Принципы построения систем защиты информации

4

В этой главе

- *Понятия защиты*
- *Системность подхода*
- *Основные трудности*
- *Основные правила*
- *Защищенная ИС и система защиты информации*
- *Как обеспечить сохранность информации?*

<<< Этапы	Направления >>>	010				020				030				040				050			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				П Э М И Н				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

Вопросы организации защиты информации должны решаться уже на стадии предпроектной разработки ИС.

Опыт проектирования систем защиты еще не достаточен. Однако уже можно сделать некоторые обобщения. Погрешности защиты могут быть в значительной мере устранены, если при проектировании учитывать следующие основные *принципы построения системы защиты:*

1. ***Простота механизма защиты***. Этот принцип общеизвестен, но не всегда глубоко осознается. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением трудоемких действий при обычной работе законных пользователей.

2. ***Постоянство защиты***. Надежный механизм, реализующий это требование, должен быть постоянно защищен от несанкционированных изменений. Ни одна компьютерная система не может рассматриваться как безопасная, если основные аппаратные и программные механизмы, призванные обеспечивать безопасность, сами являются объектами несанкционированной модификации или видоизменения.

3. ***Всеобъемлющий контроль***. Этот принцип предполагает необходимость проверки полномочий любого обращения к любому объекту и лежит в основе системы защиты.

4. ***Несекретность проектирования***. Механизм защиты должен функционировать достаточно эффективно даже в том случае, если его структура и содержание известны злоумышленнику. Не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того, насколько опытны потенциальные нарушители. Защита не должна обеспечиваться только секретностью структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно способствовать ее преодолению (даже автору).

5. ***Идентификация***. Каждый объект ИС должен однозначно идентифицироваться. При попытке получения доступа к информации решение о санкционировании его следует принимать на основании данных претендента и определения высшей степени секретности информации, с которой ему разрешается работать. Такие данные об идентификации и полномочиях должны надежно сохраняться и обновляться компьютерной системой для каждого активного участника системы, выполняющего действия, затрагивающие ее безопасность. Пользователи должны иметь соответствующие полномочия, объекты (файлы) — соответствующий гриф, а система должна контролировать все попытки получения доступа.

6. ***Разделение полномочий***. Применение нескольких ключей защиты. Это удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.

7. ***Минимальные полномочия***. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для работы.

8. ***Надежность***. Система ЗИ должна иметь механизм, который позволил бы оценить обеспечение достаточной надежности функционирования СЗИ (соблюдение правил безопасности, секретности, идентификации и отчетности). Для этого необходимы выверенные и унифицированные аппаратные и программные средства контроля. Целью применения данных механизмов является выполнение определенных задач методом, обеспечивающим безопасность.

9. ***Максимальная обособленность механизма защиты*** означает, что защита должна быть отделена от функций управления данными.

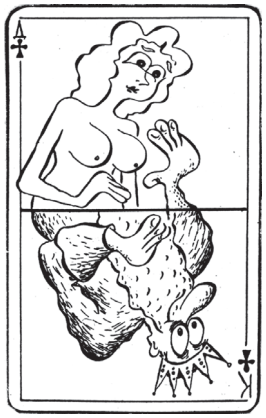
10. ***Защита памяти***. Пакет программ, реализующих защиту, должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно.

11. ***Удобство для пользователей***: схема защиты должна быть в реализации простой, чтобы механизм защиты не создавал для пользователей дополнительных трудностей.

12. ***Контроль доступа*** на основании авторизации пользователя по его физическому ключу и личному PIN-коду. Это обеспечивает защиту от атак неавторизованных пользователей на доступ:

- к ресурсам ПК;
- к областям HD ПК;
- к ресурсам и серверам сети;
- к модулям выполнения авторизации пользователей.

13. ***Авторизация*** пользователя на основании физического ключа позволяет ис-



Механизмы защиты ресурсов должны контролировать доступ к объектам...

ключить непреднамеренную дискредитацию его прав доступа.

14. ***Отчетность***. Необходимо защищать контрольные данные от модификации и несанкционированного уничтожения, чтобы обеспечить обнаружение и расследование выявленных фактов нарушения безопасности. Надежная система должна сохранять сведения о всех событиях, имеющих отношение к безопасности, в контрольных журналах. Кроме того, она должна гарантировать выбор интересующих событий при проведении аудита, чтобы минимизировать стоимость аудита и повысить эффективность анализа. Наличие программных средств аудита или создание отчетов еще не означает ни усиления безопасности, ни наличия гарантий обнаружения нарушений.

15. ***Доступность к исполнению*** только тех команд операционной системы, которые не могут повредить операционную среду и результат контроля предыдущей аутентификации.

16. ***Наличие механизмов защиты*** от:

- несанкционированного чтения информации;
- модификации хранящейся и циркулирующей в сети информации;
- навязывания информации;
- несанкционированного отказа от авторства переданной информации.

17. ***Системный подход*** к защите информации предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенных для обеспечения безопасности ИС.

18. ***Возможность наращивания защиты***. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

19. ***Комплексный подход*** предполагает согласованное применение разнородных средств защиты информации.

20. ***Адекватность*** — обеспечение необходимого уровня защиты (определяется степенью секретности подлежащей обработке информации) при минимальных издержках на создание механизма защиты и обеспечение его функционирования. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и масштаб возможного ущерба были бы приемлемыми (задача анализа риска).

21. ***Минимизация привилегий*** в доступе, предоставляемых пользователям, т.е. каждому пользователю должны предоставляться только действительно необходимые ему права по обращению к ресурсам системы и данным.

22. ***Полнота контроля*** — обязательный контроль всех обращений к защищаемым данным.

23. ***Наказуемость нарушений***. Наиболее распространенная мера наказания — отказ в доступе к системе.

24. ***Экономичность механизма*** — обеспечение минимальности расходов на создание и эксплуатацию механизма.

25. ***Принцип системности*** сводится к тому, что для обеспечения надежной защиты информации в современных ИС должна быть обеспечена надежная и согласованная защита во всех структурных элементах, на всех технологических участках автоматизированной обработки информации и во все время функционирования ИС.

26. ***Специализация***, как принцип организации защиты, предполагает, что надежный механизм защиты может быть спроектирован и организован лишь профессиональными специалистами по защите информации. Кроме того, для обеспечения эффективного функционирования механизма защиты в состав ИС должны быть включены соответствующие специалисты.

27. ***Принцип неформальности*** означает, что методология проектирования механизма защиты и обеспечения его функционирования в основе своей — неформальна. В настоящее время не существует инженерной (в традиционном понимании этого термина) методики проектирования механизма защиты. Методики проектирования, разработанные к настоящему времени, содержат комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое их осуществление в общем случае невозможно.

28. ***Гибкость системы защиты***. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

29. ***Принцип непрерывности*** защиты предполагает, что защита информации — это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а *непрерывный целенаправленный процесс*, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС. Разработка системы защиты должна осуществляться параллельно с разработкой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном сче-

те, создать более эффективные защищенные информационные системы.

Понятия защиты (001)

На формулирование понятия защиты оказывает влияние большое количество разноплановых факторов, основными из которых выступают:

- влияние информации на эффективность принимаемых решений;
- концепции построения и использования защищенных информационных систем;
- техническая оснащенность информационных систем;
- характеристики информационных систем и их компонентов с точки зрения угроз сохранности информации;
- потенциальные возможности злоумышленного воздействия на информацию, ее получение и использование;
- наличие методов и средств защиты информации.

Кстати

Развитие подходов к защите информации происходит под воздействием перечисленных факторов, при этом можно условно выделить три периода развития СЗИ:

первый — относится к тому времени, когда обработка информации осуществлялась по традиционным (ручным, бумажным) технологиям;

второй — когда для обработки информации на регулярной основе применялись средства электронно-вычислительной техники первых поколений;

третий — когда использование ИТ приняло массовый и повсеместный характер.

Системность подхода (001)

Генеральным направлением поиска путей защиты информации является неуклонное повышение системности подхода к самой проблеме защиты информации. Понятие системности интерпретировалось прежде всего в том смысле, что защита информации заключается не только в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рационально объединяются в единый целостный механизм — систему защиты, которая должна обеспечивать, говоря военным языком, глубокоэшелонированную оборону, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала.

В этой системе должно быть, по крайней мере, четыре защитных пояса: внешний, охватывающий всю территорию, на которой расположены сооружения; пояс сооружений, помещений или устройств системы; пояс компонентов системы (технических средств, программного обеспечения, элементов баз данных) и пояс технологических процессов обработки данных (ввод/вывод, внутренняя обработка и т.п.).

Трудности реализации СЗИ (001)

Основные трудности реализации систем защиты состоят в том, что они должны удовлетворять двум группам противоречивых требований. С одной стороны, должна быть обеспечена надежная защита находящейся в системе информации, что в более конкретном выражении формулируется в виде двух обобщенных задач: исключение случайной и преднамеренной выдачи информации посторонним лицам и разграничение доступа к устройствам и ресурсам системы всех пользователей, администрации и обслуживающего персонала. С другой стороны, системы защиты не должны создавать заметных неудобств в процессе работы с использованием ресурсов системы.

В частности должны быть гарантированы:

- полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий;
- удобство работы с информацией для групп взаимосвязанных пользователей;
- возможности пользователям допускать друг друга к своей информации.

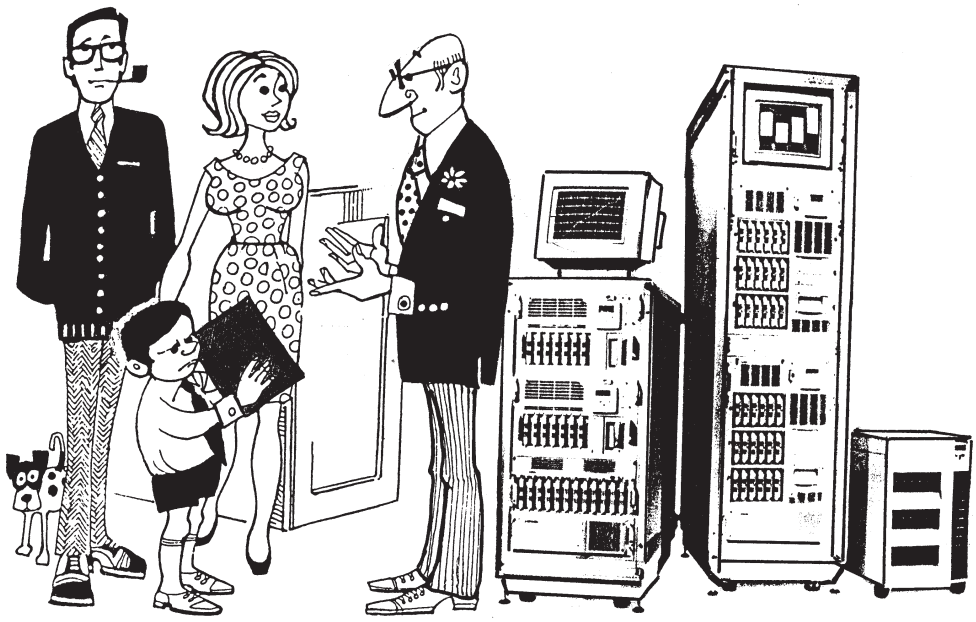
Основные правила защиты (001)

Основные правила, которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты.



Надлежащая подготовка пользователей...

4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

С самых первых этапов, т.е. с той поры, когда проблема защиты информации в системах обработки данных стала рассматриваться как самостоятельная, основными средствами, используемыми для защиты, были технические и программные.

Техническими названы такие средства, которые реализуются в виде электрических, электромеханических, электронных устройств. Всю совокупность технических средств принято делить на аппаратные и физические.

Определение

Под аппаратными средствами защиты понимают устройства, внедряемые непосредственно в аппаратуру обработки данных, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Наиболее известные аппаратные средства, используемые на первом этапе – это схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры (например, регистры границ поля ЗУ) и т.п.

Физическими средствами названы такие, которые реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения, замки на дверях, решетки на окнах и т.п.).

Программные средства защиты, как известно, образуют программы специально предназначенные для выполнения функций, связанных с защитой информации.

Первоначально программные механизмы защиты включались в состав операционных систем или систем управления базами данных. Этим, видимо, и объясняется, что ***практически все без исключения операционные системы содержат механизмы защиты информации от несанкционированного доступа, а именно:***

- динамическое распределение ресурсов вычислительной системы и запрещение задачам пользователей использовать чужие ресурсы;
- разграничение доступа пользователей к ресурсам системы по паролям;
- разграничение доступа к полям оперативной и долговременной памяти по ключам защиты;
- защита таблицы паролей с помощью так называемого главного пароля.

Защищенная ИС и система защиты информации (001)

Многие специалисты считают, что точный ответ на вопрос, что же такое “защищенная информационная система”, пока не найден.

Существуют следующие представления защищенности ИС:

- это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;
- это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;
- это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Для упрощения подачи материала предлагается следующее определение защищенной ИС.

Определение

Защищенной будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС.

При этом механизмы выполнения указанных правил чаще всего реализуются в виде *системы защиты информации*.

Следовательно, *под СЗИ будем понимать* совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Таким образом, список угроз информации определяет основу для формирования требований к защите. Когда такие требования известны, могут быть определены соответствующие правила обеспечения защиты. Эти правила, в свою очередь, определяют необходимые функции и средства защиты, объединенные в комплексную СЗИ.

Можно утверждать, что чем полнее будет список требований к защите и соответствующих правил защиты, тем эффективнее будет СЗИ для данной ИС.

Для того чтобы построить защищенную ИС, целесообразно провести анализ угроз информации, составить перечень требований к защите, сформулировать правила организации непосредственной защиты и реализовать их выполнение путем создания комплексной СЗИ, которая представляет собой действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту важной информации от всех выявленных угроз и возможных каналов утечки.

Как обеспечить сохранность информации? (001)

Как же обеспечить сохранность своей информации? Ведь многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. Вместе с тем, в настоящее время разработано и применяется большое количество технологий, способов и средств защиты информации, которые необходимо проанализировать и использовать в информационных системах уже сегодня. Это позволит резко сократить утечку сведений конфиденциального характера.

Руководителям следует помнить, что закон Мерфи актуален и для проблем защиты информации. Напомним его содержание:

Это важно

Если какая-нибудь неприятность может случиться, она случается.

Следствия.

1. Все не так легко, как кажется.
2. Всякая работа требует больше времени, чем вы думаете.
3. Из всех неприятностей произойдет именно та, ущерб от которой больше.
4. Если четыре причины возможных неприятностей заранее устранены, то всегда найдется пятая.
5. Предоставленные самим себе, события имеют тенденцию развиваться от плохого к худшему.
6. Как только вы принимаетесь делать какую-то работу, находится другая, которую надо сделать еще раньше.
7. Всякое решение плодит новые проблемы.

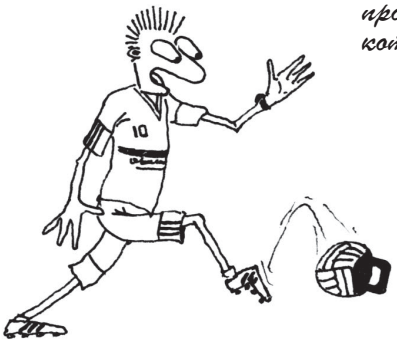
Приступая к работе по созданию защищенной ИС, желательно в собственном представлении создать образ Вашей ИС в любом удобном для простого понимания виде. Попробуйте включить фантазию в этот процесс.

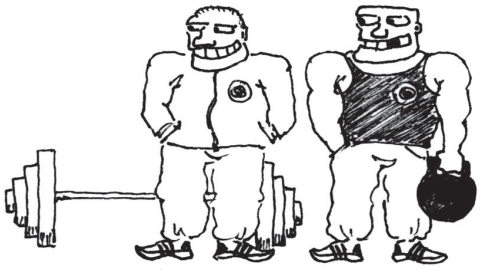
Для примера: работу нескольких пользователей на одном ПК (как это часто бывает) можно сравнить с банком или кассой, когда все стараются взять как можно больше, а вернуть как можно меньше. При этом соратники-пользователи объединены общей идеей, но преследуют разные цели. Возникающая в таких случаях неразбериха может привести к серьезным конфликтам.

Юмор

Если в такой ситуации не будут приняты соответствующие меры по разграничению доступа и полномочий, то в лучшем случае у Вас может оказаться список телефонов чьих-то любовниц, а в худшем — потеряете всю информацию, что нажита непосильным трудом.

Из всех неприятностей произойдет именно та, ущерб от которой больше...





Прежде чем начать разговор о возможных путях организации зашиты информации (ЗИ), необходимо определиться, имеется ли у Вас информация, которую нельзя не защищать; это важно, поскольку, как правило, ЗИ потребует дополнительных средств и достаточно больших.

СЗИ — довольно дорогостоящее удовольствие (а чаще необходимость). И если после долгих колебаний и споров решено, что в ИС имеет место информация, которую необходимо защищать, не расстраивайтесь. Смело идите вперед.

Далее необходимо определить конкретные сведения, подлежащие защите, для чего и от кого их защищать, а так же степень надежности такой защиты — проделать это не сложно.

После этого следует выявить потенциальные угрозы и наиболее вероятные каналы утечки информации для конкретных условий. Их может оказаться достаточно много, но не стоит огорчаться, так как злоумышленник не будет их использовать все сразу.

Следующим шагом будет выбор из множества предлагаемых вариантов таких методов, мероприятий и средств, которые можно было бы использовать конкретно в Вашей ИС.

После того как удалось найти конкретные варианты организационных и технических решений, необходимо подсчитать затраты на их реализацию. Вот здесь можно и огорчиться. Сомнения и чувство досады, возникающие в такие моменты — это вполне нормальное явление. Часто при этом всплывают воспоминания о том, как спокойно жилось, пока проблемы защиты информации не были Вам знакомы.

Но рано или поздно наступает момент, когда становится ясно: как бы мы этого не хотели, а придется выложить дополнительные средства на организацию защиты своих данных. Было бы неплохо, чтобы такая мысль пришла пораньше, поскольку построить систему защиты информации для готовой (законченной) информационной системы можно лишь путем введения целого ряда ограничений, а это, естественно, снижает эффективность функционирования информационной системы в целом.

Лучше всего анализировать опасности еще на стадии проектирования рабочего места, локальной сети или всей системы, чтобы сразу определить потенциальные потери и установить требования к мерам обеспечения безопасности.

Выбор защитных и контрольных мероприятий на этой ранней стадии требует гораздо меньших затрат, чем выполнение подобной работы с эксплуатируемой компьютерной системой.

Кстати

Чаще всего бывает достаточно анализа возможных опасностей, чтобы осознать проблемы, которые могут проявиться во время работы. Недаром эксперты по безопасности компьютерных систем часто подчеркивают, что проблемы ЗИ в значительной степени являются социальными, и если эти проблемы загонять внутрь, они могут "выйти боком". Все усилия и средства по защите информации должны быть объединены в стройную систему защиты информации, работающую по принципу: "копейка рубль бережет".

Современные популярные и доступные широкому кругу пользователей персональные компьютеры в действительности не обеспечивают безопасность информации, поскольку любой, кто имеет доступ к компьютеру, может изменять, читать или копировать данные. Изначально ПК были созданы для решения бытовых и

офисных задач и не предназначались для обработки секретной или конфиденциальной информации.

Несколько позднее на базе таких ПК появились локальные сети, а вместе с ними — и "головная боль" от проблем защиты информации. Конечно, решить все эти проблемы непросто. Но, как говорится, вместо того, чтобы хвататься за голову, необходимо просто взяться за ум.

Создание СЗИ можно сравнить с пошивом костюма. При наличии обязательных составляющих (брюки, пиджак, рукава, воротник...) имеется множество фасонов (вариантов покроя), при этом необходимо учитывать индивидуальные особенности каждого заказчика (пропорции тела, вкусы, привычки...). В итоге все стремятся получить удобную, практичную, качественную, красивую, современную вещь.

Серьезная работа по практическому использованию информационных технологий началась сравнительно недавно. Широкий выбор разнообразного аппаратного и программного обеспечения позволяет построить ИС под свои конкретные задачи. Но, как это часто бывает, наблюдается существенный разрыв между тем, что мы имеем в своем распоряжении и тем, что мы можем из этого извлечь... Иначе говоря, компьютер можно использовать не только в качестве неплохой пишущей машинки.

Но самое интересное в том, что чем дольше процесс освоения информационных технологий, тем чаще возникает проблема обеспечения сохранности информации и однажды наступает момент, когда становится ясно, что какого бы высокого уровня ни достигла в своем развитии ИС, проблему ЗИ все-таки придется решать.

Было бы неплохо, если бы такая мысль пришла пораньше, поскольку построить СЗИ для (готовой) законченной ИС можно лишь путем введения целого ряда ограничений, а это, естественно, снижает эффективность ИС в целом.

Давно известно, что рыть траншею и прокладывать кабель (или трубы) желательно до того, как в этом месте положат асфальт. Так и СЗИ целесообразно строить одновременно с ИС, начиная с этапа проектирования.

А можно ли сэкономить на своей информационной безопасности? Да, можно! Но стоить это будет дороже!

А если говорить серьезно, то хорошие аппаратные и программные средства защиты информации стоят значительно дороже, и ошибка кроется в том, что их реальную стоимость отождествляют с ценой при покупке. В дальнейшем такая экономия обернется дополнительными расходами в процессе эксплуатации (на доделки, ремонты, потери от отказов и сбоев в процессе старения). Это легко подсчитать, но побеждает странная надежда, что все эти расходы ожидаются в будущем, когда мы разбогатеем. Хотя жизнь упорно подтверждает, что богатеет тот, кто изначально ориентируется на самое лучшее. Мы же зачастую пытаемся экономить на спичках... Вот и приходится тратить неоправданно большие средства на организацию защиты дорогой и ценной информации, которая обрабатывается с помощью бытовой (дешевой) вычислительной техники.

Кстати

Впрочем, для получения важной информации не обязательно использовать приемы Джеймса Бонда. Грамотно проведенный анализ больших объемов несекретной информации позволяет получить ответы на любые вопросы секретного характера. Вот почему наряду с известными всем АНБ, ЦРУ и ФБР в США успешно функционируют аналитические службы министерств торговли, энергетики, финансов и другие, которые тесно сотрудничают с многочисленными международными статистическими организациями. Информация, добытая таким простым путем, может быть использована для выработки экономической, торговой или финансовой политики по отношению к интересующим государствам.

Развернувшийся процесс конверсии сопровождается созданием на базе оборонных предприятий различных научно-технических центров, акционерных обществ, совместных предприятий. Уникальные конструкторские и технологические разработки, которые ранее использовались исключительно для выпуска оборонных изделий, стали основой для выпуска наукоемкой, конкурентоспособной продукции и охотно приобретаются предпринимателями, правда, за бесценок.

Таким образом, большую часть информации, которую мы "дарим" всем желающим, в цивилизованном мире либо продают, либо предоставляют в урезанном виде.

Следует признать, что в настоящее время существует некоторое недопонимание проблем защиты информации со стороны государственных министерств и ведомств, а также негосударственных и коммерческих структур. Ссылаясь на экономические трудности, они откладывают решение вопросов защиты информации на второй план. Хотя логика говорит, что системы защиты должны развиваться одновременно с информационными системами, начиная с этапа проектирования.

Резюме

Опыт проектирования систем защиты еще не достаточен. Однако уже можно сделать некоторые обобщения. Погрешности защиты могут быть в значительной мере устранены, если при проектировании учитывать основные *принципы построения системы защиты:*

Генеральным направлением поиска путей защиты информации является неуклонное повышение системности подхода к самой проблеме защиты информации. Понятие системности интерпретировалось прежде всего в том смысле, что защита информации заключается не просто в создании соответствующих механизмов, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла систем обработки данных при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для защиты информации, непременно и наиболее рациональным образом объединяются в единый целостный механизм — систему защиты, которая должна обеспечивать, говоря военным языком, глубокоэшелонированную оборону, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала.

***Основные правила*,** которыми рекомендуют руководствоваться специалисты при организации работ по защите информации, сводятся к следующему:

1. Обеспечение безопасности информации есть непрерывный процесс, состоящий в систематическом контроле защищенности, выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

2. Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

3. Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты.

4. Никакую систему защиты нельзя считать абсолютно надежной, следует исходить из того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

Существуют следующие представления защищенности ИС:

защищенность это совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС;

защищенность это минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС;

защищенность это комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС.

Защищенной ИС будем называть ИС, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой ИС.

При этом механизмы выполнения указанных правил чаще всего реализуются в виде *системы защиты информации*.Следовательно, *под СЗИ будем понимать* совокупность механизмов защиты, реализующих установленные правила, удовлетворяющие указанным требованиям.

Выбор защитных и контрольных мероприятий на этой ранней стадии требует гораздо меньших затрат, чем выполнение подобной работы с эксплуатируемой компьютерной системой.

Чаще всего бывает достаточно анализа возможных опасностей, чтобы осознать проблемы, которые могут проявиться во время работы. Недаром эксперты по безопасности компьютерных систем часто подчеркивают, что проблемы ЗИ в значительной степени являются социальными, и если эти проблемы загонять внутрь, они могут “выйти боком”. Все усилия и средства по защите информации должны быть объединены в стройную систему защиты информации, работающую по принципу: “копейка рубль бережет”.