Структура и задачи органов, осуществляющих защиту информации

В этой главе

- *Перечень задач, решаемых службой информационной безопасности*
- *Создание службы информационной безопасности*
- *Организационно-правовой статус службы*
- *Структура службы информационной безопасности*

<<< 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

Под понятием “структурные органы” подразумевается служба информационной безопасности. Зачастую это лишь несколько сотрудников.

Опишем состав, назначение и функции структуры органов в соответствии с предложенным подходом (рис. 7.1).

Отметим, что СТРУКТУРА должна:

- руководствоваться нормативной БАЗОЙ (001), где описаны ее состав, назначение и функции;
- действовать в соответствии с установленными МЕРАМИ (003), т.е. выполнять принятую в организации политику информационной безопасности;
- иметь в своем распоряжении соответствующие СРЕДСТВА (004), т.е. – техническое оснащение.

При этом СТРУКТУРА должна решать задачи обеспечения безопасности информации по ЭТАПАМ (100–700), на соответствующих НАПРАВЛЕНИЯХ (010–050).

При описании общих (не привязанных к конкретной СЗИ) вопросов, трудно выдержать строгие требования предложенной классификации. Поэтому при желании сделать материал более интересным и доступным для читателя, неизбежны некоторые “вольности” в изложении.

БАЗА

Разумеется, основные положения политики безопасности должны быть закреплены в соответствующих распорядительных документах, состав и содержание которых определяются спецификой объекта защиты. Однако, как правило, ни одна организация не может обойтись без положений о коммерческой тайне, о защите информации, об администраторе безопасности сети, о разграничении прав доступа к информации.

МЕРЫ

Основу политики безопасности составляет перечень обязательных мероприятий, направленных на выработку плана действий по информационной защите объекта: определение состава службы по защите информации (СЗИ), ее место в организационной структуре предприятия, сфера ее компетенции, права и полномочия, варианты действий в различных ситуациях во избежание конфликтов между подразделениями.

Работы по обеспечению функционирования СЗИ входят в комплекс организационных мер, на основе которых может быть достигнут высокий уровень безопасности информации. Тем не менее, перечисленные

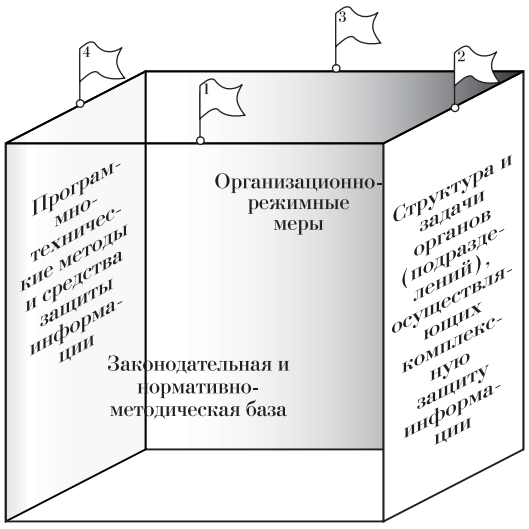


РИС. 7.1

меры не позволят на должном уровне поддерживать функционирование системы защиты без целого ряда организационно-технических мероприятий. Их проведение позволяет своевременно выявлять новые каналы утечки информации, принимать меры по их нейтрализации, совершенствованию системы защиты и оперативно реагировать на нарушения режима безопасности.

СРЕДСТВА

Использование качественных средств защиты позволяет закрыть большинство уязвимых мест, если информация о “дырах” в системах безопасности обновляется достаточно оперативно — по мере их нахождения специальными группами экспертов в области информационной безопасности.

Правильно отработанная методика проведения работ по ЗИ гарантирует, что ни один аспект информационной безопасности не останется без внимания.

Перечень решаемых задач службы информационной безопасности

Служба информационной безопасности должна участвовать в работах по созданию корпоративной системы с начала ее проектирования до момента ввода в эксплуатацию. Вместе с тем, уже работающую систему необходимо периодически обследовать на предмет выявления новых слабостей и рисков.


Это важно

Пренебрежение безопасностью корпоративных систем и надежда "на авось" неминуемо приводят к крупным финансовым потерям от реализации внутренних или внешних угроз. По оценкам и данным опросов, проведенных SANS Institute, убыток только от одной атаки на корпоративную систему для банковского и IT-секторов экономики США (где безопасности уделяется особое внимание) составляет в среднем около 500 тыс. $.

Рассмотрим содержание некоторых задач службы индивидуальной безопасности.

Определение информационных и технических ресурсов, подлежащих защите (102)

Для решения этой задачи необходимо рассмотреть функции органов (лиц), ответственных за определение информации (сведений) и средств, подлежащих защите:

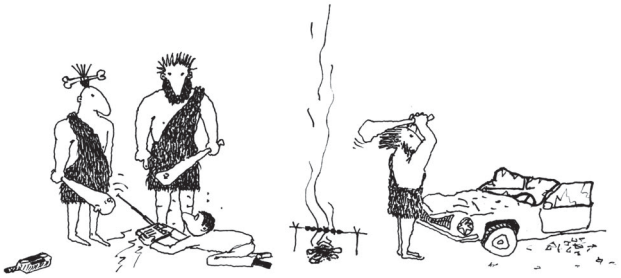
- на объектах ИС (112),
- при использовании их в процессах и программах (122),
- передаваемых по каналам связи (132),
- подверженных утечке за счет ПЭМИН (142),
- в процессе управления системой защиты (152)

Современная система безопасности информации была разработана для документов в виде "твердых копий". Вся учетная информация — входящий номер, учетный номер, дата документа, количество страниц, — относится к "твердым копиям".


Это важно

В последние несколько лет информационные технологии развивались с поразительной скоростью. Оптимисты-пользователи этих новых технологий предполагают, что бумага будет заменена электронным распределением и хранением информации. Однако безопасность информации, независимо от того, какой носитель — бумажный или электронный — используется, тесно связана с общим управлением потоками информации. Если в организации имеется четкое распределение обязанностей, потоки информации хорошо организованы, меры безопасности информации применить легко.

К сожалению, чаще бывает так, что меры безопасности информации становятся и мерами распределения потоков информации. Это может привести к довольно громоздким процедурам и вызвать впечатление у сотрудников, что меры безопасности усложняют их работу.


Служба информационной безопасности играет ведущую роль...

Если придется создавать систему безопасности информации, рекомендуется сначала присмотреться к процедурам распределения информации в этой организации.

В идеальном варианте организация должна иметь отдел (режимный) для приема и отправки всех документов, должны быть ясные инструкции о распределении входящих документов между сотрудниками, и о подготовке и утверждению выходящих документов.

Система хранения должна обеспечивать доступность и постоянное обновление информации по определенным вопросам. Все передачи документов должны регистрироваться в соответствующих журналах, чтобы прием (передача) документа были подтверждены, и было ясно, откуда он пришел или куда направляется. На каждом документе должен быть зафиксирован входящий или учетный номер и дата. Из записи должно быть видно, кому документ расписан и где он находится в данный момент и когда он подшит на хранение. Если такие правила действуют независимо от степени секретности информации, то меры по безопасности информации будут введены легко.

Выявление полного множества потенциально возможных угроз и каналов утечки информации (202)

- на объектах ИС (212),
- при использовании их в процессах и программах (222),
- в каналах связи (232),
- подверженной утечке за счет ПЭМИН (242),
- в процессе управления системой защиты (252)

Интересно

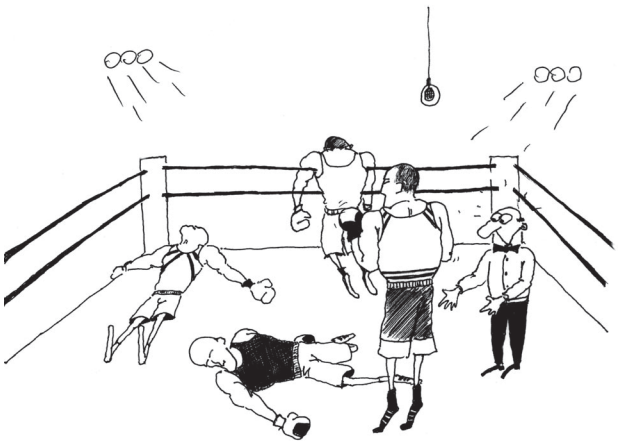
Не следует недооценивать возможности непрофессионалов по совершению компьютерных преступлений. Как метко сказано в руководстве для офицеров морской пехоты США о рядовых: "Они невежественны, но очень смекалисты". Нелояльные сотрудники, имеющие доступ к компьютерам, играют главную роль в большинстве финансовых преступлений. Это скорее организационная, чем техническая проблема. Если хорошо подобранным наемным служащим хорошо платят, то маловероятно, что они представят угрозу безопасности. Технология может играть здесь лишь вспомогательную роль.

Статистика приводит печальные данные о том, что лишь четверть сотрудников банка вполне лояльна, четверть, безусловно, настроена к фирме враждебно и не имеет моральных ограничителей, лояльность же второй половины сотрудников зависит исключительно от обстоятельств. Процедуры безопасности могут обеспечивать проверку паролей и строгий контроль доступа к ценным общим данным, но взломщика, хорошо знающего внутреннее устройство системы, практически невозможно остановить.Одной из наиболее уязвимых точек любой организации с точки зрения безопасности становится ее персонал, и, соответственно, большое значение приобретают грамотная реализация внутренней политики и работа с персоналом.

Работа с персоналом предусматривает:

- подбор и расстановку кадров;
- адаптирование сотрудника к новому коллективу;
- распределение задач и ответственности;
- обучение и повышение квалификации;
- мотивацию поведения сотрудников;
- контроль за исполнением сотрудником возложенных на него функций;
- мониторинг психологического климата в коллективе;
- выявление неудовлетворенных своим положением и нелояльных сотрудников;
- увольнение сотрудников.

Среди перечисленных задач в компетенцию службы безопасности (СБ) организации входит выявление нелояльных сотрудников (сотрудников, которые работают на конкурента) и сотрудников, не удовлетворенных своим положением в коллективе и поэтому потенциально готовых работать на конкурента.



Работа с персоналом...

Проведение оценки уязвимости и рисков для информации и ресурсов ИС (302)

- на объектах ИС (312),
- при использовании их в процессах и программах (322),
- в каналах связи (332),
- подверженных утечке за счет ПЭМИН (342),
- в процессе управления системой защиты (352)

Для построения надежной защиты необходимо выявить возможные угрозы безопасности информации, оценить их последствия, определить необходимые меры и средства защиты и оценить их эффективность.

Поскольку анализ всей информационной инфраструктуры (особенно для крупных объектов) далеко не всегда оправдан с экономической точки зрения, иногда бывает целесообразно сосредоточиться на наиболее важных объектах, отдавая себе отчет в приближенности итоговой оценки. С этих же позиций следует оценивать возможные угрозы и их последствия.

Разнообразие потенциальных угроз столь велико, что не позволяет предусмотреть каждую из них, поэтому анализируемые виды следует выбирать с позиций здравого смысла, одновременно выявляя не только угрозы, вероятность их осуществления, размер потенциального ущерба, но и их источники.

Оценка рисков производится с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации. На основании результатов анализа выявляются наиболее высокие риски, переводящие потенциальную угрозу в разряд реально опасных и, следовательно, требующие

принятия дополнительных защитных мер. Как правило, для каждой подобной угрозы существует несколько вариантов решения по ее нейтрализации.

При оценке их стоимости и эффективности следует учитывать не только расходы на закупку оборудования и программных средств, но и такие обстоятельства, как возможность экранирования одним сервисом безопасности нескольких прикладных, его совместимость с аппаратно-программной структурой организации, стоимость обучения персонала для работы с ним.

Определение требований к системе защиты информации (402)

- на объектах ИС (412),
- при использовании их в процессах и программах (422),
- в каналах связи (432),
- относительно утечки за счет ПЭМИН (442),
- в процессе управления системой защиты (452)

На основе анализа рисков строится функциональная схема системы защиты информации, основанная на задачах последней, а также предъявляемых к ней требованиях с учетом специфики конкретного объекта. Данная схема вместе с политикой безопасности, ответственностью персонала, порядком ввода в действие средств защиты, планом их размещения и модернизации составляют план защиты.

Элементы системы защиты выбираются путем сравнительного анализа технических и экономических показателей, предлагаемых на рынке средств защиты, которые размещаются на объекте в строгом соответствии с разработанной ранее схемой.

Общие затраты на обеспечение информационной безопасности объекта согласно предъявляемым требованиям по защищенности определяются в спецификациях средств реализации плана защиты информации. Необходимо учитывать, что прямое сокращение рекомендуемых средств защиты неминуемо приведет к появлению слабых мест в системе безопасности. В случае недостатка средств для полноценной реализации плана защиты необходимо либо снижать требования к защищенности объекта, либо оговаривать допустимые затраты на его защиту перед началом работ по обследованию.

Осуществление выбора средств защиты информации и их характеристик (502)

- на объектах ИС (512),
- при использовании их в процессах и программах (522),
- в каналах связи (532),
- от утечки за счет ПЭМИН (542),
- в процессе управления системой защиты (552)

Решение организационных вопросов предваряет этап работ, который должен ответить на вопрос: что необходимо сделать для реализации выбранной политики безопасности? Рынок средств защиты информации столь широк по стоимости, назначению и качеству продуктов, что выбор наиболее оптимальных из них для конкретного объекта представляется весьма непростой задачей.

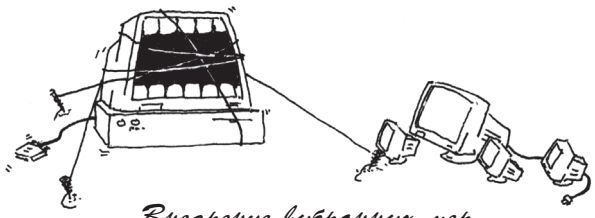
Внедрение и организация использования выбранных мер, способов и средств защиты (602)

- на объектах ИС (612),
- при использовании их в процессах и программах (622),
- в каналах связи (632),
- от ПЭМИН (642),
- в процессе управления системой защиты (652)

Внедрение и эксплуатация системы защиты требуют организационно-технической и организационно-правовой поддержки. Такая поддержка предусматривает разработку соответствующих нормативных документов, управление средствами защиты, их администрирование и контроль за правильностью эксплуатации, выявление попыток и фактов несанкционированного доступа к информационным ресурсам, поддержание непрерывности процесса обработки информации.

В связи с тем, что обработка информации на объекте осуществляется по децентрализованному принципу, управление системой защиты также не может быть возложено исключительно на службу информационной безопасности. Определенную часть подобных функций (эксплуатацию средств защиты, присвоение идентификаторов пользователям, мониторинг функционирования компьютерных систем, анализ регистрационных журналов и др.) целесообразно возложить на специально назначенных сотрудников тех подразделений, в которых ведется обработка критичной информации.

Условия для успешной реализации задачи по внедрению и эксплуатации системы защиты информации заключаются в обеспечении надлежащей организационной поддержки и создании подразделения, выполняющего функции управления средствами защиты, контроля за правильностью их эксплуатации, соблюдения плана защиты и плана обеспечения непрерывной работы и восстановления информации, выявления попыток и



Внедрение выбранных мер...

фактов несанкционированного доступа к ней и принятия мер по их нейтрализации.

Осуществление контроля целостности и управление системой защиты (702)

- на объектах ИС (712),
- при использовании их в процессах и программах (722),
- в каналах связи (732),
- от утечки за счет ПЭМИН (742),
- в процессе управления системой защиты (752)

План защиты нуждается в ежегодном пересмотре с учетом изменяющейся внешней обстановки. Такой срок вполне достаточен для своевременного внесения необходимых изменений, но только в том случае, если не возникают причины для внеочередного пересмотра: реорганизация организационно-штатной структуры предприятия, изменение территориального расположения компонентов или архитектуры автоматизированной системы, модификация используемого программного обеспечения или вычислительной техники.

Когда намеченные меры приняты, необходимо проверить их действенность, например, произвести автономное и комплексное тестирование программно-технического механизма защиты. Если проверка показывает, что в результате проделанной работы остаточные риски снизились до приемлемого уровня, то можно намечать дату ближайшей переоценки, если нет, следует проанализировать допущенные ошибки и провести повторную оценку рисков.

Создание службы информационной безопасности (002)

Подумать о создании службы безопасности необходимо сразу, как только появилась реальная опасность благополучному развитию фирмы (утечка закрытой информации, нанесение материального или финансового ущерба, угрозы руководству или сотрудникам), если объем сведений, составляющих коммерческую тайну, значителен и ваши партнеры требуют обеспечить безопасность сотрудничества.

Однако не всякой фирме под силу нести расходы по обеспечению эффективной системы безопасности, поэтому, прежде всего, необходимо провести экономическое обоснование ее создания.

Кстати

В развитых странах на содержание служб безопасности выделяется до 20% чистой прибыли в год. Таким образом, если фирма "зарабатывает" пять миллионов в год, то один миллион может быть истрачен на службу безопасности.

Как же рационально распределить расходы? Практика деятельности некоторых фирм в этой области показывает, что на содержание физической охраны расходуется до 50%, на техническое оснащение – до 30%, на другие нужды службы безопасности – до 20% средств.

Руководители крупных производственных и коммерческих организаций содержат охрану численностью в несколько сот человек. Оценив расходы на услуги охранников, оплату руководителей службы безопасности, приобретение технических средств и оснащение защиты (охранная и пожарная сигнализация, блокировочные замки, генераторы шума, криптографическая аппаратура и т.д.) экономисты могут легко подсчитать, во сколько обойдется содержание службы безопасности и сделать соответствующие выводы о целесообразности ее создания.

Не мешает навести справки о личности нанимаемого в службу безопасности, запросить характеристики с прежних мест работы, получить рекомендации от заслуживающих доверия лиц. Эффективный способ проверки — испытательный срок с соответствующими поручениями для кандидатов, когда уместно подготовить и провести несколько безобидных экспериментов, в ходе которых можно удостовериться в наличии необходимых для этой работы качеств испытуемого, например: знании законодательства; хорошей профессиональной и физической подготовке; критическом творческом мышлении; способности быстро и глубоко анализировать события и т.д.

Пока же лишь наиболее дальновидные предприниматели понимают, что своевременное получение достоверной информации о клиентах, предполагаемых партнерах и конкурентах, а также обеспечение безопасности сделок квалифицированными специалистами приносит желаемый эффект.

В связи с тем, что до 80% случаев утечки информации и утраты документов происходит по вине персонала, служба безопасности тщательно проводит подбор и проверку сотрудников, обучает их работе с секретной информацией.

СИБ может иметь открытую и закрытую области деятельности. Работа открытого характера связана с поддержанием официальных контактов с представителями других предприятий, прессой, персоналом фирмы. Закрытая деятельность обычно не афишируется. Это, как правило, скрытая проверка персонала, выполнение различных конфиденциальных поручений руководства фирмы.

Экономически оправдано для небольших фирм, с целью обеспечения безопасности, привлекать специализированные организации, с помощью которых профессионально определяется объем услуг по защите информации и принимаются необходимые меры.

С целью оказания давления на сотрудников, игнорирующих принятый порядок защиты информации, нужны четкие, продуманные правила, определяющие меры обеспечения безопасности информационных технологий.

Однако одни лишь правила не решат всех проблем. Самые лучшие правила не имеют никакой ценности, если сотрудники не подозревают об их существовании или не соблюдают их.

Разработка правил может быть одной из основных функций службы информационной безопасности.

Служба информационной безопасности представляет собой подразделение для организации работ по созданию системы защиты информации и последующего обеспечения ее функционирования.

Типовой перечень задач службы информационной безопасности (002)

Ниже приведен примерный перечень задач службы информационной безопасности, который можно использовать на начальном этапе создания подобных служб, подразделений или ответственного сотрудника.

Основной задачей службы информационной безопасности является определение направления развития и поддержки усилий организации, направленных на защиту информации от несанкционированного ознакомления, изменения, разрушения или отказа в доступе. Это достигается путем внедрения соответствующих правил, инструкций и указаний.

Служба информационной безопасности отвечает за:

- разработку и издание правил (инструкций и указаний) по обеспечению безопасности, соответствующих общим правилам работы организации и требованиям к обработке информации;
- внедрение программы обеспечения безопасности, включая классификацию степени секретности информации (если таковая имеется) и оценку деятельности;
- разработку и обеспечение выполнения программы обучения и ознакомления с основами информационной безопасности в масштабах организации;
- разработку и сопровождение перечня минимальных требований к процедурам контроля за доступом ко всем компьютерным системам, независимо от их размера;
- отбор, внедрение, проверку и эксплуатацию соответствующих методик планирования восстановления работы для всех подразделений организации, принимающих участие в автоматизированной обработке самой важной информации;
- разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а также рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;
- участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;
- изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации.

При необходимости на службу информационной безопасности возлагается выполнение других обязанностей:

- формирование требований к системе защиты в процессе создания ИС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования ИС;
- распределение между пользователями необходимых реквизитов защиты;
- наблюдение за функционированием системы защиты и ее элементов;
- организация проверок надежности функционирования системы защиты;
- обучение пользователей и персонала ИС правилам безопасной обработки информации;
- контроль за соблюдением пользователями и персоналом ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;
- принятие мер при попытках НСД к информации и при нарушениях правил функционирования системы защиты.

Организационно-правовой статус службы (002)

- Численность службы защиты должна быть достаточной для выполнения всех перечисленных функций;
- служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием ИС;
- сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура ИС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;
- руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы ИС, если они не отвечают требованиям защиты информации;
- служба защиты информации должна иметь все условия, необходимые для выполнения своих функций.

Структура службы информационной безопасности (002)

В структуру службы безопасности (002) могут входить:

- директор (заместитель директора) или руководитель, непосредственно подчиненный главе фирмы;
- заместитель начальника службы безопасности — на некоторых предприятиях он руководит физической, а иногда и технической службами охраны;
- аналитик;
- юрист;
- специалисты в области обеспечения безопасности, экономической разведки, промышленной контрразведки;
- технические специалисты, умеющие применять специальную технику для защиты помещений;
- сотрудники физической охраны и пропускного режима (по найму), но подчиненные руководителю службы безопасности).

Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям:

Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника группы безопасности.

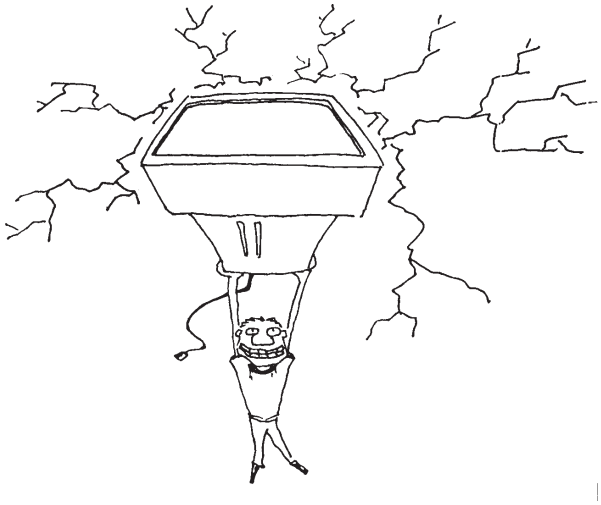
Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

Руководитель группы. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах ИС (при децентрализованном управлении).

В небольших организациях функции руководителя службы обычно выполняет либо глава фирмы, либо его заместитель.

Количественный состав службы безопасности различен и зависит, прежде всего, от возможностей самой фирмы. Возможны различные варианты состава такой группы. Кроме того, перечень необходимых знаний и навыков, а также функциональных обязанностей лиц, входящих в группу защиты информации может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной ИС.



Администратор безопасности...

К сожалению, на современном этапе отдается предпочтение физической и технической охране, время “оперативников” и аналитиков только начинается.

Резюме

Не секрет, что руководители очень крупных производственных и коммерческих организаций содержат охрану численностью в несколько сот человек. Оценив расходы на услуги охранников, оплату руководителей службы безопасности, приобретение технических средств и оснащение защиты (охранная и пожарная сигнализация, блокировочные замки, генераторы шума, криптографическая аппаратура и т.д.) экономисты могут легко подсчитать, во сколько обойдется содержание службы безопасности и сделать соответствующие выводы о целесообразности ее создания.

Часть предпринимателей предпочитает формировать службу безопасности из профессионалов — сотрудников органов безопасности, подразделений разведки, МВД. Однако стороны не всегда находят общий язык. Например, предприниматель, действующий на грани закона и подбирающий в службу безопасности тех, кто его “прикроет” в трудную минуту, не может рассчитывать на молчание каждого из своих сотрудников, связанных с правоохранительными органами. Поэтому некоторые руководители фирм требуют от принимаемых на работу прекращения всех деловых контактов с органами безопасности и милиции.

В структуру службы безопасности (002) могут входить:

- руководитель, непосредственно подчиненный главе фирмы или сам являющийся директором (заместителем директора) фирмы;
- заместитель начальника службы безопасности — на некоторых предприятиях он руководит физической, а иногда и технической службами охраны;
- аналитик;
- юрист;
- специалисты в области обеспечения безопасности, экономической разведки, промышленной контрразведки;
- технические специалисты, умеющие применять специальную технику для защиты помещений;
- сотрудники физической охраны и пропускного режима (по найму), но подчиняются руководителю службы безопасности).