4. Законодательный уровень информационной безопасности. Подсистема организационно-правовой защиты. Защита программного обеспечения авторским правом

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Комплексная защита информации создается на объектах для блокирования(парирования) всех возможных или наиболее вероятных угроз безопасности информации. Для парирования той или иной угрозы используется определенная совокупность средств и методов защиты, некоторые из них защищают от нескольких угроз одновременно.

Среди методов защиты имеются и универсальные методы, являющиеся базовыми при построении любой системы защиты.

Правовые методы защиты информации служат основой легитимного построения и использования системы защиты любого назначения.

Организационные методы защиты информации используются для парирования нескольких угроз, кроме того, их использование в любой системе защиты обязательно.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ОБЛАСТИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Государство должно обеспечить в стране защиту информации как в масштабах всего государства, так и на уровне организаций и своих граждан. Для этого государство обязано:

- выработать государственную политику безопасности в области информационных технологий;
- законодательно определить правовой статус ИВС, информации, систем защиты информации, владельцев и пользователей информации и т.д.;
- создать иерархическую структуру государственных органов, вырабатывающих и проводящих в жизнь политику безопасности информационных технологий;
- создать систему стандартизации, лицензирования и сертификации в области защиты информации;
- обеспечить приоритетное развитие отечественных защищенных информационных технологий;
- повышать уровень образования граждан в области информационных технологий, воспитывать у них патриотизм и бдительность;
- установить ответственность граждан за нарушения законодательства в области информационных технологий.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственниками информации. Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. По типу источника угрозы делят на связанные и несвязанные с деятельностью человека. Примерами могут служить удаление пользователем файла с важной информацией и пожар в здании, соответственно. Угрозы, связанные с деятельностью человека, разделяют на угрозы случайного и преднамеренного характера. В последнем случае источник угрозы называют нарушителем или злоумышленником.

Уязвимость (информационной системы) – свойство информационной системы, обуславливающее возможность реализации угроз безопасности, обрабатываемой в ней информации. Например, угроза потери информации из-за сбоя в сети электропитания

реализуется, если в АС не применяются источники бесперебойного питания или средства резервного электроснабжения (это является уязвимостью).

Если говорить об информационных ресурсах, то реализация угрозы может привести к таким последствиям как получение информации людьми, которым она не предназначена, уничтожение или изменение информации, недоступность ресурсов для пользователей. Таким образом, мы подошли к определению трех основных угроз безопасности.

Угроза конфиденциальности (угроза раскрытия) – это угроза, в результате реализации которой, конфиденциальная или секретная информация становится доступной лицу, группе лиц или какой-либо организации, которой она не предназначалась. Здесь надо пояснить разницу между секретной и конфиденциальной информацией. В отечественной литературе «секретной» обычно называют информацию, относящуюся к разряду государственной тайны, а «конфиденциальной» – персональные данные, коммерческую тайну и т. п.

Угроза целостности – угроза, в результате реализации которой информация становится измененной или уничтоженной. Необходимо отметить, что и в нормальном режиме работы АС данные могут изменяться и удаляться. Являются ли эти действия легальными или нет, должно определяться политикой безопасности.

Политика безопасности – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Угроза отказа в обслуживании (угроза доступности) – угроза, реализация которой приведет к отказу в обслуживании клиентов АС, несанкционированному использованию ресурсов злоумышленниками по своему усмотрению.

Таким образом, **безопасность информации** – это состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. А защита информации может быть определена как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Выделяются следующие направления защиты информации:

- **правовая защита информации** – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением;
- **техническая защита информации** – защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;
- **криптографическая защита информации** – защита информации с помощью ее криптографического преобразования;
- **физическая защита информации** – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Защита информации осуществляется с использованием способов и средств защиты.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. Отдельно выделяют:

- средства контроля эффективности защиты информации;
- средства физической защиты информации;
- криптографические средства защиты информации.

ОБЩАЯ СХЕМА ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Рассмотрим теперь взаимосвязь основных субъектов и объектов обеспечения безопасности, как это предлагается в международном стандарте ISO/IEC-15408.

Безопасность связана с защитой активов от угроз. Разработчики стандарта отмечают, что следует рассматривать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны с действиями человека. Рисунок 1.1 иллюстрирует взаимосвязь между высокоуровневыми понятиями безопасности.

За сохранность активов отвечают их владельцы, для которых они имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Действия нарушителей приводят к появлению угроз. Как уже отмечалось выше, угрозы реализуются через имеющиеся в системе уязвимости. Владельцы активов анализируют возможные угрозы, чтобы определить, какие из них могут быть реализованы в отношении рассматриваемой системы. В результате анализа определяются риски (т. е. события или ситуации, которые предполагают возможность ущерба) и проводится их анализ.

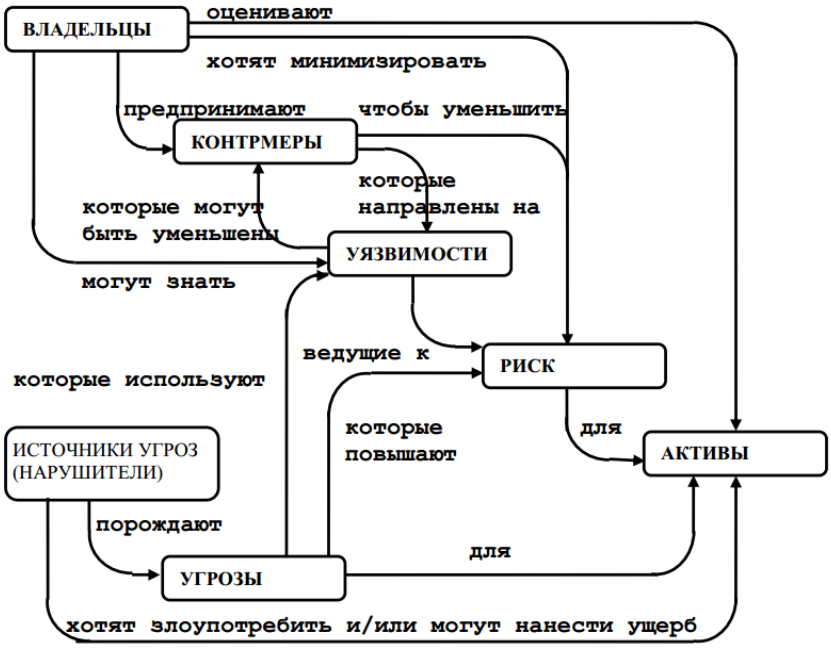

Рис. 1.1. Понятия безопасности и их взаимосвязь

Владельцы актива предпринимают контрмеры для уменьшения уязвимостей и выполнения политики безопасности. Но и после введения этих контрмер могут сохраняться остаточные уязвимости и соответственно – остаточный риск.

ОБЩАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИОННЫХ МЕТОДОВ ЗАЩИТЫ

Законы и нормативные акты исполняются только в том случае, если они подкрепляются организаторской деятельностью соответствующих структур, создаваемых в государстве, в ведомствах, учреждениях и организациях. При рассмотрении вопросов безопасности информации такая деятельность относится к организационным методам защиты информации.

Организационные методы защиты информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации ИВС для обеспечения заданного уровня безопасности информации.

Организационные методы защиты информации тесно связаны с правовым регулированием в области безопасности информации. В соответствии с законами и нормативными актами в министерствах, ведомствах, на предприятиях (независимо от форм собственности) для защиты информации создаются специальные службы безопасности. Эти службы подчиняются, руководству учреждения. Руководители служб организуют создание и функционирование систем защиты информации.

На организационном уровне решаются следующие задачи обеспечения безопасности информации в ИВС:

- организация работ по разработке системы защиты информации;
- ограничение доступа на объект и к ресурсам КС;
- разграничение доступа к ресурсам КС;
- планирование мероприятий;
- разработка документации;
- воспитание и обучение обслуживающего персонала и пользователей;
- сертификация средств защиты информации;
- лицензирование деятельности по защите информации;
- аттестация объектов защиты;
- совершенствование системы защиты информации;
- оценка эффективности функционирования системы защиты информации;
- контроль выполнения установленных правил работы в КС.

Организационные методы являются стержнем комплексной системы защиты информации в КС. Только с помощью этих методов возможно объединение на правовой основе технических, программных и криптографических средств защиты информации в единую комплексную систему. Конкретные организационные методы защиты информации будут приводиться при рассмотрении парирования угроз безопасности информации.

Наибольшее внимание организационным мероприятиям уделяется при изложении вопросов построения и организации функционирования комплексной системы защиты информации.

ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОРСКИМ ПРАВОМ

Прежде всего, рассмотрим вопрос о защите программного обеспечения авторским правом.

Авторское право восходит к британскому законодательству начала XVIII века, когда Парламентом был принят так называемый "Статус Анны" (1710), в котором говорилось о "поощрении ученых мужей составлять и писать полезные книги". Летом 1787 г. на Конституциональном конвенте в Филадельфии была принята Конституция Соединенных Штатов (ратифицирована в июне 1788 г.). В ней было заложено будущее патентное и авторское право. Согласно Конституции, Конгресс имеет право "поощрять развитие наук и полезных искусств, обеспечивая на определенный срок авторам и изобретателям исключительное право на их произведения и открытия" (Конституция США).

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 защищаться 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.

Провести четкую демаркационную линию между выражением и идеей нельзя. Известно следующее рассуждение судьи Л.Хэнда, так называемый "Абстракционный тест":

"Любое произведение, особенно пьесу, можно хорошо уложить в последовательность схем, общность которых будет возрастать по мере того, как все больше эпизодов опускается. Последняя из них может, пожалуй, оказаться не более чем общим утверждением, о чем эта пьеса, а иногда может попросту состоять из ее названия; однако в этой серии абстракций имеется пункт, начиная с которого они уже не защищаемы, ибо в противном случае драматург мог бы воспрепятствовать использованию его "идей", на которые, в отличие от их выражения, его собственность никогда не распространялась". Ни законодательно, ни прецедентно указать эту демаркационную линию не удалось.

Авторское право обеспечивает автоматическую защиту. Защита авторским правом возникает вместе с созданием произведения независимо от того, предоставил ли автор копию произведения в Бюро 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 воспринимаемой 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 предоставляет автору следующие пять прав:

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

Авторское право, как уже говорилось, защищает не идею, а ее выражение, конкретную форму представления. Поэтому в основу защиты программ авторским правом кладутся следующие соображения.

Последовательность команд

1. **Программа** — это последовательность команд, поэтому она может рассматриваться как "выражение" идеи автора, т.е. как его произведение.
2. **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 (с ленты на диск, в ПЗУ (ROM) и т.п.). 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 преобразуется в объект b, который при переходе с 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 защищается авторским правом; одинаковость функциональных свойств, как таковая, еще не свидетельствует о воспроизведении "формы", т.е. о копировании.

3. **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.

4. **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, которым все это проделывается, придает программе ее характерные особенности и даже стиль.

5. **Алгоритм**

Собственно, шаги представляют собой элементы, с помощью которых строится программа, т.е. алгоритмы, не могут защищаться от неавторизованного воспроизведения. Это — аналоги слов в литературе или — мазков кистью 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).

Оригинальность программ — первое основное требование авторского права — часто основана на отборе и сопряжении этих общеизвестных элементов.

6. **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.

Мы не останавливаемся на этих вопросах, а также на вопросах сравнения законодательства по защите программ авторским правом в разных странах и на сравнении этого законодательства с основными международными конвенциями (UCC (Universal Copyright Convention) — Всеобщая конвенция по авторскому праву; Буэнос-Айресская и Бернская конвенции).

Детальное рассмотрение их проблем требует отдельной работы. Имеются и более специфические вопросы, хуже осмысленные на сегодня в правовом отношении. К ним относятся: вопрос о форматах данных, используемых при вводе/выводе информации и вопрос об интерфейсе пользователь/программа; а также о структуре и организации программы.

Первая проблема состоит в следующем. Является ли нарушением авторского права использование форматов данных, особенно графических форматов — “экранов”, примененных в программах другого автора. Графические форматы сегодня широко

распространены, например, в связи со вводом оперативной экономической информации (системы key-to-disk в банковском деле и т.п.).

Вопрос об интерфейсе пользователь/программа получил название "look and feel" — "облик и ощущение". В какой мере пользовательский интерфейс новой программы выглядит как интерфейс более ранней программы, в какой степени он создает такое же ощущение? Эти вопросы важны, поскольку "удачность" программы связана в первую очередь с "приятным ощущением пользователя".

Программное обеспечение (software) состоит из трех компонент:

- замысла (основания, подосновы);
- собственно, программ;
- сопровождающей документации.

Замысел (подоснова) — это идеи, концепции, алгоритмы, соображения по реализации и т.п.

Программа может выступать в одной из трех форм: исходный, объектный или исполняемый коды.

К документации относятся: руководство по использованию, блок диаграммы, книги по обучению; иногда сложное программное изделие, такое, как операционная система, сопровождается специальным аудиовизуальным курсом обучения.

Мы не рассматриваем здесь аппаратных и программных средств защиты программных изделий (аппаратные ключи, вставляемые в параллельный порт, ключевые дискеты, прожигание отверстий лазером, привязка к аппаратному идентификатору машины и пр.). Мы касаемся только правовой защиты.

Имеется два основных подхода к правовой защите программного обеспечения:

- защита на основе уже существующей правовой системы;
- использование нового законодательства, независимо от существующего.

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.

Сменяемость компьютерных систем составляет характерную для рынка аппаратных средств величину: 40 мес. При сдаче компьютерной системы в аренду помесячная оплата составляет 1/40 от стоимости системы; эта цифра приводится, например, в таких справочниках, как GML Corporation booklet. Через 40 мес. система устаревает и должна быть заменена новой моделью. Никто, по-видимому, не проводил анализа, который позволил бы выяснить, какова "постоянная времени" для сменяемости программных изделий. За 14 лет существования (1976–1990гг.) операционной системы VAX/VMS (корпорация ДЭК) она прошла путь от первой версии до версии 5.3 через многие промежуточные версии (4.5, 4.7 и т.д.). Во всяком случае она претерпела за это время четыре крупных перехода и около 20 мелких. По-видимому, правильной "постоянной времени" для сменяемости программных изделий является 24–30 мес. Эта оценка важна потому, что срок патентования составляет несколько лет (до 5 и более). Так что даже если бы не было никаких правовых трудностей с патентованием программного обеспечения, механизм патентной защиты плохо подходил бы к программному обеспечению.