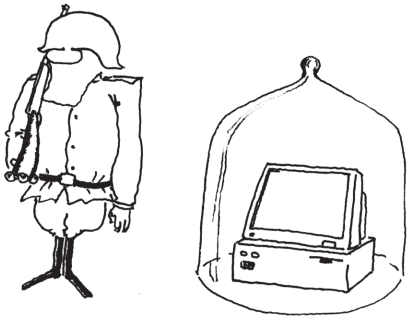
Информационная система как объект защиты

В этой главе

- *Что такое информационная система*
- *ИС всякие нужны, ИС всякие важны…*
- *Разработка и производство информационных систем*
- *Структура ИС и принципы ее функционирования*
- *Типовые компоненты ИС*
- *Проблемы защиты локальных сетей*
- *Проблемы защиты открытых систем клиент/сервер*
- *Проблемы интеграции систем защиты*

<<< 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

Информационная система как объект защиты...



В современной динамичной обстановке возникают проблемы, связанные с повышением эффективности и качества управления. Очевидно, что без достаточного информационного обеспечения невозможно принимать правильные решения, которые непосредственно влияют на судьбу предприятия или организации, на его развитие и жизнеспособность. Обстановка постоянно изменяется, число решений растет, их последствия все сложнее прогнозировать, а цена ошибки с каждым днем повышается.

Одним словом, информация представляет собой незаменимое сырье для выработки любого решения, такое же сырье, как и любое другое, которое необходимо добыть, переработать и поставить до истечения срока годности тому, кому оно необходимо. Все это определяет необходимость внедрения сложных систем сбора, обработки и анализа различной информации. Ценные сведения, добываемые с большим трудом, должны вовремя поступить тому, кому они необходимы, поскольку информация полезна только тогда, когда ее можно использовать для принятия серьезных решений.

Что такое информационная система (010)

Учитывая, что предлагаемый материал рассчитан на широкий круг читателей и не претендует на статус научного трактата, введем некоторые понятия:

Информационная система **(ИС)** — организационно-техническая система, реализующая информационные технологии и предусматривающая аппаратное, программное и другие виды обеспечения, а также соответствующий персонал.

Под информационной системой можно также понимать автоматизированную систему, предназначенную для организации, хранения, пополнения, поддержки и предоставления пользователям информации в соответствии с их запросами.

Определение

Другими словами информационная система — это сложная распределенная в пространстве система, состоящая из множества сосредоточенных (локальных) подсистем (информационных узлов), располагающих программно-аппаратными средствами реализации информационных технологий, и множества средств, обеспечивающих соединение и взаимодействие этих подсистем с целью предоставления территориально удаленным пользователям широкого набора услуг из сферы информационного обслуживания.

Таким образом, термин "*информационная система*" может быть отнесен к весьма широкому классу систем, от простейших ("телефон — секретарь — компьютер — база данных") до "ситуационного центра Президента".

Целью любой информационной системы, независимо от области ее применения, программного и аппаратного обеспечения, является предоставление полной, достоверной и своевременной информации.

Информационные системы можно разделить на две основные группы: системы информационного обеспечения и системы, имеющие самостоятельное целевое назначение и область применения.

Системы (или подсистемы) информационного обеспечения входят в состав любой ИС. Они — важнейшие компоненты интенсивно развиваемых в настоящее время систем интегральной автоматизации производственных систем, систем автоматизированного проектирования, автоматизированных систем научных исследований и др.

К числу ИС самостоятельного значения относятся информационно-поисковые (ИПС), информационно-справочные (ИСС) и информационно-управляющие системы. Информационно-поисковые и информационно-справочные системы предназначены для хранения и представления пользователю информации (данных, фактографических записей, текстов, документов и т.п.) в соответствии с некоторыми формально задаваемыми характеристиками.

Для ИПС и ИСС характерны два этапа функционирования:

- сбор и хранение информации;
- поиск и выдача информации пользователю.

Движение информации в таких системах осуществляется по замкнутому контуру от источника к потре-

бителю. При этом ИПС или ИСС выступает лишь как средство ускорения поиска данных.

Наиболее сложный процесс с точки зрения его реализации — поиск информации, осуществляемый в соответствии со специально издаваемым поисковым образом документа, текста и т.п. Для оценки смысловой релевантности вводятся критерии смыслового соответствия, а для оценки соответствия поисковых признаков (формальной релевантности) — критерии формального соответствия текстов, по которым осуществляется сравнение и определение соответствия найденных текстов запросам пользователей.

В зависимости от режима организации поиска ИПС и ИСС могут быть разделены на документальные, библиографические, библиотечные, фактографические.

Документальными называют информационно-поисковые системы, в которых реализуется поиск в информационном фонде ИПС документов или текстов в соответствии с полученным запросом с последующим предоставлением пользователю этих документов или их копий. Вся обработка информации в документальных ИПС осуществляется пользователем.

В зависимости от того, по каким хранимым документам или по их описаниям (вторичным документам) осуществляется поиск, документальные ИПС делят на системы с ***библиотечным*** или с ***библиографическим*** поиском. В первом случае поиск ведется в информационном фонде, содержащем первичные документы, во втором — в информационном фонде вторичных документов.

Заметим, что наибольшее практическое значение имеют документальные ИПС, поиск в которых организован по двум контурам: библиографическому, с определением основных характеристик первичного документа и предоставлением пользователю возможности оценить, может ли данный документ удовлетворить его информационные потребности, и библиотечному, когда в информационном фонде осуществляется нахождение требуемого документа с последующей его (или копии) выдачей пользователю.

Фактографические информационно-поисковые системы реализуют поиск и выдачу фактов, текстов, документов, содержащих сведения, которые могут удовлетворить поступивший запрос пользователя. В этом случае осуществляется поиск не какого-то конкретного документа, а совокупности сведений по данному запросу, хранящихся в информационном фонде ИПС или ИСС. Отметим, что основным отличием фактографических информационно-поисковых систем от документальных является то, что эти системы выдают пользователю не какой-либо ранее введенный документ, а уже в той или иной степени обработанную информацию.

Широкое применение в таких системах находят персональные компьютеры, локальные и распределенные сети, средства передачи данных и многие другие технические устройства. Они пронизали структуры ИС на всех уровнях и являются их неотъемлемой частью.

Информационные системы способствуют значительному повышению эффективности и скорости информационного обеспечения, однако при этом резко возрастает угроза сохранности информации. В недалеком будущем ИС станут составной частью жизни общества. Их неправильное функционирование может вызвать гибельные последствия для правительств, общества, бизнеса и отдельного гражданина (стоит лишь задуматься о последствиях неправильного функционирования электронной почты или банковской службы). Поэтому дальновидные руководители не жалеют средств на защиту нужной информации.

Основой для изучения теории ИС являются исходные положения теории информационных процессов.

Под информационным процессом в технике понимают совокупность взаимосвязанных и взаимообусловленных процессов выявления, анализа, ввода и отбора информации, ее передачи и обработки, хранения, поиска, выдачи, принятия решений и т.д.

Определение

Кроме того, ИС характеризуют:

- наличие прямых, обратных, многоканальных и разветвленных связей, а также процессов управления;
- сложность, понимаемая как принципиальная невозможность в полной мере, без дополнительных условий и ограничений, иметь адекватное формализованное описание;
- обилие разнообразных составляющих информационного процесса, распределенных в пространстве, непрерывно сменяющих друг друга во времени.

Информация — сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами. Информация может существовать в различных формах в виде совокупностей некоторых знаков (символов, сигналов и т.п.) на носителях различных типов.

Определение

Обработка информации...

Обработка информации в ИС – любая совокупность операций (прием, сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием технических средств ИС.

Специфичным для ИС является понятие структуры, которое раскрывает схему связей (физическая структура) и взаимодействия между элементами (логическая структура). Остановимся на этих понятиях.

Физическая структура ИС – это схема связей таких физических элементов, как технические средства, аппаратура узлов, собственно узлы и вычислительная техника, устанавливаемая в них. К основным компонентам физической структуры можно отнести узлы, каналы и линии связи.

Логическая структура ИС определяет принципы установления связей, алгоритмы организации процессов и управления ими, логику функционирования программных средств. В общем виде она определяет соединение и взаимодействие двух принципиально различных по назначению и функциям составных частей архитектуры ИС: множества автономных информационных подсистем (узлов) и множества средств их связи и взаимодействия (физических средств соединений).

Обобщенная геометрическая модель физической структуры ИС определяет *топологическую структуру* ИС.

Более конкретный состав аппаратно-программных средств и схема их связей называются также *конфигурацией* ИС.

Под *архитектурой ИС* будем понимать согласованность всевозможных структур ИС. Так, при некоторой логической структуре, соответствующей принятой архитектуре ИС, может быть построено множество физических структур, влияющих на свойства и возможности системы. В свою очередь, логическая структура ИС в достаточной мере определяет свойства архитектуры ИС в целом.

Информационный узел – это техническая или организационно-техническая система определенной сложности, осуществляющая те или иные заданные процессы (например, обработка и накопление поступающей информации, распределение по каналам и др.).

Узлы, в которых информация выходит за пределы системы или поступает в систему, называют конечными пунктами. Здесь устанавливаются технические средства, называемые терминалами ("абонентский" пункт).

Внутренние сетевые узлы – это обычно транзитные или в общем случае коммуникационные связные узлы. Соединение отдельных информационных узлов осуществляется с помощью различных каналов связи (проводных, беспроводных, комбинированных).

Группы людей или отдельные лица, пользующиеся услугами ИС называют пользователями.

ИС всякие нужны, ИС всякие важны... (010)

Уровень развития ИС определяют ***особенности сетевой архитектуры.*** К таковым относятся:

- применяемые в ИС методы распределения информации и установления связей между взаимодействующими системами;
- виды предоставляемых услуг;
- способы управления процессами;
- наличие средств защиты и обеспечения целостности данных и сохранности ресурсов;
- возможность организации связи с другими сетями и осуществления межсетевых переходов.

Известны два основных метода распределения информации — коммутация и селекция.

Коммутация осуществляется тремя способами: коммутацией каналов, сообщений или пакетов.

Селекция основывается на выбранном методе доступа взаимодействующих систем к передающей физической среде связи, в которой одновременно распространяется множество сигналов, формируемых несколькими взаимодействующими терминальными системами.

Виды услуг, предоставляемых ИС:

- установление связи — наиболее простой вид услуг, реализуемый средствами коммуникационной системы с помощью любого способа коммутации;
- передача данных. (Сеть оснащается аппаратурой и каналами передачи данных. Обеспечивает высокие скорости передачи и имеет лучшие качественные характеристики, чем коммуникационные системы других типов);
- телеобработка;
- передача файлов;
- доступ к распределенным базам данных и др.

Развитая архитектура ИС связана с наличием в ней сложной системы управления взаимодействующими процессами. Эта система обеспечивает необходимую эффективность функционирования ИС, управляет информационными потоками, предохраняет сеть от перегрузок, восстанавливает нормальные режимы функционирования в случаях возможных отклонений их от допустимых.

Определение

Ресурсы ИС — все компоненты ИС, ее аппаратное и программное обеспечение. Понятие ресурса может быть распространено и на другие компоненты ИС — процедуры, протоколы, управляющие структуры и т.п. Следовательно, понятие ресурса определяется в широком смысле.

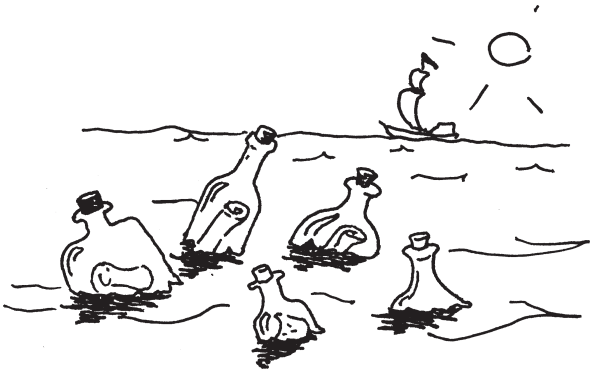
Пользователи ИС — это в первую очередь лица, имеющие соответствующий доступ в систему и использующие ресурсы ИС. Кроме того, в понятие "пользователь" можно включать и процессы, выполняемые на различных ресурсах ИС. Понятно, что поведение такого "пользователя" существенно отличается от поведения человека, но есть и некоторое сходство, если считать их активными компонентами сети.

В зависимости от вида средств, методов и алгоритмов управления можно выделить ИС с централизованным и распределенным управлением. При этом могут выполняться как жесткие (фиксированные), так и гибкие (адаптивные) алгоритмы управления ИС, учитывающие многочисленные факторы.

Средства защиты и обеспечения целостности данных и сохранности ресурсов являются важным аспектом функционирования системы. Вопросы защиты информации и ресурсов в ИС будут рассмотрены далее.

Объединение сетей осуществляется либо через общий узел, либо путем создания специальных каналов, соединяющих узлы одной системы с узлами другой. Если сеть может быть соединена с другими, то она называется открытой, если не может или не должна соединяться, то — закрытой. Закрытость системы (или ее части) для некоторой категории пользователей является одним из способов защиты информационных и вычислительных ресурсов системы.

По функционально-целевому и прикладному назначению существующие ИС можно разделить на две группы: общего пользования и специального назначения.



ИС общего назначения...

ИС общего пользования предназначены для различных сфер применения независимо от конкретного содержания данных, обрабатываемых в ИС. Средства, структура и функциональные возможности таких ИС оказываются одинаковыми для многих случаев применения и обеспечивают широкий диапазон услуг. Это, как правило, большие системы, использующие в качестве базовых коммуникационных подсетей государственные системы передачи данных. Практика использования сетей общего пользования привела к необходимости разработки программно-аппаратных средств, реализующих принципы открытости, универсальности сетей и типизации технических решений.

ИС специального назначения предназначены для решения задач в определенной предметной или ведомственной области.

Качество ИС можно оценить по следующим показателям:

- ***общее число связей ИС***; определяет потенциальную способность устанавливать взаимодействия между пользователями и распределенными ресурсами;
- ***временные характеристики качества ИС***; оценивают скорость обслуживания пользователя по следующим показателям: среднее время доступа, зависимое от размеров системы, удаленности пользователей, загрузки

системы запросами, поступающими от других пользователей;

- ***среднее время обслуживания***, показывающее время, затрачиваемое на обработку запроса пользователя в том или ином режиме и др.;
- ***надежность обслуживания***; характеризуется вероятностью безотказной работы ИС при взаимодействии с ней пользователя, удобством доступа в обслуживании, а также наличием средств диагностики и резервирования, применяемых для улучшения качества обслуживания и повышения надежности;
- ***достоверность передачи***, сохранность и целостность информации;
- ***возможность доступа*** к информационным и вычислительным ресурсам; обеспечивается математическими средствами и протоколами, гарантирующими функции вызова и активизации запрашиваемых ресурсов с учетом полномочий пользователя.

Целостность — свойство информации, состоящее в ее существовании в неискаженном виде, неизменном по отношению к некоторому фиксированному ее состоянию.

Определение

Конфиденциальность — свойство информации, состоящее в том, что она не может быть обнаружена и стать доступной без разрешения отдельным лицам, модулям или процессам.

Доступность информации — свойство системы (среды, средств и технологии ее обработки), в которой циркулирует информация, характеризуемое способностью обеспечивать своевременный беспрепятственный доступ к интересующей информации, когда в этом возникает необходимость;

При проектировании и анализе ИС существенное значение имеет ее топологическая структура, т.е. схематично представленные данные о множестве физических элементов системы, их распределении и связях.

Более строго, **топология ИС** — это схема взаимного расположения узлов, конечных пунктов, коммутационных устройств и других физических элементов ИС, которая путем указания направлений и линий связи определяет потенциальные возможности передачи и обмена информацией между элементами ИС.

Топологическая структура может быть представлена в виде геометрической модели на плоскости или в пространстве.

По топологической структуре все ИС можно разделить на системы с централизованной или децентрализованной структурой, т.е. такие, в которых имеются центральные узлы или нет.

Важным топологическим признаком будет количество связей одних узлов с другими. В зависимости от этого системы будут либо односвязные (древовидные), либо многосвязные.

Разработка и производство информационных систем (001)

Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков. Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

Средства обеспечения информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;

Собственник информационных ресурсов, ИС, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам. Собственник информационной системы, технологии и средств их

обеспечения обязан защищать права их автора в соответствии с законодательством

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в установленном порядке.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется соответствующим законодательством.

Структура ИС и принципы ее функционирования (010)

Основой современных ИС, как правило, являются территориально распределенные компьютерные системы (вычислительные сети) интенсивно взаимодействующие. Основу аппаратных (технических) средств таких систем составляют ЭВМ (группы ЭВМ), периферийные, вспомогательные устройства и средства связи, сопрягаемые с ЭВМ. Состав программных средств определяется возможностями ЭВМ и характером задач, решаемых при обработке информации.

Структурная схема ИС представлена на рис. 2.1.

Из множества компонентов ИС для рассмотрения в данной работе выделим следующие объекты, которые в свою очередь могут быть разбиты на соответствующие составные элементы:

- локальная сеть;
- каналы и средства связи (КС);
- узлы коммутации;
- условный кабинет руководителя (либо любое другое помещение, где для обработки информации используются различные технические средства);
- рабочее место удаленного (легального) пользователя системы;
- рабочее место постороннего пользователя (потенциального злоумышленника);
- носители информации (магнитные, оптические и др.);
- печатающая и множительная техника;
- отдельные ПК и рабочие станции (терминалы);
- и наконец, непосредственно пользователи (обыкновенные люди).

Такую схему можно расширить, добавив другие устройства, например рабочее место специального назначения, каналы цифровой связи и т.п.

Основу технических средств ИС составляет обычно ЭВМ высокой производительности. Комплекс средств сбора и выдачи информации выполняет функции связи и общения между ИС и внешней средой — отдельными пользователями, технологическими процессами, другими ИС и т.д.

При значительном удалении абонентов ИС от вычислительных средств информация принимается и выдается по телефонным, телеграфным или широкополосным каналам связи.

Комплекс сбора и выдачи информационно связан с внешними запоминающими устройствами ИС, управление которыми обычно осуществляется специализированной ЭВМ, распределяющей потоки данных и каналы памяти в соответствии с приоритетом источников заявок. Центральные процессоры выполняют обработку информации в ИС, а быстродействующая основная память обеспечивает хранение программ и данных решаемых задач.

Связь и передачу информации в ИС обеспечивает устройство коммутации (коммутационный центр).

Определяющее значение для организации эффективного функционирования ИС имеет ее программное обеспечение.

Основными особенностями распределенных ИС являются:

- территориальная удаленность компонентов системы друг от друга и интенсивный обмен информацией между ними;
- широкий спектр используемых информационных технологий;
- интеграция данных различного назначения, принадлежащих разным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;
- абстрагирование пользователей и владельцев данных от физических структур и места размещения данных;
- использование режимов распределенной обработки данных;
- участие в процессе функционирования ИС большого количества пользователей и персонала;
- одновременный доступ к ресурсам ИС большого числа пользователей (субъектов) различных категорий;
- высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;
- отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в ИС.

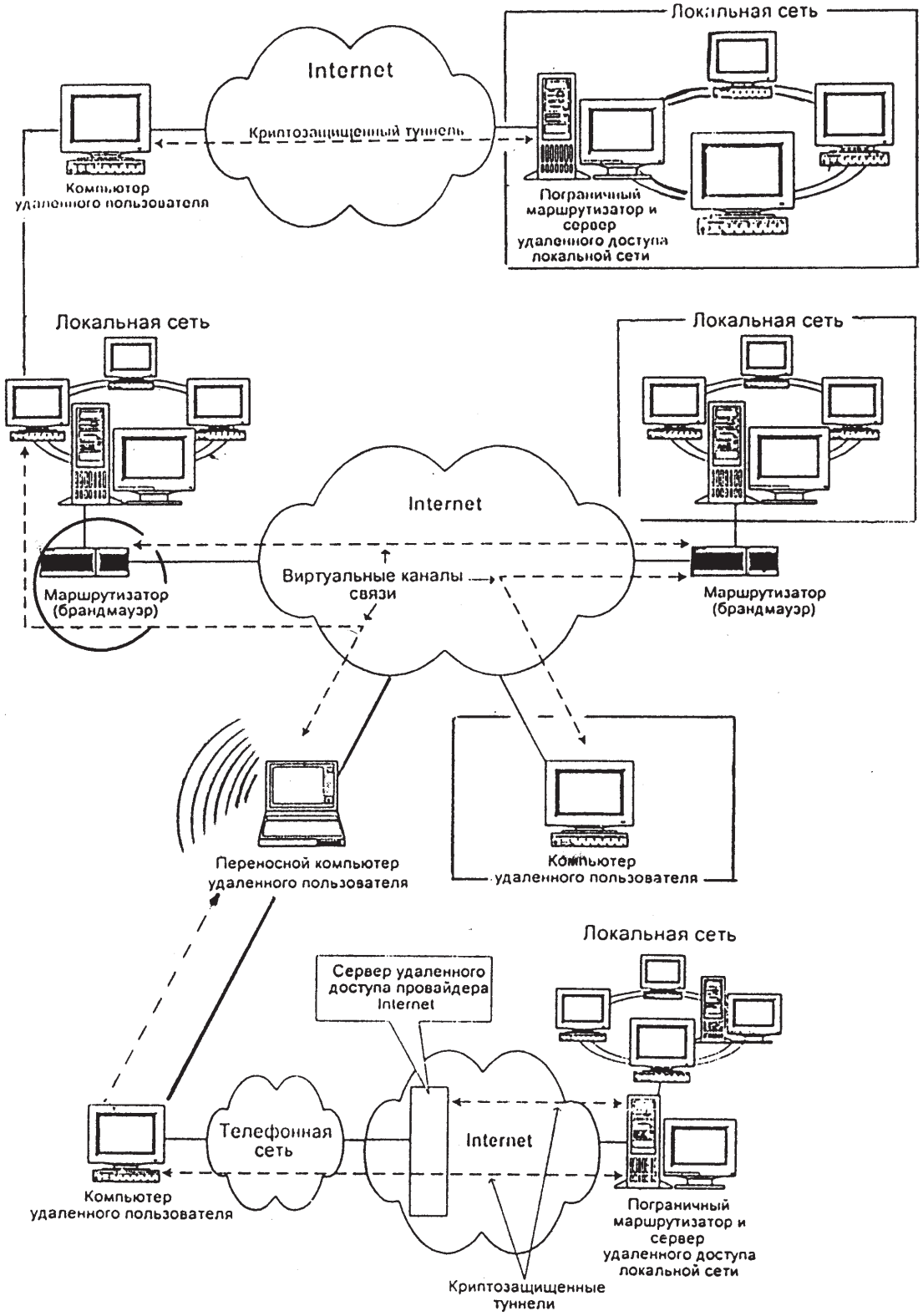


РИС. 2.1. *Структурная схема ИС*

Типовые компоненты ИС (010)

В зависимости от форм и способов организации ИС можно выделить **основные типовые компоненты**, позволяющие описать любую ИС.

Типовые компоненты определяют структуру ИС...

Рабочие места пользователей и персонала ИС

Можно выделить следующие ***типы рабочих мест:***

- пользователя дисплейного (непрограммируемого) типа с визуальным отображением информации;
- пользователя (программируемый ПК), который может функционировать в режиме обмена информацией с сопряженной ЭВМ и в автономном режиме;
- оператора, предназначенное для обслуживания серверов;
- программиста, предназначенное для отладки программы;
- администратора, предназначенное для управления и контроля за использованием каких-либо ресурсов ИС, например администраторы сети, базы данных, службы безопасности.

Связные компоненты (010):

- межсетевые мосты (шлюзы, центры коммутации пакетов, коммуникационные ЭВМ) — элементы, обеспечивающие соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналы связи с узлами коммутации;
- аппаратура связи типа модем (модулятор-демодулятор), осуществляющая преобразование цифровых данных в электрические сигналы для передачи по линиям связи и обратное преобразование на приеме при обмене между удаленными друг от друга ЭВМ;
- аппаратура связи типа мультиплексор передачи данных (МПД), обеспечивающая сопряжение нескольких источников (например, нескольких ЭВМ) для передачи информации по одному каналу связи;
- каналы связи, выделенные и коммутируемые.

Вспомогательные элементы ИС (010):

- помещения, в которых размещены внешние запоминающие устройства больших ЭВМ;
- помещения, в которых размещены устройства предварительной подготовки данных;
- хранилище машинных носителей информации;
- хранилища документов на бумажных носителях;
- служебные помещения пользователей и персонала ИС.

С точки зрения защиты информации типовые компоненты ИС рассматриваются как объекты защиты.

ЭВМ различного функционального назначения (010):

- центральная ЭВМ (мейнфрейм), которая осуществляет основные процедуры обработки информации в ИС;
- сервер или Host машина — высокопроизводительная ЭВМ, предназначенная для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п.;
- ЭВМ с функциями связной машины, шлюза, моста между сетевыми структурами.

Проблемы защиты ИС (010)

Следует признать, что в качестве базового уровня ИС применяются обычные (бытовые) ПК, которые в последующем объединяют с помощью дополнительного оборудования в локальные и распределенные вычислительные сети.

С точки зрения защиты информации при таком подходе приходится тратить неоправданно большие средства на организацию защиты ценной информации, обрабатываемой с помощью дешевой техники. И поскольку в условиях, когда пользователи имеют доступ к нескольким серверам и базам данных и даже обладают правами удаленной регистрации, защита настолько усложняется, что ее создание становится не по карману даже мощным фирмам; однако в силу мнимой экономии денежных средств по такому пути идут как коммерческие, так и государственные организации.

Проблемы защиты...

Возможно ли в таких условиях организовать защиту информации? Ответить на этот вопрос не просто. Безусловно, современная политика в области развития информационных технологий, делающая ставку на открытость систем, крайне затрудняет выполнение поставленной задачи. Действительно, когда структуры, алгоритмы, текст операционной системы опубликованы, попробуй защити ПК или открытую сеть от несанкционированного доступа (НСД).

Бытует мнение, что все изложенное относится только к операционной системе MS-DOS, а вот коммерческий UNIX лишен этого недостатка. Такой взгляд ошибочен. И система MS-DOS, и системы WINDOWS, OS/2 и WINDOWS NT, и разновидности UNIX — все они в той или иной мере открытые системы.

По мнению многих специалистов, будущее систем защиты — это централизованное управление и единственные "точки выхода" для пользователей. Сервер санкционирования или единый сервер паролей содержит не только БД паролей, но и правила ограничения прав и доступа. В таких централизованных системах администратор может управлять доступом и проверкой полномочий из одного пункта.

Таким образом, единственный способ обеспечить безопасность компьютерных сетей — это заставить все средства защиты работать как единое целое. Такой подход позволит сотрудникам, отвечающим за защиту информации, сосредоточить все средства на одной рабочей станции, которую можно будет предоставлять для доступа под жестким контролем. Программа контроля должна содержать общий набор средств для защиты распределенных ресурсов и одновременно позволять работать с прежней системой.

В ИС можно скрыто получить доступ к информационным архивам, которые концентрируются в одном месте в больших объемах. Кроме того, появилась возможность дистанционного получения информации через терминалы, расположенные в удалении от мест хранения данных. Поэтому для защиты информации требуются принципиально новые методы и средства, разработанные с учетом ценности информации, условий работы, технических и программных возможностей ИС и других средств сбора, передачи и обработки данных. Особые мероприятия защиты необходимы, когда ресурсы ИС используются несколькими абонентами через терминалы в многопрограммном режиме и в режиме разделения времени. В этом случае возникает ряд правовых проблем, связанных с массивами информации, представляющих собой общественную и национальную ценность. Использование такой информации не по назначению наносит значительный ущерб как обществу в целом, так и отдельной личности.

В ИС принято устанавливать и строго соблюдать регламент доступа в различные служебные помещения для разных категорий сотрудников.

Степень защиты информации от неправомерного доступа и противозаконных действий зависит от качества разработки организационных мер, направленных на исключение:

- доступа к аппаратуре обработки информации;
- бесконтрольного выноса персоналом различных носителей информации;
- несанкционированного введения данных в память, изменения или стирания хранящейся в ней информации;
- незаконного пользования системами обработки информации и полученными данными;
- доступа в системы обработки информации посредством самодельных устройств;
- неправомочной передачи данных по каналам связи из информационно-вычислительного центра;
- бесконтрольный ввод данных в систему;
- обработка данных по заказу без соответствующего требования заказчика;
- неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Основными проблемами в процессе защиты информации в ИС является:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- гарантия прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Некоторые проблемы защиты информации представлены на рис. 2.2.

Проблемы защиты открытых систем клиент/сервер (023)

Открытые системы клиент/сервер подкупают администраторов ИС исключительно простым доступом к корпоративной информации, но обескураживают сложностью решения задач защиты данных в связи с разнородностью вычислительных компонентов — аппаратных платформ, операционных систем, СУБД и прикладного ПО.

Проблема не только в том, чтобы добиться согласованной работы средств защиты различных звеньев, но и упростить жизнь рядовых пользователей, дабы не заставлять их в поисках нужных данных продираться через множество заградительных кордонов.

Сторонники архитектуры клиент/сервер получили возможность исключительно простого доступа к корпоративным данным. Однако это осложнило проблему безопасности, что в полной мере почувствовали администраторы информационных систем на больших машинах. Для них понятия “открытая система” и “безопасность” казались вообще несовместимыми.

На мэйнфреймах обеспечение безопасности данных всегда стояло на первом месте и проблемы защиты информации фактически были решены: имелись эффективные программы защиты и в каждом вычислительном центре был специально выделенный персонал, который с помощью этих средств и поддерживал безопасность системы.

Пользователи локальных сетей вспоминали о существовании средств защиты редко — в момент ввода сетевых паролей. При столь неразвитых инструментах защиты администраторы ЛС, естественно, не очень серьезно относились и к проблеме компьютерной защиты.

Когда закрытая хост-система интегрируется с локальными сетями и серверами баз данных, ее пользователи страдают не столько от недостатка средств защиты, сколько от их избытка и несовместимости. В дополнение к собственным средствам защиты для мэйнфреймов появляются системы защиты мониторов транзакций, локальных сетей и серверов БД. Созданные разными производителями, как правило, они не приспособлены для кооперативной работы.

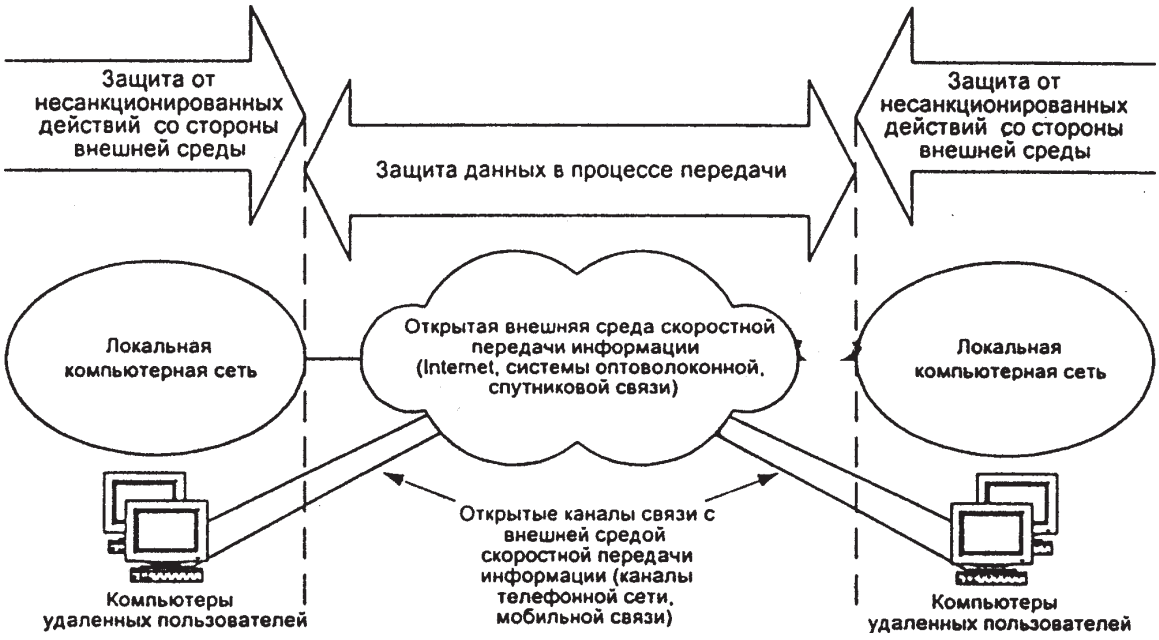


РИС. 2.2. *Проблемы защиты информации в ИС*

Таким образом, возникает необходимость синхронизировать работу средств безопасности всех платформ. При этом возникает фрагментация ответственности, когда для ухода за каждой платформой назначается отдельный администратор, а система в целом остается беззащитной.

Распределенная система имеет несколько точек входа, через которые осуществляется доступ к данным. Это могут быть файл-серверы локальной сети, рабочие станции и серверы БД. Чем больше в системе таких входов, тем острее проблема безопасности.

Уровень защиты всей системы определяется степенью защиты ее самого уязвимого звена, которым, как правило, являются включенные в сеть персональные компьютеры. Многие производители СУБД, стараясь облегчить жизнь конечных пользователей, перекладывают функции контроля доступа к данным на операционные системы. Возникающей лазейкой охотно пользуются хакеры, маскируясь под клиентов.

Защита для открытых ИС (023)

Процесс обеспечения БИТ появляется не тогда, когда случилось первое нарушение, а когда идет формирование будущей компьютерной системы. Он начинается с составления спецификаций на приобретаемое оборудование и программное обеспечение для ИС.

Как правило, заказчик хочет получить определенный набор сервисов. Назовем их основными. Например: система автоматизации офиса, бухгалтерская система, электронный документооборот и т.п.

Однако, чтобы основные сервисы могли функционировать, необходимо приобрести ряд вспомогательных сервисов. Имеются в виду серверы баз данных, почтовые серверы, сетевые сервисы, мониторы транзакций и т.д. Операционные системы и оборудование также можно отнести к вспомогательным сервисам.

Когда определены все необходимые основные и вспомогательные сервисы, следует проанализировать информационные потоки между ними. Это важно, чтобы проконтролировать взаимную совместимость сервисов и сформулировать требования к пропускной способности коммуникационных каналов.

В защите нуждаются все сервисы и коммуникационные пути между ними. В то же время, не все запланированные сервисы обладают полным набором механизмов безопасности. Для каждого сервиса основные цели, а именно: конфиденциальность, целостность и доступность, трактуются по-своему.

Целостность с точки зрения системы управления базами данных и с точки зрения почтового сервера — понятия принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты.

Следует анализировать защищенность сервисов, функционирующих в сети. Часто для разных сервисов защиту строят по-разному. Например, обычно межсетевые экраны свободно пропускают через себя почтовый трафик — почта является относительно безобидным сервисом, но контролируют попытки доступа к другим, более мощным или более уязвимым сервисам.

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы. Это обычно осуществляется разрешением пользователю присоединить некоторую файловую систему (или каталог) к рабочей станции пользователя для дальнейшего использования в качестве локального диска. Однако сервер может обеспечить защиту доступа только на уровне каталога, поэтому если пользователю разрешен доступ к каталогу, то он получает доступ ко всем файлам, содержащимся в этом каталоге. Чтобы минимизировать риск в этой ситуации, важно соответствующим образом структурировать и управлять файловой системой ИС.

Следующая проблема заключается в неадекватных механизмах защиты локальной рабочей станции. Например, ПК может обеспечивать минимальную защиту или не обеспечивать никакой защиты информации, хранимой на нем. Копирование пользователем файлов с сервера на локальный диск ПК приводит к тому, что файл перестает быть защищенным теми средствами защиты, которые защищали его, когда он хранился на сервере. Для некоторых типов информации это может быть приемлемо. Однако другие типы информации могут нуждаться в более сильной защите. Эти требования фокусируются на необходимости контроля среды ПК.

Удаленные вычисления должны контролироваться таким образом, чтобы только авторизованные пользователи могли получать доступ к удаленным компонентам и приложениям. Серверы должны обладать способностью аутентифицировать удаленных пользователей, запрашивающих услуги или приложения. Эти запросы могут также выдаваться локальными и удаленными серверами для взаимной аутентификации.

Невозможность аутентификации может привести к тому, что и неавторизованные пользователи будут иметь доступ к удаленным серверам и приложениям. Должны существовать некоторые гарантии в отношении целостности приложений, используемых многими пользователями.

Современные топологии и протоколы требуют, чтобы сообщения были доступны большому числу узлов при передаче к желаемому назначению. Это гораздо дешевле и легче, чем иметь прямой физический путь между каждой парой машин. Вытекающие из этого возмож-

ные угрозы предусматривают как активный, так и пассивный перехват сообщений, передаваемых в линии.

При пассивном перехвате происходит не только чтение информации, но и анализ трафика (использование адресов, других данных заголовка, длины сообщений и частоту сообщений).

При активном — изменение потока сообщений (включая модификацию, задержку, дублирование, удаление или неправомочное использование реквизитов).

Службы Обмена сообщениями увеличивают риск для информации, хранимой на сервере или передаваемой между источником и отправителем. Неадекватно защищенная электронная почта может быть легко перехвачена, изменена или повторно передана, что влияет как на конфиденциальность, так и на целостность сообщения.

Прочие проблемы безопасности ИС:

- неадекватная политика управления и безопасности ИС;
- отсутствие обучения особенностям использования ИС и защиты;
- неадекватные механизмы защиты для рабочих станций;
- неадекватная защита в ходе передачи информации.

Необходима формальная политика безопасности, которая определяла бы правила использования ИС.

Политика безопасности является сжатой формулировкой позиции высшего руководства по вопросам информационных ценностей, ответственности по их защите и организационным обязательствам. Политика должна определять роль каждого служащего при обеспечении адекватной защиты ИС и передаваемой в ней информации.

Определение

Управление ИС должно иметь необходимые финансовые средства, время и ресурсы. Слабое управление сетью может привести к ошибкам защиты. В результате могут появиться следующие проблемы: ослабленная конфигурация защиты, небрежное выполнение мер защиты или даже не использование необходимых механизмов защиты.

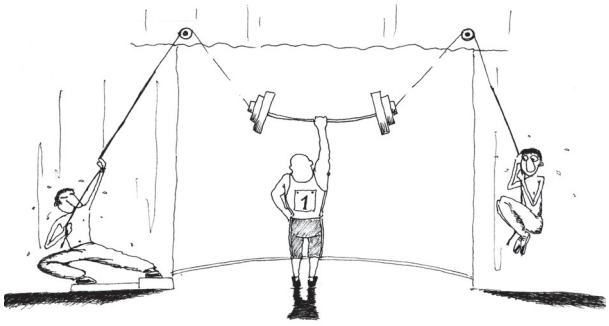
Пользователи, не знакомые с механизмами и мерами защиты могут использовать их неправильно и, возможно, небезопасно. Ответственность за внедрение механизмов и мер защиты, а также за следование правилам использования ПК в среде ИС обычно ложится на пользователей ПК. Пользователи должны иметь соответствующие инструкции и рекомендации, необходимые для поддержания приемлемого уровня защиты в среде ИС.

Будем защищать... или пусть живет? (200)

Архитектурно территориально-распределенная сеть представляет собой совокупность локальных вычислительных сетей (ЛВС/LAN) с архитектурой клиент/сервер и индивидуальных рабочих станций с правом удаленного доступа, объединенных базовой сетью, выделенных и коммутируемых каналов связи.

ИС предполагает автоматизацию подготовки и обмена разнообразными электронными документами. Подготовка документов ведется на рабочих станциях пользователей ИС, включенных в соответствующую ЛВС и функционирующих, как правило, по технологии клиент/сервер, в том числе на удаленных рабочих станциях, подключаемых к ЛВС через модем или факс-модем сервер.

В процессе формирования электронных документов пользователи используют общесетевые ресурсы файл-серверов, выделенных серверов баз данных и серверов приложений. Обмен электронными документами также предусматривает использование электронной почты и в ряде случаев — ручную доставку на носителях.



В распределенной ИС функции отдельных элементов взаимосвязаны...

Информация, обрабатываемая в ИС, в достаточной степени уязвима как перед случайными, так и перед злоумышленными дестабилизирующими факторами (угрозами), что вызывает потребность в защите информации.

Под ***защитой*** информации в ИС понимается регулярное использование средств и методов, принятие мер и осуществление мероприятий с целью системного обеспечения требуемой надежности информации, хранимой и обрабатываемой с использованием средств ИС.

Под ***надежностью*** информации в ИС понимается интегральный показатель, характеризующий качество информации с точки зрения:

1) ***физической целостности***, т.е. наличия (отсутствия) искажений или уничтожения элементов этой информации;

2) ***доверия к информации (аутентичности)***, т.е. наличия (отсутствия) в ней подмены (несанкционированной модификации) ее элементов при сохранении целостности;

3) ***безопасности информации (конфиденциальности)***, т.е. наличия (отсутствия) несанкционированного получения ее лицами или процессами, не имеющими на это полномочий;

4) ***недопущения несанкционированного размножения информации***. Эффективность защиты информации в ИС достигается лишь в том случае, если обеспечивается ее надежность на всех объектах и элементах системы, которые могут быть подвергнуты угрозам со стороны дестабилизирующих факторов.

Под ***объектом защиты*** понимается такой структурный компонент системы, в котором находится или может находиться подлежащая защите информация.

Объект защиты должен соответствовать следующим условиям:

- принадлежность к одному и тому же организационному компоненту ИС;
- участие в осуществлении одних и тех же функций, связанных с автоматизированной обработкой информации в ИС;
- локализация (ограничение) с точки зрения территориального расположения ИС.

Исходя из структуры ИС, к объектам защиты можно отнести:

- рабочие станции пользователей ИС;
- рабочие станции администраторов (сети, СУБД, системы защиты и др.);
- серверы (сетевые, баз данных, приложений);
- аппаратура связи (модемы, маршрутизаторы);
- каналы связи (выделенные, коммутируемые);
- периферийные устройства коллективного пользования (принтеры);
- помещения, связанные с автоматизированной обработкой информации (места установки оборудования, хранилища машинных носителей информации и т.п.).

Под ***элементом защиты*** подразумевается находящаяся в ИС совокупность данных, которая может содержать подлежащие защите сведения.

Элементы защиты специфицируются, как правило, для каждого отдельного объекта защиты. Так, по признаку локализации можно выделить следующие основные элементы защиты данных:

- обрабатываемых в ЭВМ;
- на дискете;
- на локальном жестком диске рабочей станции;
- на жестком диске сервера;
- обрабатываемые в аппаратуре связи;
- передаваемые по каналу (линии) связи;
- данные, выводимые из ЭВМ на периферийные устройства.

Сложность решения задач защиты информации в ИС характеризуется следующими факторами:

- предъявляются высокие требования к целостности системного и прикладного ПО, СУБД и целого ряда электронных документов (справочные, статистические, отчетные документы и инструкции);
- работа в территориально-распределенной сети предъявляет высокие требования к аутентичности информации и источников данных;
- переход на безбумажную технологию требует обеспечения юридической значимости электронных документов;
- распределенное использование ресурсов ИС требует обеспечения безопасности информации на уровне разграничения доступа;
- ряд электронных документов требует обеспечения безопасности на уровне скрытия смыслового содержания, а в некоторых случаях и недопущения несанкционированного размножения.

Не надо нас пугать... (200)

ИС могут быть очень сложными и содержать широкий спектр вычислительных ресурсов — от одиночных устройств до связок неоднородных ЭВМ (групп ЭВМ), функционирующих в условиях множественных полномочий. Соответственно и типы угроз могут изменяться в широких пределах в зависимости от состава ИС.

В процессе эксплуатации таких информационных систем, накапливаемая и обрабатываемая информация является достаточно уязвимой, подверженной как разрушению, так и несанкционированному использованию.

Наиболее ***распространенными путями утечки информации*** являются:

- хищение носителей информации и документов, получаемых в результате работы информационных систем;
- копирование информации на ПК;
- несанкционированное подключение к аппаратуре и линиям связи;
- перехват электромагнитных излучений в процессе обработки информации. Кроме того, пользователи ИС могут допускать различные ненамеренные ошибки и быть предметом злоупотреблений.

В настоящее время большая концентрация массивов информации, отсутствие элементарного контроля за ее сохранностью и относительно низкий уровень надежности технических средств вызывают серьезную тревогу в обеспечении сохранности информации.

С появлением ИС, работающих в режиме реального времени значительно возросло число лиц, имеющих доступ к вычислительным средствам. Это пользователи, системные и прикладные программисты, обслуживающий и административный персонал. Совершенствование технологии обработки информации привело к созданию информационных баз данных, содержащих большие объемы разнообразной информации, что также предъявляет дополнительные требования к обеспечению сохранности информации.

Современные информационные системы обеспечивают одновременный доступ к вычислительным ресурсам для многих пользователей с территориально удаленных рабочих мест. В связи с этим возникла и новая проблема обеспечения сохранности программ и данных пользователя от неавторизованного воздействия со стороны других пользователей информационной системы во время передачи информации по каналам связи.

Характеристики, влияющие на безопасность информации (200)

Рассматривая ИС как объект защиты, полезно обратить внимание на следующие характеристики:

- категории обрабатываемой в ИС информации, высший гриф секретности информации;
- общая структурная схема и состав ИС (перечень и состав оборудования, технических и программных средств, пользователей, данных и их связей, особенности конфигурации и архитектуры и т.п.);
- тип ИС (одно- либо многопользовательская система, открытая сеть, одно- либо многоуровневая система и т.п.);
- объемы основных информационных массивов и потоков,
- скорость обмена информацией и производительность системы при решении функциональных задач,
- продолжительность процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.;
- технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами ИС и пользователями и т.п.);
- территориальное расположение компонентов ИС, их физические параметры и т.п.;
- наличие особых условий эксплуатации и др.

Знал бы прикуп... (200)

Большое число различных компонентов, операций, ресурсов и объектов ИС создает весьма привлекательную среду для различного рода вторжений и несанкционированных операций.

Необходимость защиты ресурсов, программ и информации в компьютерной информационной системе от несанкционированного доступа и использования определяется наличием следующих угроз:

Оператор — может заменить защищенный монитор на незащищенный или имеющий только входы

Системный программист — нарушает защиту. Обеспечивает себе право входа в систему. Выявляет механизмы защиты.

Особые условия эксплуатации...

Программное обеспечение — попытки преодолеть защиту. Управление доступом. Идентификация пользователя. Управление ограничениями.

Инженер по эксплуатации — нарушает защиту технических средств. Использует автономные утилиты для доступа к файлам и входа в систему.

Доступ. Попытки получить копию (пишущая лента, валик принтера и т.п.). Неточности, вызванные действиями пользователей с низким уровнем полномочий.

Пользователь. Идентификация. Подтверждение подлинности. Искусная модификация программного обеспечения.

Рабочие станции — наиболее доступные компоненты сетей и именно с них могут быть предприняты наиболее многочисленные попытки несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На видеомониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия.

Серверы. Нуждаются в особой защите. Одни — как концентраторы больших объемов информации, другие — как элементы, в которых осуществляется преобразование данных при согласовании протоколов обмена в различных участках сети. Здесь злоумышленники прежде всего будут искать возможности повлиять на работу различных подсистем, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. При этом используются все возможности и средства, вплоть до специальных программных закладок для преодоления системы защиты, которые могут быть внедрены как с удаленных станций (посредством вирусов или иным способом), так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи. В силу большой пространственной протяженности линий связи через неконтролируемую территорию практически всегда имеется возможность подключения к ним, либо вмешательства в процесс передачи данных со стороны злоумышленников.

Ввод информации. Возможно случайное или преднамеренное нарушение целостности и истинности вводимой или хранящейся информации.

Обработка информации. Возможна утечка, нарушение целостности, истинности и сохранности информации. Перечисленные нарушения происходят в результате случайных или преднамеренных неправильных (неразрешенных) действий пользователя (санкционированного или несанкционированного для работы в данной ИС). Указанные нарушения могут возникать в результате воздействия компьютерных вирусов, занесенных в систему ее пользователями с непроверенным программным обеспечением;

Можно привести и другие угрозы, и другие каналы утечки информации, имеющие место в процессе функционирования ИС.

Проблемы интеграции систем защиты (600)

Проблемы интеграции...

В мировой практике уже давно используется такое понятие, как ***комплексная система защиты***, под которой подразумевается единая совокупность законодательных, организационных и технических мер, направленных на выявление, отражение и ликвидацию различных видов угроз безопасности.

Однако, зачастую, необходимость комплексного обеспечения безопасности организации не находит должного понимания у пользователей.

В настоящее время большинство организаций пытаются решать вопросы создания систем безопасности ***собственными силами***. Такой подход приводит к следующим отрицательным последствиям:

- создание эффективно действующей системы безопасности растягивается на большой срок;

- немногие организации имеют свою внутреннюю службу безопасности или хотя бы сотрудника, которые грамотно смогли бы решить все вопросы безопасности;
- руководители организаций, осознавая необходимость надежных систем безопасности, не могут преодолеть "барьер" необходимости установки этих систем у себя в организации. У одних этот "барьер" выражается в нехватке денежных средств, а другие не решаются на приобретение и установку систем безопасности, пока сами не убедятся в возможности несанкционированного доступа к их информации;
- использование только тех технических и технологических решений, которые известны сотрудникам служб безопасности организации приводит к применению устаревших методов и средств защиты, что в свою очередь может стать реальной угрозой для ИС.

В этом плане привлечение независимых фирм — системных интеграторов в области безопасности позволяет значительно повысить эффективность вложения средств. Такой подход обеспечивает создание комплексной системы безопасности, адаптированной под нужды и особенности Заказчика, в кратчайшие сроки. При этом обеспечивается: учет факторов, влияющих на информационную безопасность, удобство эксплуатации, приспособленность системы для работы в конкретных условиях и возможность ее дальнейшего развития и наращивания.

"Абсолютная защита" (600)

Абсолютной защиты быть не может. Распространено мнение, что "установил защиту и можно ни о чем не беспокоиться". Использование постоянных, не развивающихся механизмов защиты опасно, и для этого есть несколько причин.

Защитные свойства систем безопасности во многом зависят от конфигурации сети и используемых в ней программ. Даже если не менять топологию сети, то все равно придется когда-нибудь использовать новые версии ранее установленных продуктов. Однако может случиться так, что новые возможности этого продукта пробьют брешь в защите.

Кроме того, не следует забывать о развитии и совершенствовании средств нападения. Техника так быстро меняется, что трудно определить, какое новое устройство или программное обеспечение, используемое для нападения, может обмануть вашу защиту.

Современные интегрированные системы защиты осуществляют полный спектр управления всеми процессами, происходящими в структуре ИС.

Комплексная система защиты позволяет:

- при помощи центральной станции управления производить сбор информации со всех устройств идентификации и контроля, обрабатывать ее и управлять исполнительными устройствами;
- собирать и обрабатывать информацию с оборудования охранных систем сигнализации, систем видео наблюдения, пожаротушения, вентиляции, энергоснабжения и др.;
- создавать журналы учета состояния этих систем и происходящих изменений, демонстрировать оператору состояние систем и аварийные ситуации в текстовом или графическом виде;
- при подключении информационных каналов, связывающих главный объект с филиалами или другими объектами, центральный оператор получает возможность контролировать состояние всей структуры в реальном режиме времени.

Резюме

Под информационной системой можно понимать автоматизированную систему, предназначенную для организации, хранения, пополнения, поддержки и предоставления пользователям информации в соответствии с их запросами.

Другими словами ***информационная система*** — это сложная распределенная в пространстве система, состоящая из множества сосредоточенных (локальных) подсистем (информационных узлов), располагающих программно-аппаратными средствами реализации информационных технологий, и множества средств, обеспечивающих соединение и взаимодействие этих подсистем с целью предоставления территориально удаленным пользователям широкого набора услуг из сферы информационного обслуживания.

Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

Основными проблемами в процессе защиты информации в ИС является:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;

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

В мировой практике уже давно используется такое понятие, как комплексная система защиты, под которой подразумевается единая совокупность законодательных, организационных и технических мер, направленных на выявление, отражение и ликвидацию различных видов угроз безопасности.

Однако, зачастую, необходимость комплексного обеспечения безопасности организации не находит должного понимания у пользователей. В настоящее время большинство организаций пытаются решать вопросы создания систем безопасности собственными силами.

Такой подход приводит к следующим отрицательным последствиям:

- создание эффективно действующей системы безопасности растягивается на большой срок;
- немногие организации имеют свою внутреннюю службу безопасности или хотя бы сотрудника, которые грамотно смогли бы решить все вопросы безопасности;
- руководители организаций, сами даже осознавая, что должны быть надежные системы безопасности, не могут преодолеть барьер необходимости установки этих систем у себя в организации. У одних этот барьер выражается в нехватке денежных средств, а другие не решаются на приобретение и установку систем безопасности, пока сами не убедятся в возможности несанкционированного доступа к их информации;
- использование только тех технических и технологических решений, которые известны сотрудникам служб безопасности организации приводит к применению устаревших методов и средств защиты, что в свою очередь может стать реальной угрозой для ИС.