый с неизбежностью становится победителем или побежденным.

“Проколы” безопасности фирм на Западе нередки, однако руководство обычно стремится быстро закрыть дело чтобы избежать огласки и не ставить под удар свою репутацию. Обычная позиция руководителя фирмы: Со мной это никогда не случится, — часто подводит его самого, его сотрудников, клиентов и акционеров. На фирмах редко проявляют серьезное отношение к угрозам со стороны спецслужб других государств, причем спецслужб даже дружественных стран.

Руководство фирм игнорирует возможность шпионажа со стороны конкурентов, не интересуется методами негласного сбора информации, а безопасность до сих пор считается объектом накладных расходов и не рассматривается в качестве объекта инвестиций в защиту ценностей и ресурсов. Когда проблема все же возникает, от нее стараются отделаться одним ударом.

Политическая философия 80-х годов внесла большой вклад в разрушение лояльности, гордости и самодисциплины работников фирм. Некогда сильный "корпоративный дух" сегодня сгорает в котле индивидуализма рыночных отношений. Сотрудник, затаивший обиду на своего начальника, представляет собой наибольшую угрозу информационной безопасности, однако это в наименьшей степени осознается руководством компаний.

В наши дни размеры "информационной биржи", где люди занимаются куплей-продажей информации, значительно расширились, причем продажа нелегально добытых сведений не является чем-то совсем необычным. О деятельности брокеров на такой бирже по понятным причинам мало что известно, и это, весьма характерно для нашей действительности.

Интересно

Оценивая правовой аспект промышленного шпионажа, журнал "International Security Revierw" отмечает, что во всех странах Европейского союза нет законов, напрямую трактующих промышленный шпионаж в качестве противоправного деяния. Так, в Великобритании парламенту еще только предстоит признать промышленный шпионаж преступлением, хотя в этой стране существует с десяток законодательных актов, регулирующих те или иные стороны информационной безопасности. Однако попытки принять закон "О промышленной информации" в 1968 г. и "О злоупотреблении доверием" в 1981 г., в которых были даны определения понятий "промышленный шпионаж" и "угроза выведывания путем инсценированного интервью", успехом не увенчались. В то же время в ряде штатов США промышленный шпионаж законодательно считается преступлением.

Основной движущей силой промышленного шпионажа в рыночном обществе всегда была конкуренция. Все конкурирующие фирмы располагают сведениями, которые обычно легко получить из отраслевых периодических изданий, в ходе обычных деловых контактов. Однако некоторые данные фирмы всегда стремятся сохранить в тайне. Это сведения, за которыми охотятся конкуренты: технологические процессы, стратегии маркетинга, результаты научно-исследовательских и опытно-конструкторских работ — обычные цели промышленного шпионажа. Именно эти сведения должны быть четко определены и надежно защищены от хищений и несанкционированного доступа. Чем больше такой информации, тем острее стоит проблема обеспечения безопасности.

Защита программного обеспечения авторским правом (021)

Основные положения авторского права устанавливают баланс между общественным интересом и защитой прав автора. С одной стороны, общество нуждается в работах "ученых мужей" во имя процветания, с другой — права автора должны быть защищены для того, чтобы поощрить его к дальнейшей работе. Такую балансировку может обеспечить только очень хорошо продуманное, взвешенное законодательство.

Задолго до принятия Акта об авторском праве 1976 г. были установлены следующие два требования к "произведению", необходимые для защиты его авторским правом: оригинальность и реализация в материальной форме. Степень "художественности" произведения не играет роли, важно, чтобы оно было собственным произведением автора.

Здесь, однако, возникает вопрос о единственности представления идеи, точнее о запасе возможных представлений идеи. Если идея представляется единственным выражением, то защита выражения равносильна запрету использования идеи. Простая идея имеет небольшой запас выражений, ее представляющих, и они, как таковые, не могут быть защищены авторским правом. Поэтому должна быть установлена некая граница, начиная с которой "произведение" защищаемо авторским правом. Это особенно актуально применительно к программам. Ассемблерная программа перемножения двух чисел с фиксированной точкой вряд ли может быть защищена авторским правом. Однако правовое определение границы, начиная с которой программы защищаемы авторским правом, представляет собой непреодолимую трудность.

Авторское право обеспечивает автоматическую защиту. Защита авторским правом возникает вместе с созданием произведения независимо от того, предоставил ли автор копию произведения в соответствующий орган по авторскому праву для регистрации. Однако без регистрации держатель авторского права не может реализовать свои права. Например, он не может возбудить иск о нарушении его права и не может получить возмещение.

Закон подробно оговаривает, в каком виде должны представляться "копии" программ или баз данных для их регистрации. В случае опубликованной или неопубликованной программы требуется представить один экземпляр "идентифицирующей порции" программы, воспроизведенной в форме, визуально воспринимае-

мой без помощи машины или какого-либо устройства, на бумаге или на микроформе. Оговаривается, какова эта "порция". После установления, что представленное произведение защищаемо авторским правом, и просмотра сопровождающих (несложных!) документов Регистр Авторского Права (Register of Copyright) регистрирует требование и выдает автору свидетельство о регистрации.

Авторское право защищает произведение от копирования, но не запрещает независимого создания эквивалентов. Таким образом, риск монополизации знания при использовании авторского права существенно меньше, чем при использовании патентного права и, как следствие, стандарты защиты авторским правом не столь строги, как стандарты защиты патентным правом.

Авторское право США позволяет автору:

- воспроизведение;
- подготовку производных произведений;
- распространение копий или звукозаписей;
- публичное исполнение;
- выставку (display).

Авторское право, как упоминалось, защищает не идею, а ее выражение, конкретную форму представления. Поэтому в основу защиты программ авторским правом положены следующие соображения:

- ***Последовательность команд***. Программа — это последовательность команд, поэтому она может рассматриваться как "выражение" идеи автора, т.е. как его произведение.
- ***Копирование***. Это понятие, используемое в авторском праве, может быть распространено на перенос программ с одного носителя на другой, в том числе — на носитель другого типа. Математически это понятие формализуется следующим образом. Пусть имеются виды носителей A и B и процессы "перехода" с одного носителя на другой: **A———>B и B————>A.**

  Если объект *a* при переходе с A на B преобразуется в объект *b*, который при переходе с B на A переходит в прежний объект *a*, то такой "переход" считается копированием.

  Судить об идентичности программ на носителях A и B можно по многим признакам, например по их одинаковым функциональным свойствам; однако совпадение функциональных свойств не защищено авторским правом; одинаковость функциональных свойств, как таковая, еще не свидетельствует о воспроизведении "формы", т.е. о копировании.
- ***Творческая активность***. Подобно другим формам фиксации, защищаемым авторским правом, компьютерная программа есть результат творчества. Хотя эта форма выражения или фиксации все еще не является общеизвестной, уровень творческой активности, искусности и изобретательности, необходимый для создания программы, позволяет утверждать, что программы подлежат защите авторским правом не менее, чем любые другие произведения, им защищаемые. Тот факт, что компьютерные программы имеют утилитарное назначение, этого не меняет.
- ***Стиль***. Творчество, искусность и изобретательность автора проявляются в том, как создается программа. Необходимо поставить задачи, подлежащие решению. Затем проанализировать, как достичь решения, выбрать цепочки шагов, ведущих к решению; все это должно быть зафиксировано написанием текста программы. Способ выполнения придает программе характерные особенности и даже стиль.
- ***Алгоритм***. Собственно шаги, представляющие собой элементы, с помощью которых строится программа, т.е. алгоритмы, не могут быть защищены от неавторизованного воспроизведения. Это — аналоги слов в литературе или — мазков кисти в живописи.
- ***Отбор и сопряжение элементов***. Как и в случае других произведений, в частности литературных, защита компьютерных программ рассматривается с точки зрения отбора и сопряжения автором этих базовых элементов, в чем и проявляется его творчество и искусность, и что отличает его произведение от произведений других авторов. Случай, когда два автора независимо друг от друга написали бы для одной и той же цели две идентичные программы, практически исключен. Однако субрутины, которыми пользуются программисты, в основном общеизвестны (их берут в одной и той же операционной среде из единой библиотеки).

Авторское право защищает не идею, а ее выражение...

- ***Оригинальность программ*** — первое основное требование авторского права — часто основана на отборе и сопряжении этих общеизвестных элементов.
- ***Удачность***. Успех в решении задачи в значительной степени определяется тем отбором элементов, который автор произвел на каждом шаге построения. Поэтому программа может работать быстрее; она проще и надежнее в обращении, легче воспринимается и в целом более производительна, чем ее предшественница или конкуренты.

Эти и другие соображения были положены в основу защиты программ авторским правом. Здесь необходимо было обсудить ряд специфических положений:

- кто является автором произведения;
- что именно защищается (замысел, программа, документация);
- какие именно права гарантируются авторским правом;
- каким должен быть срок действия авторского права применительно к программе;
- в чем должна состоять процедура “регистрации” произведения;
- какие процедуры следует применять в случае нарушения авторского права и др.

Правовая защита программного обеспечения по своей проблематике во многом совпадает с более широкой задачей — правовой защитой интеллектуальной собственности.

В настоящее время имеется ***пять основных правовых механизмов защиты программного обеспечения:***

- авторское право;
- патентное право;
- право промышленных тайн;
- право, относящееся к недобросовестным методам конкуренции;
- контрактное право.

Два основных игрока на этой арене — авторское и патентное право. Три последних механизма защиты часто объединяют в одну группу.

Недостатки существующих стандартов и рекомендаций (051)

Стандарты и рекомендации образуют понятийный базис, на котором строятся все работы по обеспечению информационной безопасности. В то же время этот базис ориентирован, в первую очередь, на производителей и “оценщиков” систем и в гораздо меньшей степени — на потребителей.

Стандарты и рекомендации статичны. Во-первых, они не учитывают постоянной перестройки защищаемых систем и их окружения. Во-вторых, они не содержат практических рекомендаций по формированию режима безопасности.

Иными словами, стандарты и рекомендации не дают ответов на два главных и весьма актуальных с практической точки зрения вопроса:

- как приобретать и комплектовать информационную систему масштаба предприятия, чтобы ее можно было сделать безопасной?
- как практически сформировать режим безопасности и поддерживать его в условиях постоянно изменяющегося окружения и структуры самой системы?

С практической точки зрения интерес представляют простые рекомендации, следование которым дает пусть не оптимальное, но достаточно хорошее решение задачи обеспечения информационной безопасности.

Таким образом стандарты и рекомендации являются лишь отправной точкой на длинном и сложном пути защиты информационных систем организаций.

Требования к содержанию нормативно-методических документов по ЗИ (401)

ИС должна быть защищена путем внедрения продуманных правил безопасности. СЗИ должна использовать набор правил для того, чтобы определить, может ли данный субъект получить доступ к данному объекту. Для ИС целесообразно внедрение правил обеспечения безопасности и получение полномочий, с помощью которых можно было бы эффективно реализовать доступ к секретной информации. Пользователи, не обладающие соответствующими полномочиями, не должны получать доступ к секретной информации. Кроме того, необходимо применение дискриминационных методов управления, обеспечивающих доступ к данным только для некоторых пользователей или пользовательских групп, например, исходя из служебных обязанностей.

ИС должна быть защищена с помощью правил безопасности, которые ограничивают доступ к объектам (файлы, приложения) со стороны субъектов (пользователи).

Нормативные документы, определяющие порядок защиты ИС должны удовлетворять следующим требованиям:

- соответствовать структуре, целям и задачам ИС,
- описывать общую программу обеспечения безопасности сети, включая вопросы эксплуатации и усовершенствования,

- перечислять возможные угрозы информации и каналы ее утечки, результаты оценки опасностей и рекомендуемые защитные меры,
- определять ответственных за внедрение и эксплуатацию всех средств защиты,
- определять права и обязанности пользователей, причем таким способом, чтобы этот документ можно было использовать в суде при нарушении правил безопасности.

Разработка нормативно-методической основы ЗИ (001)

Прежде чем приступить к разработке документов, определяющих порядок ЗИ, нужно провести оценку угроз, определить информационные ресурсы, которые целесообразно защищать в первую очередь, и подумать, что необходимо для обеспечения их безопасности.

Целесообразно обратить внимание на следующие вопросы:

- **принадлежность информации**; об информации обязан заботиться тот, кому она принадлежит;
- **определение важности информации**; пока не определена значимость информации, не следует ожидать проявлений должного отношения к ней;
- **значение секретности**; как пользователи хотели бы защищать секретность информации? Нужна ли она им вообще?

Нормативно-методическая документация должна содержать следующие вопросы защиты информации:

- какие информационные ресурсы защищаются;
- какие программы можно использовать на служебных компьютерах;
- что происходит при обнаружении нелегальных программ или данных;
- дисциплинарные взыскания и общие указания о проведении служебных расследований;
- на кого распространяются правила;
- кто разрабатывает общие указания;
- кто имеет право изменять указания;
- точное описание полномочий и привилегий должностных лиц;
- кто может предоставлять полномочия и привилегии;
- порядок предоставления и лишения привилегий в области безопасности;
- полнота и порядок отчетности о нарушениях безопасности и преступной деятельности;
- особые обязанности руководства и служащих по обеспечению безопасности;
- объяснение важности правил (пользователи, осознающие необходимость соблюдения правил, точнее их выполняют);
- даты ввода в действие и пересмотра;
- кто и каким образом ввел в действие эти правила.

Некоторые нормативно-методические документы, необходимые для организации защиты информации (001)

Для организации и обеспечения эффективного функционирования СЗИ должны быть разработаны документы, определяющие порядок и правила обеспечения безопасности информации при ее обработке в ИС, а также документы, определяющие права и обязанности пользователей при работе с электронными документами юридического характера (договор об организации обмена электронными документами).

План защиты информации может содержать следующие сведения:

- назначение ИС;
- перечень решаемых ею задач;
- конфигурация;
- характеристики и размещение технических средств и программного обеспечения;
- перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите в ИС;
- требования по обеспечению доступности, конфиденциальности, целостности различных категорий информации;
- список пользователей и их полномочий по доступу к ресурсам системы;
- цель защиты системы и пути обеспечения безопасности ИС и циркулирующей в ней информации;
- перечень угроз безопасности ИС, от которых требуется защита, и наиболее вероятных путей нанесения ущерба;
- основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;
- требования к условиям применения и определение зон ответственности, установленных в системе технических средств защиты от НСД;
- основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС (особые обязанности должностных лиц ИС);
- цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и пути ее достижения;

- перечень и классификация возможных кризисных ситуаций;
- требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов и т.п.);
- обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;
- разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;
- определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.п.);
- определение порядка разрешения споров в случае возникновения конфликтов.

Научно-методологический базис защиты информации (001)

Научно-методологический базис защиты информации можно представить как совокупность трех иерархически взаимосвязанных компонентов следующего содержания:

- **первый** (верхний) уровень — общеметодологические принципы формирования любой науки, обобщенные до уровня мировоззренческих основ;
- **второй** (средний) уровень — общая методологическая база того фундаментального направления, составной ветвью которого является рассматриваемая;
- **третий** (низший) уровень — методы решения задач, учитывающие специфику конкретного направления.

Что касается **общеметодологических принципов** формирования науки, то они представляются следующим перечнем:

- строгое следование главной задаче науки — выявлению за внешними проявлениями внутренних движений, которые, как правило, — скрыты;
- упреждающая разработка общих концепций решения проблем;
- формирование концепций на основе реальных фактов, а не на основе абстрактных умозаключений;
- учет диалектики взаимосвязей количественных и качественных изменений в изучаемом фрагменте действительности;
- своевременное видоизменение постановок изучаемых задач;
- радикальная эволюция в реализации разработанных концепций;
- максимально возможная структуризация компонентов разработанных концепций и систем;
- унификация и типизация предлагаемых решений.

Для формирования структуры и содержания **второго уровня научно-методологического базиса** отправной точкой должна служить та посылка, что защита информации к настоящему времени уже выросла в достаточно серьезное и относительно самостоятельное научное направление, составляющее одну из ветвей того фундаментального научного направления информатики. Отсюда следует, что в качестве данного уровня для защиты информации должна выступать методологическая база информатики.

Существует еще одна проблема, связанная с формированием научно-методологического базиса современной информатики и имеющая непосредственное отношение к защите информации.

По мере расширения фронта решаемых задач защиты информации, управления качеством информации, обеспечения информационной безопасности, информационного обеспечения освоения информационного поля человечества и других подобных задач все более настойчивой становится необходимость накопления, хранения и аналитико-синтетической переработки сверхбольших объемов информации, характеризуемой повышенным уровнем неопределенности и противоречивости.

Современные методы и средства обработки не полностью удовлетворяют этим потребностям даже при нынешнем состоянии упомянутых задач.

Третий уровень **научно-методологического базиса** защиты информации составляют методы и модели непосредственного решения задач. Как известно из теории систем, все задачи, связанные с изучением, созданием, организацией и функционированием больших систем, разделены на три класса:

1. Анализ, состоящий в определении текущих и прогнозировании будущих значений, представляющих интерес характеристик изучаемых систем;

2. Синтез, состоящий в проектирование систем и их компонентов, оптимальных по заданной совокупности критериев;

3. Управление, состоящее в определении оптимальных управляющих воздействий, необходимость в которых может возникнуть в процессе функционирования систем.

Из изложенного очевидным представляется вывод о том, что основы научно-методологического базиса защиты информации в настоящее время имеются, но они нуждаются в серьезном развитии и, прежде всего, в сторону приспособления к адекватному учету неформальных факторов. Теперь есть основание говорить о наличии предпосылок успешного решения этой задачи.

Стратегическая направленность защиты информации (001)

Под стратегией понимается общая направленность в организации соответствующей деятельности, разрабатываемая с учетом объективных потребностей в данном виде деятельности, потенциально возможных условий ее осуществления и возможностей организации.

Осознание необходимости разработки стратегических подходов к защите формировались по мере осознания важности, многоаспектности и трудности защиты и невозможности эффективного ее осуществления простым использованием некоторого набора средств защиты.

Серьезным побудительным мотивом к проведению перспективных исследований в области защиты информации послужили те постоянно нарастающие количественные и качественные изменения в сфере информатизации, которые имели место в последние годы и которые, безусловно, должны быть учтены в концепциях защиты информации.

Исходя из большого разнообразия условий, при которых может возникнуть необходимость защиты информации, общая целевая установка на решение стратегических вопросов заключалась в разработке множества стратегий защиты, т.е. такого минимального их набора, который позволял бы рационально обеспечивать требуемую защиту в любых условиях.

В соответствии с наиболее реальными вариантами сочетаний значений рассмотренных факторов выделено три стратегии защиты:

- ***оборонительная*** — защита от уже известных угроз, осуществляемая автономно, т.е. без оказания существенного влияния на информационно-управляющую систему;
- ***наступательная*** — защита от всего множества потенциально возможных угроз, при осуществлении которой в архитектуре информационно-управляющей системы и технологии ее функционирования должны учитываться условия, продиктованные потребностями защиты;
- ***упреждающая*** — создание информационной среды, в которой угрозы информации не имели бы условий для проявления.

Характеристика и содержание указанных стратегий приведены в табл. 5.1, а содержание этапов построения СЗИ применительно к различным стратегиям отражено в табл. 5.2.

Инструментальный базис защиты информации (001)

Под инструментальным базисом защиты информации будем понимать организованную совокупность методов, моделей, средств и массивов (баз) данных, необходимых для эффективного решения специалистами по защите задач создания систем защиты, организации и обеспечения их функционирования.

Основное назначение инструментального базиса заключается в обеспечении:

- научно-методологического единства при массовом проведении работ по защите;
- специалистов органов защиты инструментальными средствами, необходимыми для решения задач защиты;
- специалистов, решающих задачи защиты, данными, необходимыми для эффективного решения задач;
- заинтересованных специалистов необходимыми справочными данными.

Чтобы соответствовать своему назначению, рассматриваемый базис должен содержать, по крайней мере, такие компоненты:

- методологический базис (учебно-методологические материалы, официальные документы, вспомогательные материалы);
- методы и модели решения задач (анализа, синтеза, управления);
- каталоги средств защиты (технических, программно-аппаратных, организационно-правовых, экономических, социально-психологических, морально-этических);

Таблица 5.1. Характеристики стратегий защиты информации.

Наименование характеристик	Стратегии защиты		
	Оборонительная	**Наступательная**	**Упреждающая**
Обеспечиваемый уровень защиты	Может быть достаточно высокий, но только относительно известных угроз	Может быть очень высоким, но только в пределах существующих представлений о природе угроз информации и возможностях их проявления	Может быть гарантирован очень высокий
Условия, необходимые для реализации	Наличие методов и средств нейтрализации известных угроз	1. Наличие перечня и характеристик полного множества потенциально возможных угроз информации 2. Наличие развитого арсенала методов и средств защиты 3. Наличие возможностей влияния на архитектуру ИС и технологию обработки информации	Наличие защищенной информационной технологии
Ресурсоемкость	Незначительная по сравнению с другими стратегиями	Значительная, причем с повышением требований к защите растет по экспоненте	1. Высокая в плане капитальных затрат 2. Незначительная в каждом конкретном случае - при наличии унифицированной защищенной информационной технологии
Рекомендации по применению	Невысокая степень секретности защищаемой информации и не очень большие ожидаемые потери при нарушении защищенности	Достаточно высокая степень секретности защищаемой информации и возможность значительных потерь при нарушении защищенности	Перспективная

Таблица 5.2. Содержание этапов построения СЗИ применительно к различным стратегиям защиты.

Наименование этапов построения СЗИ	Стратегии защиты		
	Оборонительная	**Наступательная**	**Упреждающая**
Формирование среды защиты		1. Структурированная архитектура ИС 2. Структурированная технология обработки защищаемой информации Четкая организация обработки защищаемой информации	Защищенная информационная технология в унифицированном исполнении
Анализ средств защиты	1. Представление организационно-структурного построения ИС в виде упорядоченного графа: узлы - типовые структурные компоненты, дуги - взаимосвязи между компонентами 2. Представление технологии обработки защищаемой информации в виде строго определенной схемы 3. Определение параметров защищаемой информации и условий ее обработки		
Оценки уязвимости информации	1. Определение значений вероятностей нарушения защищаемой информации в тех условиях, в которых она будет обрабатываться 2. Оценки размеров возможного ущерба при нарушениях защищенности информации		
Определение требований к защите	Определение вероятности надежной защиты информации, которая должна быть обеспечена при обработке защищаемой информации		
Построение системы защиты	Определение тех средств защиты, которые должны быть использованы при обработке защищаемой информации	Выбор типового варианта или проектирование индивидуальной системы защиты	Определение тех механизмов защиты, которые должны быть задействованы при обработке защищаемой информации
Организация функционирования систем защиты	Определение порядка использования выбранных средств защиты	Разработка технологии функционирования системы защиты	
Требования к среде защиты		Определяется в зависимости от требований к защите информации	Осуществление на базе унифицированной защищенной информационной технологии

При этом очевидно, что работы эти должны выполняться непрерывно, целенаправленно и профессионально только при четком организационном обеспечении.

При разработке неоднократно упомянутых ранее основ теории защиты доказано, что при нынешних масштабах работ по защите информации для обеспечения квалифицированного их выполнения необходима сеть специализированных центров защиты. Формирование и организация использования инструментального базиса должно стать одной из основных функций указанных центров.

Функции центров защиты могут быть представлены таким перечнем:

- участие в исследованиях и разработках основных вопросов защиты информации;
- аккумулирование всех новейших достижений в области защиты информации;
- приобретение (сбор), разработка, накопление, систематизация и хранение средств и сведений о средствах защиты;
- оказание конкретным объектам — абонентам услуг по созданию, организации и обеспечению функционирования систем защиты;
- сбор, накопление, хранение и аналитико-синтетическая обработка данных о функционировании систем защиты в информационно-управляющих системах своих абонентов.

В соответствии с таким перечнем функций центр защиты информации представляется как специализированное научно-производственное предприятие (объединение), профессионально ориентированное на разработку, практическую реализацию и внедрение концептуальных решений в области защиты информации, а также конкретных методов и средств защиты.

Особенно остро стоит вопрос о методах получения данных...

Особенно сложным представляется вопрос о методах получения данных, необходимых для формирования и поддержания инструментального базиса. Помимо того, что объем необходимых данных (о чем уже упоминалось) достаточно велик, получение многих из них (например, вероятностей проявления каналов несанкционированного получения информации, показателей эффективности неформальных средств защиты и им подобных) представляется неопределенной задачей.

Инструментальный базис защиты информации (001)

Под инструментальным базисом защиты информации будем понимать организованную совокупность методов, моделей, средств и массивов (баз) данных, необходимых для эффективного решения специалистами по защите задач создания систем защиты, организации и обеспечения их функционирования.

Основное назначение инструментального базиса заключается в обеспечении:

в научно-методологического единства при массовом проведении работ по защите;

- специалистов органов защиты инструментальными средствами, необходимыми для решения задач защиты;
- специалистов, решающих задачи защиты, данными, необходимыми для эффективного решения задач;
- заинтересованных специалистов необходимыми справочными данными.

Чтобы соответствовать своему назначению, рассматриваемый базис должен содержать, по крайней мере, такие компоненты:

- методологический базис (учебно-методологические материалы, официальные документы, вспомогательные материалы);
- методы и модели решения задач (анализа, синтеза, управления);
- каталоги средств защиты (технических, программно-аппаратных, организационно-правовых, экономических, социально-психологических, морально-этических);

При этом очевидно, что работы эти должны выполняться непрерывно, целенаправленно и профессионально только при четком организационном обеспечении.

При разработке неоднократно упоминавшихся ранее основ теории защиты доказано, что при нынешних масштабах работ по защите информации для обеспечения квалифицированного их выполнения необходима сеть

специализированных центров защиты. Формирование и организация использования инструментального базиса должно стать одной из основных функций указанных центров.

Функции центров защиты могут быть предоставлены таким перечнем:

- участие в исследованиях и разработках основных вопросов защиты информации;
- аккумулирование всех новейших достижений в области защиты информации;
- приобретение (сбор), разработка, накопление, систематизация и хранение средств и сведений о средствах защиты;
- оказание конкретным объектам — абонентам услуг по созданию, организации и обеспечению функционирования систем защиты;
- сбор, накопление, хранение и аналитико-синтетическая обработка данных о функционировании систем защиты в информационно-управляющих системах своих абонентов.

В соответствии с таким перечнем функций центр защиты информации представляется как специализированное научно-производственное предприятие (объединение), профессионально ориентированное на разработку, практическую реализацию и внедрение концептуальных решений в области защиты информации, а также конкретных методов и средств защиты.

Особенно сложным представляется вопрос о методах получения данных, необходимых для формирования и поддержания инструментального базиса. Помимо того, что объем необходимых данных (о чем уже упоминалось) достаточно велик, получение многих из них (например, вероятностей проявления каналов несанкционированного получения информации, показателей эффективности неформальных средств защиты и им подобных) представляется неопределенной задачей.

Резюме

К сожалению, законодательная база еще отстает от потребностей практики. Имеющиеся законы и указы носят в основном запретительный характер. Ряд нормативных положений по защите информации в информационных системах, разработанных ранее, не соответствует современным требованиям и современным информационным технологиям. Работы в этом направлении заметно отстают от потребностей и носят однобокий характер (в основном сведены к защите информации от утечки по техническим каналам перехвата).

Информационное право − это система охраняемых государством социальных норм и отношений, возникающих в информационной сфере — сфере производства, преобразования и потребления информации.

Основные объекты правового регулирования — это информационные отношения, т.е. отношения, возникающие при осуществлении информационных процессов — процессов создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации

Информационное право совокупность юридических норм и институтов, регулирующих информационные отношения в информационной сфере.

Таким образом, информационное право можно определить как комплексную отрасль права, представляемую системой охраняемых государством социальных норм и отношений (информационных отношений), возникающих в информационной сфере (производства, преобразования и потребления информации).

Авторское право защищает произведение от копирования, но не запрещает независимого создания эквивалентов. Таким образом, риск монополизации знания при использовании авторского права существенно меньше, чем при использовании патентного права и, как следствие, стандарты защиты авторским правом не столь строги, как стандарты защиты патентным правом.

Авторское право США предоставляет автору следующие пять прав:

- воспроизведение;
- подготовка производных произведений;
- распространение копий или звукозаписей;
- публичное исполнение;
- выставка (display).

Основы научно-методологического базиса защиты информации в настоящее время имеются, но они нуждаются в серьезном развитии и, прежде всего, в сторону приспособления к адекватному учету неформальных факторов. Теперь есть основание говорить о наличии предпосылок успешного решения этой задачи.

Под инструментальным базисом защиты информации понимается организованная совокупность методов, моделей, средств и массивов (баз) данных, необходимых для эффективного решения специалистами по защите задач создания систем защиты, организации и обеспечения их функционирования.

Основное назначение инструментального базиса заключается в обеспечении:

- научно-методологического единства при массовом проведении работ по защите;
- специалистов органов защиты инструментальными средствами, необходимыми для решения задач защиты;
- специалистов, решающих задачи защиты, данными, необходимыми для эффективного решения задач;
- заинтересованных специалистов необходимыми справочными данными.