Политика информационной безопасности (организационно-технические и режимные меры)

8

В этой главе

- *Определение политики информационной безопасности*
- *Принципы политики безопасности*
- *Виды политики безопасности*
- *Организация секретного делопроизводства*
- *Политики безопасности для Internet*
- *Уровни политики безопасности*
- *Роли и обязанности*
- *Краткое содержание документов ПИБ*

<<< 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

Определение политики информационной безопасности (003)

При принятии решений администраторы ИС сталкиваются с проблемой выбора вариантов решений по организации ЗИ на основе учета принципов деятельности организации, соотношения важности целей и наличия ресурсов. Эти решения включают определение того, как будут защищаться технические и информационные ресурсы, а также как должны вести себя служащие в тех или иных ситуациях.

Политика информационной безопасности – набор законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Определение

В соответствии с предложенным в книге подходом политика (МЕРЫ) информационной безопасности (003) реализуется соответствующей СТРУКТУРОЙ органов (002) на основе нормативно-методической БАЗЫ (001) с использованием программно-технических методов и СРЕДСТВ (004), определяющих архитектуру системы защиты.

Для конкретной ИС политика безопасности должна быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д.

Следует рассматривать такие направления защиты ИС:

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

Очевидно, что каждое из указанных НАПРАВЛЕНИЙ должно быть детализировано в зависимости от особенностей структуры ИС.

Кроме этого ПИБ должна описывать следующие ***ЭТАПЫ создания СЗИ:***

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

Принципы политики безопасности (003)

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. При разработке и проведении ее в жизнь ***целесообразно руководствоваться следующими принципами:***

1. Невозможность миновать защитные средства;
2. Усиление самого слабого звена;
3. Недопустимость перехода в открытое состояние;
4. Минимизация привилегий;
5. Разделение обязанностей;
6. Многоуровневая защита;
7. Разнообразие защитных средств;
8. Простота и управляемость информационной системы;
9. Обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

1. **Принцип невозможности** миновать защитные средства означает, что все информационные потоки в защищаемую сеть и из нее должны проходить через СЗИ. Не должно быть “тайных” модемных входов или тестовых линий, идущих в обход экрана.

2. **Надежность любой СЗИ** определяется самым слабым звеном. Часто таким звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. **Принцип недопустимости перехода** в открытое состояние означает, что при любых обстоятельствах (в том числе нештатных), СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ.

4. **Принцип минимизации привилегий** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей...

5. **Принцип разделения обязанностей** предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно для предотвращения злонамеренных или неквалифицированных действий системного администратора.

6. **Принцип многоуровневой защиты** предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией — управление доступом и, как последний рубеж, — протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

7. **Принцип разнообразия защитных средств** рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками преодоления СЗИ.

8. **Принцип простоты и управляемости информационной системы** в целом и СЗИ в особенности определяет возможность формального или неформального доказательства корректности реализации механизмов защиты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

9. **Принцип всеобщей поддержки мер безопасности** носит нетехнический характер. Рекомендуется с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Виды политики безопасности (603)

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности.

Для изучения свойств способа управления доступом создается его формальное описание — математическая модель. При этом модель должна отражать состояния всей системы, ее переходы из одного состояния в другое, а также учитывать, какие состояния и переходы можно считать безопасными в смысле данного управления. Без этого говорить о каких-либо свойствах системы, и тем более гарантировать их, по меньшей мере некорректно.

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная, основанные, соответственно на избирательном и полномочном способах управления доступом.

Кроме того, существует набор требований, усиливающий действие этих политик и предназначенный для управления информационными потоками в системе.

Следует отметить, что средства защиты, предназначенные для реализации какого-либо из названных способа управления доступом, только предоставляют возможности надежного управления доступом или информационными потоками. Определение прав доступа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т.д.) входит в компетенцию администрации системы.

Избирательная политика безопасности (603)

Основой избирательной политики безопасности является избирательное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого правила (свойство избирательности).

Для описания свойств избирательного управления доступом применяется модель системы на основе **матрицы доступа** (МД), иногда ее называют матрицей контроля доступа. Такая модель получила название матричной.

Матрица доступа представляет собой прямоугольную матрицу, в которой объекту системы соответствует строка, а субъекту столбец. На пересечении столбца и строки матрицы указывается тип разрешенного дос-

тупа субъекта к объекту. Обычно выделяют такие типы доступа субъекта к объекту, как “доступ на чтение”, “доступ на запись”, “доступ на исполнение” и др.

Множество объектов и типов доступа к ним субъекта может изменяться в соответствии с некоторыми правилами, существующими в данной системе. Определение и изменение этих правил также является задачей МД.

Решение на доступ субъекта к объекту принимается в соответствии с типом доступа, указанным в соответствующей ячейке матрицы доступа. Обычно избирательное управление доступом реализует принцип “что не разрешено, то запрещено”, предполагающий явное разрешение доступа субъекта к объекту. Матрица доступа — наиболее простой подход к моделированию систем доступа.

Избирательная политика безопасности наиболее широко применяется в коммерческом секторе, так как ее реализация на практике отвечает требованиям коммерческих организаций по разграничению доступа и подотчетности, а также имеет приемлемую стоимость и небольшие накладные расходы.

Факты

“Один наш клиент, занимающийся финансовыми операциями, испытывал беспокойство в связи с подключением к Internet. Нам удалось быстро выяснить, что главные опасения вызывала защита данных отдела кадров; при его переводе на онлайновую работу могла пострадать конфиденциальность информации. Компания рассматривала вопрос об установке какого-нибудь технического средства, например брандмауэра интрасети, чтобы остальную часть компании можно было подключить к Internet.

В течение нескольких минут мы определили, что из 5000 сотрудников компании осуществлять доступ к компьютерам отдела кадров должны всего шестеро, и как раз им-то нужны только самые простые Internet-функции для доступа к корпоративной почтовой системе.

Мы предложили простое, дешевое и эффективное решение: воздушный зазор. Отсоедините компьютеры отдела кадров от корпоративной сети и Internet. Дайте каждому из шести сотрудников по дополнительному персональному компьютеру младшего класса (которые пылятся на складе безо всякого использования) для доступа к корпоративной почтовой системе. Цена данного решения составляет сотую долю от стоимости того, которое компания изначально предполагала реализовать, а проблемы с управлением сводятся на нет. Не всегда техника может сделать все то, чего от нее ожидают”.

(Уинн Швартау — президент Interpact, Inc., международной консалтинговой компании, занимающейся вопросами безопасности.)

Полномочная политика безопасности (603)

Основу полномочной политики безопасности составляет полномочное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности. Организация меток имеет иерархическую структуру и, таким образом, в системе можно реализовать иерархически восходящий поток информации (например, от рядовых исполнителей к руководству). Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности.

Каждый субъект, кроме уровня прозрачности, имеет текущее значение уровня безопасности, которое может изменяться от некоторого минимального значения до значения его уровня прозрачности.

Основное назначение полномочной политики безопасности — регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии в нижние, а также блокирование возможного проникновения с нижних уровней в верхние. При этом она функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности).

Интересно

Изначально полномочная политика безопасности была разработана в интересах МО США для обработки информации с различными грифами секретности. Ее применение в коммерческом секторе сдерживается следующими причинами:

- отсутствием в коммерческих организациях четкой классификации хранимой и обрабатываемой информации, аналогичной государственной классификации (грифы секретности сведений);
- высокой стоимостью реализации и большими накладными расходами.

Организационно-технические мероприятия (603)

Приведем ***перечень основных организационно-технические мероприятия по ЗИ*:**

- разработка и утверждение функциональных обязанностей должностных лиц службы информационной безопасности;
- внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов ИС и действиям в случае возникновения кризисных ситуаций;
- оформление юридических документов (договора, приказы и распоряжения руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитраж, третейский суд) о правилах разрешения споров, связанных с применением электронной подписи;
- создание научно-технических и методологических основ защиты ИС;
- исключение возможности тайного проникновения в помещения, установки прослушивающей аппаратуры и т.п.;
- проверка и сертификация используемых в ИС технических и программных средств на предмет определения мер по их защите от утечки по каналам побочных электромагнитных излучений и наводок;
- определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;
- разработка правил управления доступом к ресурсам системы, определение перечня задач, решаемых структурными подразделениями организации с использованием ИС, а также используемых при их решении режимов обработки и доступа к данным;
- определение перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в ИС;
- выявление наиболее вероятных угроз для данной ИС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней;
- оценка возможного ущерба, вызванного нарушением безопасности информации, разработка адекватных требований по основным направлениям защиты;
- организация надежного пропускного режима;
- определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;
- организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;
- организация и контроль за соблюдением всеми должностными лицами требований по обеспечению безопасности обработки информации;
- определение перечня необходимых мер по обеспечению непрерывной работы ИС в критических ситуациях, возникающих в результате НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий и т.п.
- контроль функционирования и управление используемыми средствами защиты;
- явный и скрытый контроль за работой персонала системы;
- контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования ИС;
- периодический анализ состояния и оценка эффективности мер защиты информации;
- распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);
- анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;
- составление правил разграничения доступа пользователей к информации;
- периодическое с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;
- рассмотрение и утверждение всех изменений в оборудовании ИС, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.;
- проверка принимаемых на работу, обучение их правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности.

Защита данных административными методами (603)

К таким мерам защиты можно отнести организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации системы обработки и передачи данных фирмы или банка с целью обеспечения защиты информации.

Насколько важны организационно-режимные мероприятия в общем арсенале средств защиты, говорит уже хотя бы тот факт, что ни одна ИС не может функционировать без участия обслуживающего персонала. Кроме того, организационно-режимные мероприятия охватывают все структурные элементы системы защиты на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверка в эксплуатации аппаратуры, оргтехники, средств обработки и передачи данных.

С одной стороны, эти меры должны быть направлены на обеспечение правильности функционирования механизмов защиты и выполняться администратором безопасности системы. С другой — руководство фирмы должно регламентировать правила обработки и защиты информации, а также установить меру ответственности за нарушение этих правил.

Совет

Ниже перечислен ряд достаточно простых действий, которые могут значительно повысить степень защиты корпоративной сети без больших финансовых затрат.

1. Более тщательное наблюдение за персоналом, в особенности за низкооплачиваемыми работниками (уборщики и охранники).

2. Незаметная проверка послужного списка нанимаемого работника, что поможет избежать проблем в будущем.

3. Ознакомление нанимаемого сотрудника с документами, описывающими политику компании в области информационной безопасности, и получение от него соответствующей расписки.

4. Изменение содержимого всех экранов для входа в систему таким образом, чтобы они отражали политику компании в области защиты данных (эта мера настоятельно рекомендуется Министерством юстиции США).

5. Повышение уровня физической защиты.

6. Блокировка всех дисководов гибких дисков в организациях, в которых установлена сеть, — это позволит минимизировать риск компьютерных краж и заражения вирусами.

7. Признание за сотрудниками определенных прав при работе с компьютерами, например организация досок объявлений, соблюдение конфиденциальности электронной почты, разрешение использовать определенные компьютерные игры.

Сотрудники компании должны быть союзниками, а не противниками администратора системы в борьбе за безопасность данных.

(Кевин Стивенс, Уинн Швартау)

В настоящее время фирмы по изготовлении технических средств для промышленного шпионажа, выпускают устройства, которые по параметрам не уступают оперативной технике, используемой спецслужбами.

Лучше вооружены те спецслужбы, у которых есть для этого денежные средства. Это обстоятельство необходимо учитывать при оценке потенциальных возможностей ваших конкурентов по ведению промышленного шпионажа.

Первым шагом в создании эффективной системы защиты фирмы от технического проникновения конкурентов или злоумышленников должна стать оценка основных методов промышленного шпионажа, которыми могут воспользоваться конкуренты, изучение характеристик имеющихся у них на вооружении средств съема информации с отдельных помещений и технических средств фирмы.

Предварительный анализ уязвимости помещений и технического оснащения фирмы от промышленного шпионажа позволяет сделать вывод о наиболее вероятных методах съема информации, которые может использовать конкурент. Такой анализ дает возможность службе безопасности фирмы выработать необходимые организационно-режимные, технические и специальные меры защиты объекта фирмы.

Организационно-режимные меры защиты базируются на законодательных и нормативных документах по безопасности информации и должны охватывать ***основные пути сохранения информационных ресурсов*:**

- ограничение физического доступа к объектам обработки и хранения информации и реализацию режимных мер;
- ограничение возможности перехвата информации вследствие существования физических полей;
- ограничение доступа к информационным ресурсам и другим элементам системы обработки данных путем установления правил разграничения доступа, криптографическое закрытие каналов передачи данных, выявление и уничтожение "закладок";
- создание твердых копий на случай утраты массивов данных;
- проведение профилактических и других мер от внедрения "вирусов".

По содержанию все организационные мероприятия можно условно разделить на следующие группы.

Мероприятия, осуществляемые при создании ИС, состоящие в учете требований защиты при:

- разработке общего проекта системы и ее структурных элементов;
- строительстве или переоборудовании помещений;
- разработке математического, программного, информационного или лингвистического обеспечения;
- монтаже и наладке оборудования;
- испытаниях и приемке системы.

Особое значение на данном этапе придается определению действительных возможностей механизмов защиты, для чего целесообразно осуществить комплекс испытаний и проверок.

***Мероприятия, осуществляемые в процессе эксплуатации* ИС:**

- организация пропускного режима;
- организация автоматизированной обработки информации;
- организация ведения протоколов;
- распределение реквизитов разграничения доступа (паролей полномочий и пр.);
- контроль выполнения требований служебных инструкций и т.п.

Мероприятия общего характера

- учет требований защиты при подборе и подготовке кадров;
- организация проверок механизма защиты;
- планирование мероприятий по защите информации;
- обучение персонала;
- проведение занятий с привлечением ведущих организаций;
- участие в семинарах и конференциях по проблемам безопасности информации и т.п.

Организация секретного делопроизводства (063)

Во время работы по защите коммерческой тайны необходимо обратить особое внимание на документы фирмы, поскольку большинство коммерческих структур в нашей стране основные объемы коммерческой информации, в том числе конфиденциальной, хранят в документах.

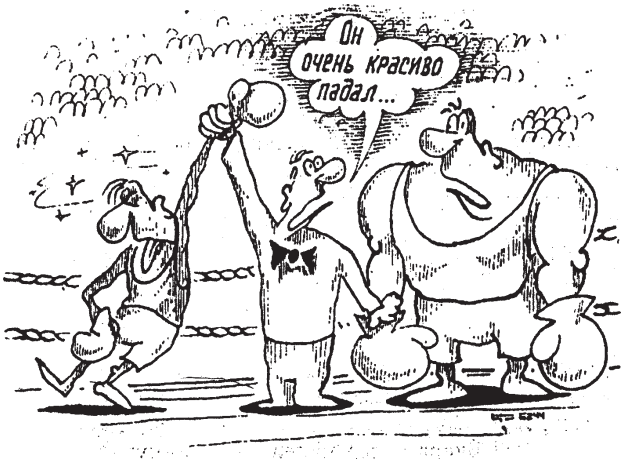
Руководитель фирмы должен упорядочить процессы фиксации и движение секретной информации в бумагах таким образом, чтобы похищение их было крайне затруднено и становилось экономически невыгодным для похитителя.

При работе с важными документами следует выполнять следующие требования:

- строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;
- назначение конкретных лиц из руководства и служащих фирмы, организующих и контролирующих секретное делопроизводство; наделение их соответствующими полномочиями;
- разработка инструкции (памятки) по работе с секретными документами, ознакомление с нею соответствующих работников фирмы;
- контроль за принятием сотрудниками письменных обязательств о сохранении коммерческой тайны фирмы;
- введение системы материального и иного стимулирования служащих фирмы, имеющих доступ к ее секретам;
- внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;
- личный контроль со стороны руководителя фирмы службы внутренней безопасности и секретного делопроизводства.

Вероятность утечки секретной информации особенно велика в процессе пересылки документов. Поскольку у коммерческих структур нет возможностей пользоваться услугами военизированной фельдсвязи, доставку секретных документов и ценностей приходится осуществлять силами собственных охранников или специальных фирм.

Служащие, ответственные за сохранность, использование и своевременное уничтожение секретных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но радикальным способом — хорошей платой за работу.



Стимулирование и поощрение сотрудников...

В процессе хранения и пересылки секретных документов фирмы могут быть применены средства защиты и сигнализации о несанкционированном доступе к ним. Одна из новинок — невидимое светочувствительное покрытие, наносимое на документы, которое проявляется под воздействием света, указывая тем самым на факт несанкционированного ознакомления с документами или их фотографирования.

Специалистам по вопросам защиты коммерческой информации известны и иные технологии и системы охраны конфиденциальных документов фирмы от несанкционированного к ней доступа или возможной утечки охраняемых сведений. За информацией по данному вопросу следует обращаться в организации и службы, которые специально занимаются данной проблемой. Основные функции обеспечения безопасности информации при работе с секретными документами рассмотрены в таблице 8.1.

Для ведения секретного делопроизводства должны привлекаться лица, прошедшие специальную проверку, и в честности которых нет сомнений. Кроме того, эти люди должны быть соответствующим образом подготовлены и обучены, так как профессиональные недочеты и отступление от рабочих правил слишком дорого обходятся фирме.

Помещения, в которых ведется работа с секретными документами, должны хорошо охраняться, а доступ туда должен быть закрыт для посторонних лиц. Эти помещения должны иметь прочные перекрытия и стены, усиленную металлическую дверь, прочные оконные рамы с двойными стеклами и решеткой, плотные шторы. Хранилище должно быть оборудовано охранной и пожарной сигнализацией и тщательно охраняться силами внутренней охраны. Не рекомендуется располагать такое помещение на первом и последнем этажах здания. Секретные документы храняться в сейфах или несгораемых металлических шкафах с надежными замками.

Различные приемы ведения секретного делопроизводства направлены на предотвращение утечки коммерческих секретов. Документы, содержащие коммерческую тайну, различаются по степени секретности и снабжаются соответствующим грифом секретности.

Даже тщательно охраняемые тайны фирмы могут стать достоянием конкурентов из обычных публикаций, если пустить это дело на самотек. Поэтому один из служащих фирмы обязательно должен быть наделен широкими цензурными полномочиями при подготовке материалов для симпозиумов, выставок, а также выступлений и научных публикаций сотрудников фирмы.

Интересы охраны секретов фирмы чаще всего находятся в постоянном противоречии с личными амбициями сотрудников фирмы, желающих профессионально самоутверждаться в ученом мире.

Не менее сложен для разрешения конфликт между стремлением сохранить коммерческие тайны фирмы и желанием использовать в рекламных целях некоторые наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Сотрудник, осуществляющий цензуру открытых публикаций рекламного, научного и популяризаторского характера, готовящихся персоналом фирмы или по ее заказам, должен руководствоваться простым, но эффективным правилом. Суть его в том, чтобы в максимально возможной степени раздробить, разобщить по времени, в пространстве и по авторам ту строго охраняемую коммерческую информацию, без которой невозможно опубликование упомянутых работ. Конечно, все это затрудняет осуществление персоналом фирмы научно-исследовательских и опытно-конструкторских работ, но существенно препятствует сбору секретной информации о фирме конкурентами и недоброжелателями.

Этот барьер преодолим лишь посредством больших затрат.

Организация мероприятий по ЗИ (603)

Нельзя приступать к внедрению правил ЗИ, пока пользователи не приобретут навыков, необходимых для их соблюдения. Безопасность требует не только знаний, но и действий. Все пользователи должны знать, что нужно предпринять и чего делать не следует, когда они сталкиваются с нарушением или возможностью его возникновения; к кому нужно обращаться при возникновении подозрений. Пользователи должны быть уверены в том, что меры по обеспечению безопасности

Таблица 8.1. Организация секретного делопроизводства.

Составные части делопроизводства	Функции обеспечения безопасности информации при работе с документами	Способы выполнения
ДОКУМЕНТИРОВАНИЕ	1. Предупреждение необоснованного изготовления документов 2. Предупреждение включения в документы избыточных конфиденциальных сведений 3. Предупреждение необоснованного завышения степени секретности документов 4. Предупреждение необоснованной рассылки	1. Определение перечня документов 2. Осуществление контроля за содержанием документов и степени секретности их содержания 3. Определение реальной степени секретности сведений, включенных в документ 4. Осуществление контроля за размножением и рассылкой документов
УЧЕТ ДОКУМЕНТОВ	1. Предупреждение утраты (хищения) документов	1. Обеспечение регистрации каждого документа и удобства его поиска 2. Осуществление контроля за местонахождением документа
ОРГАНИЗАЦИЯ ДОКУМЕНТООБОРОТА	1. Предупреждение необоснованности ознакомления с документами 2. Предупреждение неконтролируемой передачи документов	1. Установление разрешительной системы доступа исполнителей к документу 2. Установление порядка приема-передачи документов между сотрудниками 3. Осуществление контроля за порядком работы с документами
ХРАНЕНИЕ ДОКУМЕНТОВ	1. Обеспечение сохранности документов	1. Выделение специально оборудованных помещений для хранения документов, исключающих доступ к ним посторонних лиц 2. Установление порядка допуска к делам 3. Осуществление контроля за своевременностью и правильностью формирования дел
УНИЧТОЖЕНИЕ ДОКУМЕНТОВ	1. Исключение из документооборота документов, потерявших свою ценность	1. Установление порядка подготовки документов для уничтожения 2. Обеспечение необходимых условий уничтожения 3. Осуществление контроля за правильностью и своевременностью уничтожения документов
ПРОВЕРКА НАЛИЧИЯ ДОКУМЕНТОВ	1. Контроль наличия документов, выполнения требований их обработки, учета, исполнения и сдачи	1. Установление порядка проведения проверок наличия документов и порядка их обработки

принимаются в их же интересах, а не по иным соображениям.

Обеспечьте пользователей руководством, в котором изложен материал приемлемого объема. Даже если пользователи усвоили правила, то у них может возникнуть вопрос, как эти правила применять. Предоставляйте вместе с правилами модельные процедуры внедрения и примеры. Записывайте вопросы сотрудников (вместе с вашими ответами и пояснениями) в сопроводительной документации к правилам. Сообщайте пользователям об этих дополнениях.

Дополняйте правила модельными процедурами и примерами реализации. Убедитесь, что ваши правила посвящены защите от истинных опасностей — от тех, вероятность возникновения которых достаточно реальна и действительно представляют для вас угрозу.

Мудрые советы...

Стивен Кац, руководитель службы информационной безопасности Citibank, рекомендует...

Прежде всего, очень важно научиться правильно мыслить. Попробуйте задать себе такие вопросы:

Как я могу узнать, кто использует вверенную мне сеть и ее информационные ресурсы?

Почему это для меня важно?

К какой категории — локальных или удаленных — относятся пользователи?

Как я могу заставить пользователей, сообщивших мне свои имена, доказать их подлинность?

Каким образом я могу управлять действиями пользователей?

Важно ли это для меня?

Должен ли быть ограничен доступ пользователей ко всему объему информации?

Если ограничения есть, то кто их устанавливает и следит за их соблюдением?

Кроме того, если вы собираетесь передавать информацию по линиям связи, определите, какая ее часть должна иметь закрытый, конфиденциальный характер. Подумайте о том, как вы можете добиться конфиденциальности при передаче данных. Может быть, позаботиться, чтобы содержимое ваших посланий не могло быть искажено? "Сегодня конфиденциальность электронных сообщений не выше, чем у почтовых открыток", — считает Кац.

Совокупность мероприятий, направленных на предотвращение угроз, определяется обеспечением следующих мер:

- введением избыточности технических средств, ПО и массивов данных;
- резервированием технических средств;
- регулированием доступа к техническим средствам, ПО, массивам информации;
- регулированием использования программно-аппаратных средств и массивов информации;
- криптографической защитой информации;
- контролем элементов ИС;
- регистрацией сведений;
- своевременным уничтожением ненужной информации;
- сигнализацией;
- своевременным реагированием.

Некоторые мероприятия по ЗИ представлены на рис. 8.2.

В рамках системы множество и разнообразие видов защиты информации определяется способами воздействия на дестабилизирующие факторы или порождающие их причины, на элементы ИС, защищаемую информацию и окружающую среду в направлении повышения показателей защищенности информации. Эти способы могут быть классифицированы следующим образом:

Физические средства — механические, электрические, электромеханические, электронные, электронно-механические и другие устройства и системы, функционирующие автономно, создавая различного рода препятствия дестабилизирующим факторам.

Аппаратные средства — различные электронные, электронно-механические и подобные устройства, встраиваемые в аппаратуру ИС или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства — специальные пакеты программ или отдельные программы, используемые для решения задач защиты.

Организационные меры — организационно-технические мероприятия, предусматриваемые в ИС с целью решения задач защиты.

Правовые меры — законодательно-правовые акты, действующие в государстве, специально издаваемые законы, связанные с обеспечением защиты информации. Они регламентируют права и обязанности всех лиц и подразделений, имеющих отношение к функционированию ИС, и устанавливают ответственность за действия, следствием которых может быть нарушение защищенности информации.

Морально-этические нормы — это сложившиеся моральные нормы и этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе.

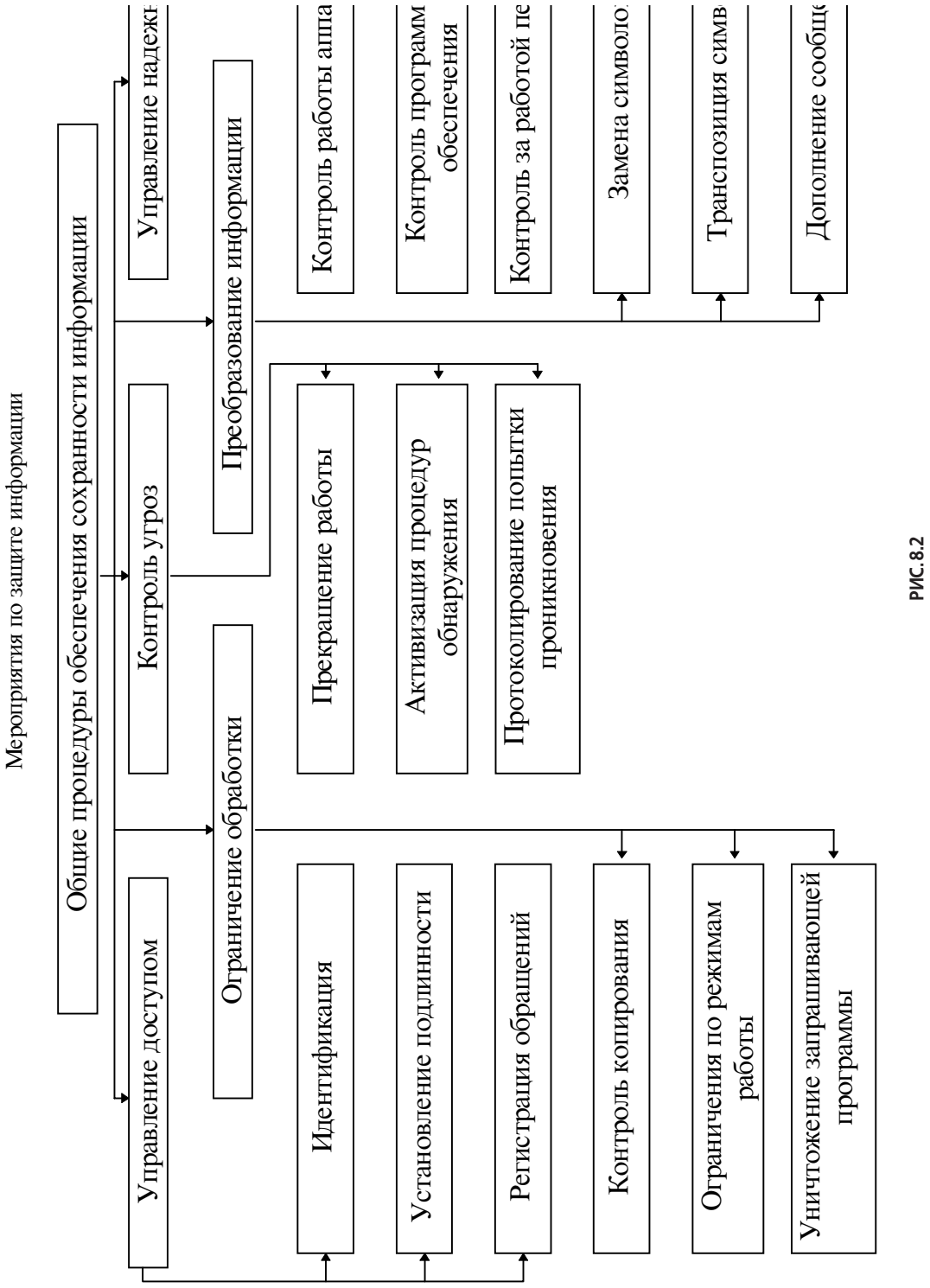

Мероприятия по защите информации
Общие процедуры обеспечения сохранности информации
Управление надежн
Управление доступом
Контроль угроз
Преобразование информации
Ограничение обработки
Контроль работы аппа
Контроль программ обеспечения
Контроль за работой пе
Замена символо
Транспозиция симв
Дополнение сообщ
Прекращение работы
Активизация процедур обнаружения
Протоколирование попытки проникновения
Идентификация
Установление подлинности
Регистрация обращений
Контроль копирования
Ограничения по режимам работы
Уничтожение запрашивающей программы

РИС. 8.2

Для обеспечения эффективности защиты информации все используемые средства и мероприятия целесообразно объединить в ***систему защиты информации***, которая должна быть функционально самостоятельной подсистемой ИС. Главным свойством системы защиты должна быть адаптивность ее при изменении структуры технологических схем или условий функционирования ИС.

Другими принципами могут быть:

- минимизация затрат, максимальное использование серийных средств;
- обеспечение решения требуемой совокупности задач защиты;
- комплексное использование средств защиты, оптимизация архитектуры;
- удобство для персонала;
- простота эксплуатации.

СЗИ целесообразно строить в виде взаимосвязанных подсистем:

- криптографической защиты;
- обеспечения юридической значимости электронных документов;
- защиты от НСД;
- организационно-правовой защиты;
- управления СЗИ.

Построение системы защиты информации в таком виде позволит обеспечить комплексность процесса защиты информации в ИС, управляемость процесса и возможность адаптации при изменении условий функционирования ИС.

Подсистема криптографической защиты объединяет средства такой защиты информации и по ряду функций кооперируется с подсистемой защиты от НСД.

Подсистема обеспечения юридической значимости электронных документов служит для придания юридического статуса документам в электронном представлении и является определяющим моментом при переходе к безбумажной технологии документооборота. Данную подсистему удобно и целесообразно рассматривать как часть подсистемы криптографической защиты.

Подсистема защиты от НСД предотвращает доступ несанкционированных пользователей к ресурсам ИС.

Подсистема управления СЗИ предназначена для управления ключевыми структурами подсистемы криптографической защиты, а также контроля и диагностирования программно-аппаратных средств и обеспечения взаимодействия всех подсистем СЗИ.

Подсистема организационно-правовой защиты предназначена для регламентации деятельности пользователей ИС и представляет собой упорядоченную совокупность организационных решений, нормативов, законов и правил, определяющих общую организацию работ по защите информации в ИС.

Система защиты информации представляет собой совокупность автоматизированных рабочих мест (АРМ), входящих в состав ИС, и программно-аппаратных средств, интегрированных в АРМ пользователей ИС.

Политики безопасности для Internet (403)

Организации должны ответить на следующие вопросы, чтобы правильно учесть возможные последствия подключения к Internet в области безопасности:

- Могут ли хакеры разрушить внутренние системы?
- Может ли быть скомпрометирована (изменена или прочитана) важная информация организации при ее передаче по Internet?
- Можно ли помешать работе организации?

Цель политики безопасности для Internet – принять решение о том, как организация предполагает защищаться. ПИБ обычно состоит из двух частей – общих принципов и конкретных правил работы (которые эквивалентны специфической политике, описанной ниже). Общие принципы определяют подход к безопасности в Internet. Правила же определяют, что разрешено, а что – запрещено. Правила могут быть дополнены конкретными процедурами и различными руководствами.

Система Internet при проектировании и не планировалась как защищенная сеть, поэтому ее ***проблемами в текущей версии TCP/IP являются:***

- Легкость перехвата данных и фальсификации адресов машин в сети – основная часть трафика Internet – это нешифрованные данные. E-mail, пароли и файлы могут быть перехвачены путем использования доступных программ.
- Уязвимость средств TCP/IP – ряд средств TCP/IP не был спроектирован быть защищенными и может быть скомпрометирован квалифицированными злоумышленниками; средства, используемые для тестирования, особенно уязвимы.
- Отсутствие политики – многие сайты по незнанию сконфигурированы таким образом, что предоставляют широкий доступ к себе со стороны Internet, не учитывая возможность злоупотребления этим доступом; многие сайты разрешают работу большего числа сервисов TCP/IP, чем им требуется для работы, и не пытаются ограничить доступ к информации о своих компьютерах, которой могут воспользоваться злоумышленники.
- Сложность конфигурирования – средства управления доступом хоста сложны; зачастую трудно правильно сконфигурировать и проверить эффективность установок. Средства, неправильно сконфигурированные, могут привести к неавторизованному доступу.

Уровни политики безопасности (403)

С практической точки зрения политику безопасности можно условно разделить на три уровня: верхний, средний и нижний.

Верхний уровень (403)

К верхнему уровню относятся решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации.

Примерный список подобных решений может включать в себя следующие элементы:

- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка управленческих решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Цели политики верхнего уровня организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности.

Если организация ответственна за поддержание критически важных баз данных, на первом плане может стоять уменьшение случаев потерь, повреждений или искажений данных. Для организации, занимающейся продажами, вероятно, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей. Режимная организация в первую очередь заботится о защите от несанкционированного доступа — конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация их использования, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.

ПИБ верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации или даже больше, если ПИБ регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров. Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь. В этом смысле ПИБ является основой подотчетности персонала.

На верхний уровень следует выносить минимум вопросов, которые определяют значительную экономию средств или когда иначе поступить невозможно.

Средний уровень (403)

К среднему уровню следует отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Примеры таких вопросов — отношение к передовым, но недостаточно проверенным технологиям: доступ к Internet (как сочетать свободу получения информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Нижний уровень (403)

Политика безопасности нижнего уровня касается конкретных сервисов. Она включает в себя два аспекта — цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая ПИБ должна быть гораздо детальнее.

Есть много вопросов, специфичных для отдельных сервисов, которые нельзя единым образом регламентировать в рамках всей организации. В то же время они настолько важны для обеспечения режима безопасности, что решения, относящиеся к ним, должны приниматься на управленческом, а не техническом уровне.

Приведем несколько примеров вопросов, на которые следует дать ответ при следовании политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей ПИБ нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна на них останавливаться. Ее цели должны быть конкретнее

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Однако слишком жесткие правила могут стать помехой в работе пользователей и, вероятно, их придется часто пересматривать.

Руководству следует найти компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а работники не окажутся чрезмерно скованы.

Политика верхнего и нижнего уровней...

Предмет политики (003)

Для того чтобы описать ПИБ для конкретной ИС, администраторы сначала должны определить область ограничений и условий в понятных всем терминах. Полезно указать цель или причины разработки ПИБ – это поможет добиться соблюдения политики.

Информация, циркулирующая в рамках ИС, является критически важной. ИС позволяет пользователям разделять программы и данные, что увеличивает риск. Следовательно, каждый из компьютеров, входящих в сеть, нуждается в более сильной защите.

ПИБ преследует две основные цели — продемонстрировать сотрудникам важность защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети, равно как и самой сети.

В отношении политики безопасности в Internet организации может понадобиться уточнение, охватывает ли эта политика все соединения, через которые ведется работа с Internet (напрямую или опосредованно) или собственно соединения Internet. Эта политика также может определять, учитываются ли другие аспекты работы в Internet, не имеющие отношения к безопасности, такие, как персональное использование соединений с Internet.

Описание позиции организации (003)

Как только предмет политики описан, даны определения основных понятий и рассмотрены условия применения политики, необходимо в явной форме описать позицию организации (т.е. решение ее руководства) по данному вопросу.

Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;

- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- предоставление пользователям достаточной информации для осознанного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия действующим законам и общеорганизационной политике безопасности.

Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще, стиль документов по политике безопасности, как и перечень этих документов, может быть существенно отличным для разных организаций.

Область применения (003)

ПИБ требует описания ее применимости. Это означает, что требуется уточнить, где, как, когда, кем и к чему применяется данная политика.

В сферу действия политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. ПИБ ориентирована также на пользователей, работающих с сетью, в том числе на субподрядчиков и поставщиков.

Следует специфицировать, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли организаций-субподрядчиков политика отношения к неофициальному программному обеспечению? Затрагивает ли она сотрудников, использующих портативные и домашние компьютеры и вынужденных переносить информацию на производственные ПК?

Управленческие меры обеспечения информационной безопасности (003)

Главная цель мер, предпринимаемых на управленческом уровне, — сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Использование информационных систем связано с определенной совокупностью рисков. Когда риск неоправданно велик, необходимо предпринять защитные меры. Периодическая переоценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

Претворение политики в жизнь [12]

Интересно

Не думайте, что как только ваша организация разработает большое число политик, директив или приказов, больше ничего не придется делать. Оглянитесь вокруг и посмотрите, соблюдаются ли формально написанные документы. Если нет, то можно либо попытаться изменить сам процесс разработки документов в организации (вообще трудно, но тем не менее возможно), либо оценить, где имеются проблемы с ее внедрением и устранять их. (Если выбрали второе, вероятно понадобятся формальные документы).

Большинство ПИБ обычно определяют то, что хочет большой начальник. Чтобы политика безопасности в Internet была эффективной, большой начальник должен понимать, какой выбор нужно сделать и делать его самостоятельно. Обычно, если большой начальник доверяет разработанной политике, она будет корректироваться с помощью неформальных механизмов.

Соблюдение политики (003)

ПИБ должна содержать общее описание запрещенных действий и наказаний за них.

Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения со стороны персонала будут рассматриваться руковод-

ством для принятия административных мер вплоть до увольнения.

Для ПИБ в Internet необходимо описание с некоторой степенью детальности, нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно описаны наказания и это должно быть увязано с общими обязанностями сотрудников в организации. Если к сотрудникам применяются наказания, они должны координироваться с соответствующими должностными лицами и отделами. Также может оказаться полезным поставить задачу конкретному отделу в организации наблюдения за соблюдением политики.

Разграничение доступа к объектам Web-сервиса (523)

В Web-серверах объектами доступа выступают универсальные локаторы ресурсов (URL — Uniform (Universal) Resource Locator). За этими локаторами могут стоять различные сущности — HTML-файлы, CGI-процедуры и т.п.

Как правило, субъекты доступа идентифицируются по IP-адресам и/или именам компьютеров и областей управления. Кроме того, можно использовать парольную аутентификацию пользователей или более сложные схемы, основанные на криптографических технологиях (об этом в следующем разделе).

В большинстве Web-серверов права разграничиваются с точностью до каталогов (директорий) с применением произвольного управления доступом. Могут предоставляться права на чтение HTML-файлов, выполнение CGI-процедур и т.д.

Для раннего выявления попыток нелегального проникновения в Web-сервер важен регулярный анализ регистрационной информации.

Разумеется, защита системы, на которой функционирует Web-сервер, должна следовать универсальным рекомендациям, главной из которых является максимальное упрощение. Все ненужные сервисы, файлы, устройства должны быть удалены. Число пользователей, имеющих прямой доступ к серверу, должно быть сведено к минимуму, а их привилегии — упорядочены в соответствии со служебными обязанностями.

Еще один общий принцип состоит в том, чтобы минимизировать объем информации о сервере, которую могут получить пользователи. Многие серверы в случае обращения по имени каталога и отсутствия файла index.HTML в нем, выдают HTML-вариант оглавления каталога. В этом оглавлении могут встретиться имена файлов с исходными текстами CGI-процедур или с иной конфиденциальной информацией. Такого рода “дополнительные возможности” целесообразно отключать, поскольку лишнее знание (злоумышленника) умножает печали (владельца сервера).

Аутентификация в открытых сетях (523)

Методы, применяемые в открытых сетях для подтверждения и проверки подлинности субъектов, должны быть устойчивы к пассивному и активному прослушиванию сети. Суть их сводится к следующему:

Субъект демонстрирует знание секретного ключа, при этом ключ либо вообще не передается по сети, либо передается в зашифрованном виде.

Субъект демонстрирует обладание программным или аппаратным средством генерации одноразовых паролей или средством, работающим в режиме “запрос — ответ”. Нетрудно заметить, что перехват и последующее воспроизведение одноразового пароля или ответа на запрос ничего не дает злоумышленнику.

Субъект демонстрирует подлинность своего местоположения, при этом используется система навигационных спутников.

Виртуальные частные сети (533)

Одной из важнейших задач является защита потоков корпоративных данных, передаваемых по открытым сетям. Открытые каналы могут быть надежно защищены лишь одним способом — криптографией.

Отметим, что так называемые выделенные линии не обладают особыми преимуществами перед линиями общего пользования в плане информационной безопасности. Выделенные линии хотя бы частично будут располагаться в неконтролируемой зоне, где их могут повредить или осуществить к ним несанкционированное подключение.

Единственное реальное достоинство — это гарантированная пропускная способность выделенных линий, а вовсе не какая-то повышенная защищенность. Впрочем, современные оптоволоконные каналы способны удовлетворить потребности многих абонентов, поэтому и указанное достоинство не всегда облечено в реальную форму.

Это важно

Любопытно упомянуть, что в мирное время 95% трафика Министерства обороны США передается через сети общего пользования (в частности через Internet). В военное время эта доля должна составлять “лишь” 70%. Можно предположить, что Пентагон — не самая бедная организация. Американские военные полагаются на сети общего пользования потому, что развивать собственную инфраструктуру в условиях быстрых технологических изменений — занятие очень дорогостоящее и бесперспективное, оправданное даже для критически важных национальных организаций только в исключительных случаях.

Представляется естественным возложить на межсетевой экран задачу шифрования и дешифрования корпоративного трафика на пути во внешнюю сеть и из нее. Чтобы такое шифрование/дешифрование стало возможным, должно произойти начальное распределение ключей. Современные криптографические технологии предлагают для этого целый ряд методов.

После того как межсетевые экраны осуществили криптографическое закрытие корпоративных потоков данных, территориальная разнесенность сегментов сети проявляется лишь в разной скорости обмена с разными сегментами. В остальном вся сеть выглядит как единое целое, а от абонентов не требуется привлечение каких-либо дополнительных защитных средств.

Управляемость системы (023)

Важнейшим аспектом информационной безопасности является управляемость системы.

Управляемость — это и поддержание высокой доступности системы благодаря раннему выявлению и ликвидации проблем, и возможность изменения аппаратной и программной конфигурации в соответствии с изменившимися условиями или требованиями, и оповещение о попытках нарушения информационной безопасности практически в реальном времени, и снижение числа ошибок администрирования, и многое, многое другое.

Наиболее остро проблема управляемости встает на клиентских рабочих местах и на стыке клиентской и серверной частей информационной системы. Причина проста — клиентских мест гораздо больше, чем серверных, они, как правило, разбросаны по довольно большей площади, их используют люди с разной квалификацией и привычками.

Обслуживание и администрирование клиентских рабочих мест — занятие чрезвычайно сложное, дорогое и чреватое ошибками. Замена и повторный ввод в эксплуатацию клиентского компьютера могут быть осуществлены очень быстро, поскольку это “клиенты без состояния”, у них нет ничего, что требовало бы длительного восстановления или конфигурирования.

На стыке клиентской и серверной частей находится Web-сервер. Это позволяет иметь единый механизм регистрации пользователей и наделения их правами доступа с последующим централизованным администрированием. Взаимодействие с многочисленными разнородными сервисами оказывается скрытым не только от пользователей, но и в значительной степени от системного администратора.

Безопасность программной среды (023)

Если заботиться о качестве пользовательского интерфейса, возникает необходимость в перемещении программ с Web-серверов на клиентские компьютеры — для создания анимации, выполнения семантического контроля при вводе данных и т.д. В каком бы направлении ни перемещались программы по сети, эти действия представляют повышенную опасность, поскольку программа, полученная из ненадежного источника, может содержать непреднамеренно внесенные ошибки или целенаправленно созданный зловредный код.

Такая программа потенциально угрожает всем основным аспектам информационной безопасности:

- доступности (программа может поглотить все наличные ресурсы);
- целостности (программа может удалить или повредить данные);
- конфиденциальности (программа может прочитать данные и передать их по сети).

Проблему ненадежных программ осознавали давно, но, пожалуй, только в рамках системы программирования Java впервые предложена целостная концепция ее решения.

Java предлагает три оборонительных рубежа:

- надежность языка;
- контроль при получении программ;
- контроль при выполнении программ.

Впрочем, существует еще одно, очень важное средство обеспечения информационной безопасности — беспрецедентная открытость Java-системы. Исходные тексты Java-компилятора и интерпретатора доступны для проверки, поэтому велика вероятность, что ошибки и недочеты первыми будут обнаруживать честные специалисты, а не злоумышленники.

Безопасность программной среды...

В концептуальном плане наибольшие трудности представляет контролируемое выполнение программ, загруженных по сети. Прежде всего, необходимо определить, какие действия допустимы для таких программ.

Интересный подход

Интересно

Интересный подход предлагают специалисты компании Sun Microsystems для обеспечения безопасного выполнения командных файлов. Речь идет о среде Safe-Tcl (Tool Comman Language, инструментальный командный язык). Sun предложила так называемую ячеечную модель интерпретации командных файлов. Существует главный интерпретатор, которому доступны все возможности языка. Если в процессе работы приложения необходимо выполнить сомнительный командный файл, порождается подчиненный командный интерпретатор, обладающий ограниченной функциональностью (например, из него могут быть удалены средства работы с файлами и сетевые возможности).

В результате потенциально опасные программы оказываются заключенными в ячейки, защищающие пользовательские системы от враждебных действий. Для выполнения действий, которые считаются привилегированными, подчиненный интерпретатор может обращаться с запросами к главному.

Здесь, очевидно, наблюдается аналогия с разделением адресных пространств операционной системы и пользовательских процессов и использованием последними системных вызовов. Подобная модель уже около 30 лет является стандартной для многопользовательских ОС.

Роли и обязанности (003)

Нужно описать обязанности ответственных должностных лиц в отношении разработки и внедрения различных аспектов политики. Для такого сложного вопроса, как безопасность в Internet, организации может потребоваться ввести ответственных за анализ безопасности различных архитектур или за утверждение использования той или иной архитектуры.

В “политический” документ необходимо включить информацию о должностных лицах, отвечающих за проведение в жизнь политики безопасности. Например, если для использования работником неофициального программного обеспечения нужно официальное разрешение, то должно быть известно, у кого и как его следует получать. Если должны проверяться дискеты, принесенные с других компьютеров, необходимо описать процедуру проверки. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Перечисленные группы людей отвечают за реализацию сформулированных ранее целей.

Руководители подразделений ответственны за доведение положений политики безопасности до пользователей и за контакты с ними.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.

Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчинятся распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

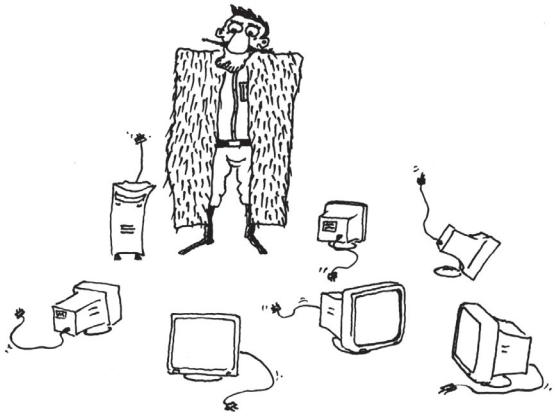
Руководители подразделений обязаны (023):

Постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же делали их подчиненные.

Проводить анализ рисков, выявляя активы, требующие защиты, и уязвимые места систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты.

Организовать обучение персонала мерам безопасности. Обратить особое внимание на вопросы, связанные с антивирусным контролем.

Информировать администраторов локальной сети и администраторов сервисов об изменении статуса каждого из подчиненных (переход на другую работу, увольнение и т.п.).



Руководитель обязан постоянно держать в поле зрения...

Позаботьтесь, чтобы каждый компьютер в подразделениях имел хозяина или системного администратора, отвечающего за безопасность и имеющего достаточную квалификацию для выполнения этой роли.

Администраторы локальной сети обязаны (023):

Информировать руководство об эффективности существующей политики безопасности и о технических мерах, которые могут улучшить защиту.

Обеспечить защиту оборудования локальной сети, в том числе интерфейсов с другими сетями.

Оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попытках нарушения защиты. Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания.

Использовать проверенные средства аудита и обнаружения подозрительных ситуаций.

Ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности.

Следить за новинками в области информационной безопасности, сообщать о них пользователям и руководству.

Не злоупотреблять данными им полномочиями. Пользователи имеют право на тайну.

Разработать процедуры и подготовить инструкции для защиты локальной сети от зловредного программного обеспечения. Оказывать помощь в обнаружении и ликвидации зловредного кода.

Регулярно выполнять резервное копирование информации, хранящейся на файловых серверах.

Выполнять все изменения сетевой аппаратно-программной конфигурации.

Гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам.

Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм.

Периодически осуществлять проверку надежности защиты локальной сети. Не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов обязаны (023):

Управлять правами доступа пользователей к обслуживаемым объектам.

Регулярно выполнять резервное копирование информации, обрабатываемой сервисом.

Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм.

Ежедневно анализировать регистрационную информацию, относящуюся к сервису.

Регулярно контролировать сервис на предмет зловредного программного обеспечения.

Периодически проверять надежность защиты сервиса. Не допускать получения привилегий неавторизованными пользователями.

Пользователи обязаны (023):

Знать и соблюдать законы, правила, политику безопасности, процедуры безопасности.

Использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации.

Использовать механизм защиты файлов и должным образом задавать права доступа.

Правильно выбирать пароли, регулярно менять их. Не записывать пароли на бумаге, не сообщать их другим лицам.

Помогать другим пользователям соблюдать меры безопасности. Указывать им на упущения.

Информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях.

Не использовать слабости в защите сервисов и локальной сети в целом.

Не совершать неавторизованной работы с данными, не создавать помех другим пользователям.

Не пытаться работать от имени других пользователей.

Обеспечивать резервное копирование информации с жесткого диска своего компьютера.

Знать принципы работы зловредного программного обеспечения, пути его проникновения и распространения, слабости, которые при этом могут быть использованы.

Знать и выполнять процедуры для предупреждения проникновения зловредного кода, для его обнаружения и уничтожения.

Знать слабости, которые используются для неавторизованного доступа, а также способы выявления нештатного поведения конкретных систем, последовательность дальнейших действий, точки контакта с ответственными лицами.

Соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Некоторые замечания по поводу ПИБ

ПИБ должна быть наглядной, что способствует реализации политики, ее знанию и пониманию всеми сотрудниками организации. Презентации, видеофильмы, семинары, вечера вопросов и ответов, статьи во внутренних изданиях организации увеличивают ее наглядность. Программа обучения в области компьютерной безопасности и контрольные проверки действий в тех или иных ситуациях могут эффективно уведомить всех пользователей о новой политике. С ней следует ознакомить всех новых сотрудников организации.

Политика безопасности должна иметь гарантию поддержки со стороны руководителей отделов, особенно, если на сотрудников постоянно сыплется масса политик, директив, рекомендаций и приказов. Кроме того, ПИБ должна быть согласована с другими действующими директивами, законами, приказами и общими задачами организации. Она также должна быть интегрирована в другие политики и согласована с ними (например, политикой по приему на работу). Одним из способов координации политик является согласование их с другими отделами в ходе разработки.

Надо знать

ПИБ может быть написана только для группы людей с близкими целями. Поэтому организации может потребоваться разделиться на части, если она слишком велика или имеет слишком различные цели, чтобы стать субъектом политики безопасности в Internet.

Internet — это как бы электронная дверь в организацию. В одну и ту же дверь может войти как с добром, так и со злом. Организация, территория которой открыта для входа, наверное, уже приняла решение на основе анализа рисков, что открытость либо необходима для выполнения своих задач, либо угроза так мала, что ею можно пренебречь.

Аналогичная логика применима к электронной двери. Тем не менее, существуют серьезные отличия. Физические угрозы более привязаны к конкретному физическому месту. А связь с Internet — это связь со всем миром. Организация, которая находится в спокойном и безопасном месте, может разрешать вход на свою территорию, но иметь строгую политику в отношении Internet.

Internet может быть формой для связи с обществом. Многие организации инструктируют сотрудников о поведении с корреспондентами или с людьми на работе. Эти правила уместно перенести и на электронное взаимодействие. Многие сотрудники не понимают общественного характера Internet.

Internet — это не единственная глобальная сеть. Организации используют телефонные и другие глобальные сети (например, SPRINT) для организации доступа удаленных пользователей к своим внутренним системам. При соединении с Internet и телефонной сетью существуют аналогичные угрозы и уязвимые места.

Поиск информации в Internet с помощью браузера (003)

Существует ряд рисков, связанных с использованием WWW-браузеров для поиска и получения информации из Internet. Программы WEB-браузеров очень сложны и станут еще сложнее. Чем сложнее программа, тем менее она безопасна. Ошибки в ней могут использоваться для сетевых атак.

Программы для поиска и просмотра информации в Internet (WWW, Gopher, WAIS, и др.) предоставляются сотрудникам в основном для более эффективного исполнения ими должностных обязанностей.

Все программы, используемые для доступа к WWW, должны быть утверждены сетевым администратором и на них должны быть установлены все доработки производителя(patch), связанные с безопасностью.

Все файлы, загружаемые с помощью WWW, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.

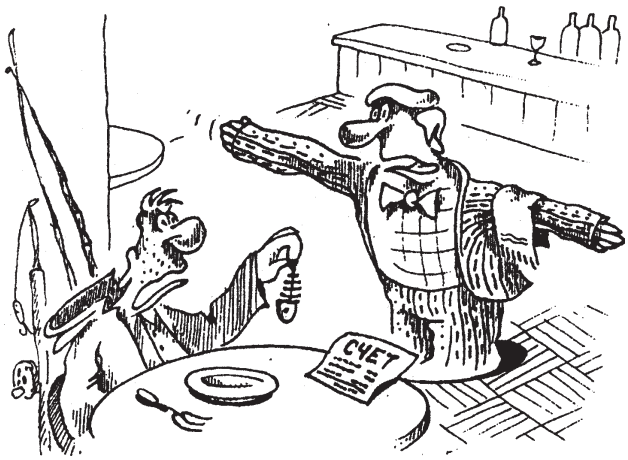
Во всех браузерах должна быть запрещена обработка с применением Java, Javascript и ActiveX из-за небезопасности данных технологий.

Могут использоваться или загружаться только версии браузеров, использование которых разрешено в организации. Другие версии могут содержать вирусы или ошибки.

Все WEB-браузеры должны быть сконфигурированы так, чтобы использовать прокси-сервер для WWW из состава брандмауэра.

Доступ к Internet должен осуществляться только через HTTP-прокси.

WEB-страницы часто содержат формы. Как и электронная почта, данные, посылаемые WEB-браузером на WEB-сервер, проходят через многие промежуточные



ПИБ должна быть наглядной...

компьютеры и сети до того, как достигнут своего конечного назначения. Любая важная информация, посылаемая с помощью ввода данных на WEB-странице, может быть перехвачена.

ПИБ для WEB-сервера (003)

Многие организации поддерживают внешние WWW-сайты, описывающие их компанию или сервисы, что является одной из форм создания имиджа и репутации компании.

По причинам безопасности эти серверы обычно размещаются за брандмауэром компании.

Кроме того, внутренние WEB-сайты компании, расположенные внутри брандмауэра организации, часто используются для рассылки информации компании сотрудникам. Это — поздравления с днем рождения, графики мероприятий, телефонные справочники и т.д. Внутренние WEB-сайты также используются для распространения внутренней информации о проектах, являясь иногда центром информации для исследовательских групп.

Хотя внутренние WEB-сайты не являются так же видимыми, как внешние страницы, они должны администрироваться с помощью специально разработанных руководств и директив. Руководители групп должны отвечать за это.

Независимо от того, как администрируется WEB-сайт, все пользователи, исполняющие эти обязанности, должны претворять в жизнь политику компании, разработанную ее руководством.

Приведем ***перечень правил, которые следует выполнять в рамках ПИБ*:**

- пользователям запрещено устанавливать или запускать WEB-серверы;
- в отношении WEB-страниц необходимо соблюдать установленный в организации порядок утверждения документов, отчетов, маркетинговой информации и т.д.;
- WEB-сервер и любые данные, являющиеся публично доступными, должны быть размещены за пределами брандмауэра организации;
- WEB-серверы должны быть сконфигурированы так, чтобы пользователи не могли устанавливать CGI-скрипты;
- все сетевые приложения, кроме HTTP, должны быть отключены (SMTP, FTP и т.д.);
- информационные серверы должны быть размещены в защищенной подсети для изоляции их от других систем организации. Это уменьшает вероятность того, что информационный сервер будет скомпрометирован и использован для атаки на другие системы организации;
- при использования средств администрирования с помощью WWW, следует ограничить доступ к нему только авторизованных систем (с помощью IP-адресов, а не имен хостов); всегда меняйте пароли по умолчанию;
- пользователям запрещено загружать, устанавливать или запускать программы WEB-серверов;
- обязателен контроль сетевого трафика для выявления неавторизованных WEB-серверов; операторы которых подвергаются дисциплинарным наказаниям;
- руководство организации должно дать в письменном виде разрешение на работу WEB-сервера, подключенного к Internet;
- содержимое WEB-серверов компании, присоединенных к Internet, должно быть утверждено и установлено WEB-мастером;
- конфиденциальная информация не должна быть доступна посредством WEB-сайта;
- к информации, размещенной на WEB-сервере, применимы все законы о ее защите. Поэтому перед размещением информации в Internet, она должна быть просмотрена и утверждена так же, как утверждаются бумажные официальные документы организации. Должны быть защищены авторские права и получено разрешение на публикацию информации на WEB-сайте.
- все публично доступные WEB-сайты должны регулярно тестироваться на предмет корректности ссылок и не должны находиться в состоянии “under construction”. При реконструкции областей они должны становиться недоступными.
- не должно быть средств удаленного управления WEB-сервером (т.е. с мест, отличных от консоли). Все действия администратора должны выполняться только с консоли. Вход в систему с удаленного терминала с правами суперпользователя должен быть запрещен.
- программы WEB-серверов и операционной системы, под управлением которой работает WEB-сервер, должны содержать все исправления, рекомендованные производителем для этой версии.
- входящий трафик HTTP следует сканировать, а о случаях появления неавторизованных WEB-серверов – докладываться.
- ограничение доступа к информации пользователями, адрес которых заканчивается на.GOV или.COM, обеспечивает минимальную защиту для информации, не разрешенной для общего показа. Может использоваться отдельный сервер или отдельная часть для информации с ограниченным доступом.
- за всеми WEB-сайтами должен осуществляться контроль как составная часть администрирования сети.

Действия всех пользователей, заподозренных в некорректном использовании Internet, могут быть запротоколированы для обоснования применения к ним в дальнейшем административных санкций.

- на UNIX-системах WEB-серверы не должны запускаться с правами суперпользователя.
- разработка и использование CGI-скриптов подлежат контролю. CGI-скрипты не должны обрабатывать входные данные без их проверки. Любые внешние программы, запускаемые с параметрами в командной строке, не должны содержать метасимволов. Разработчики отвечают за использование правильных регулярных выражений для сканирования метасимволов командного процессора и их удаление перед передачей входных данных программы на сервере и операционной системе.
- все WWW-серверы организации, подключенные к Internet, должны находиться между брандмауэром и внутренней сетью организации. Любые внутренние WWW-серверы организации, обеспечивающие работу критических приложений организации должны быть защищены внутренними брандмауэрами. Критическая, конфиденциальная и персональная информация никогда не должны храниться на внешнем WWW-сервере.

Краткое содержание документов ПИБ (003)

"**Концепция обеспечения информационной безопасности в ИС**" содержит:

- общую характеристику объекта защиты (описание состава, функций и существующей технологии обработки данных в типовой ИС);
- формулировку целей создания системы защиты, основных задач обеспечения информационной безопасности и путей достижения целей (решения задач);
- перечень типичных угроз информационной безопасности и возможных путей их реализации, неформальная модель вероятных нарушителей;
- основные принципы и подходы к построению системы обеспечения информационной безопасности, меры, методы и средства достижения целей защиты.

"**План защиты" от несанкционированного доступа к информации** и незаконного вмешательства в процесс функционирования ИС содержит:

- определение целей, задач защиты информации в ИС и основных путей их достижения (решения);
- требования к организации и проведению работ по защите информации в ИС,
- описание применяемых мер и средств защиты информации от рассматриваемых угроз, общих требований к настройкам применяемых средств защиты информации от НСД;
- распределение ответственности за реализацию "Плана защиты ИС" между должностными лицами и структурными подразделениями организации.

"Положение о категорировании ресурсов ИС**"** содержит:

- формулировку целей введения классификации ресурсов (АРМ, задач, информации, каналов передачи) по степеням (категориям) защищенности;
- предложения по числу и названиям категорий защищаемых ресурсов и критериям классификации ресурсов по требуемым степеням защищенности (категориям);
- определение мер и средств защиты информации, обязательных и рекомендуемых к применению на АРМ различных категорий;
- общие положения, специальные термины и определения, встречающиеся в документе;
- образец формуляра ЭВМ (для учета требуемой степени защищенности (категории), комплектации, конфигурации и перечня решаемых на ЭВМ задач);
- образец формуляра решаемых на ЭВМ ИСфункциональных задач (для учета их характеристик, категорий пользователей задач и их прав доступа к информационным ресурсам данных задач).

"**Порядок обращения с информацией, подлежащей защите**" содержит:

- определение основных видов защищаемых (конфиденциальных) сведений (информационных ресурсов);
- общие вопросы организации учета, хранения и уничтожения документов и магнитных носителей конфиденциальной информации;
- порядок передачи (предоставления) конфиденциальных сведений третьим лицам;
- определение ответственности за нарушение установленных правил обращения с защищаемой информацией;
- форму типового Соглашения (обязательства) сотрудника организации о соблюдении требований обращения с защищаемой информацией.

"**План обеспечения непрерывной работы и восстановления**" включает:

- общие положения (назначение документа);
- классификацию возможных (значимых) кризисных ситуаций и указание источников получения информации о возникновении кризисной ситуации;
- перечень основных мер и средств обеспечения непрерывности процесса функционирования ИС и своевременности восстановления ее работоспособности;

- общие требования к подсистеме обеспечения непрерывной работы и восстановления;
- типовые формы для планирования резервирования ресурсов подсистем ИС и определения конкретных мер и средств обеспечения их непрерывной работы и восстановления;
- порядок действий и обязанности персонала по обеспечению непрерывной работы и восстановлению работоспособности системы.

"**Положение об отделе технической защиты информации**" содержит:

- общие положения, руководство отделом;
- основные задачи и функции отдела;
- права и обязанности начальника и сотрудников отдела, ответственность;
- типовую организационно-штатную структуру отдела.

"**Обязанности администратора информационной безопасности подразделения**" содержат:

- основные права и обязанности по поддержанию требуемого режима безопасности;
- ответственность за реализацию принятой политики безопасности в пределах своей компетенции.

"**Памятка пользователю**"

Определяет общие обязанности сотрудников подразделений при работе со средствами ИС и ответственность за нарушение установленных порядков.

"**Инструкция по внесению изменений в списки пользователей**"

Определяет процедуру регистрации, предоставления или изменения прав доступа пользователей к ресурсам ИС.

"**Инструкция по модификации технических и программных средств**"

Регламентирует взаимодействие подразделений Организации по обеспечению безопасности информации при проведении модификаций программного обеспечения и технического обслуживания средств вычислительной техники.

"**Инструкция по организации парольной защиты**"

Регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе Организации, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

"**Инструкция по организации антивирусной защиты**" содержит:

- требования к закупке, установке антивирусного программного обеспечения;
- порядок использования средств антивирусной защиты, регламенты проведения проверок и действия персонала при обнаружении вирусов;
- распределение ответственности за организацию и проведение антивирусного контроля.

"**Инструкция по работе с ключевыми дискетами (ключами шифрования)**" содержит:

- порядок изготовления, работы, хранения ключевых дискет и уничтожения ключевой информации;
- обязанности и ответственность сотрудников по использованию и сохранности ключевой информации;
- формы журналов учета ключевых дискет;
- порядок действий персонала в случае утери, порчи ключевой дискеты, компрометации ключевой информации.

Резюме

Политика информационной безопасности — набор законов, правил и практических рекомендаций и практического опыта, определяющих управленческие и проектные решения в области ЗИ. На основе ПИБ строится управление, защита и распределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Ниже перечислен ряд весьма простых действий, которые могут значительно повысить степень защиты корпоративной сети без больших финансовых вливаний:

1. Более тщательный контроль за персоналом, в особенности за самыми низкооплачиваемыми работниками, например уборщиками и охранниками.

2. Аккуратная незаметная проверка послужного списка нанимаемого работника, которая поможет избежать возникновения проблем в будущем.

3. Ознакомление нанимаемого сотрудника с документами, описывающими политику компании в области информационной безопасности, и получение от него соответствующей расписки.

4. Изменение содержимого всех экранов для входа в систему таким образом, чтобы они отражали политику компании в области защиты данных (эта мера настоятельно рекомендуется Министерством юстиции США).

5. Повышение уровня физической защиты.

6. Блокировка всех дисководов гибких дисков в организациях, в которых установлена сеть, – это позволит минимизировать риск компьютерных краж и заражения вирусами.

7. Признание за сотрудниками определенных прав при работе с компьютерами, например организация досок объявлений, соблюдение конфиденциальности электронной почты, разрешение использовать определенные компьютерные игры.

Цель политики безопасности для Internet – принять решение о том, как организация собирается защищаться. ПИБ обычно состоит из двух частей – общих принципов и конкретных правил работы(которые эквивалентны специфической политике, описанной ниже). Общие принципы определяют подход к безопасности в Internet. Правила же определяют что разрешено, а что – запрещено. Правила могут дополняться конкретными процедурами и различными руководствами.

Internet при проектировании и не задумывался как защищенная сеть, поэтому его проблемами в текущей версии TCP/IP являются:

- Легкость перехвата данных и фальсификации адресов машин в сети – основная часть трафика Internet – это нешифрованные данные. E-mail, пароли и файлы могут быть перехвачены, используя легко доступные программы.
- Уязвимость средств TCP/IP – ряд средств TCP/IP не был спроектирован быть защищенными и может быть скомпрометирован квалифицированными злоумышленниками; средства, используемые для тестирования особенно уязвимы.
- Отсутствие политики – многие сайты по незнанию сконфигурированы таким образом, что предоставляют широкий доступ к себе со стороны Internet, не учитывая возможность злоупотребления этим доступом; многие сайты разрешают работу большего числа сервисов TCP/IP, чем им требуется для работы и не пытаются ограничить доступ к информации о своих компьютерах, которая может помочь злоумышленникам.
- Сложность конфигурирования – средства управления доступом хоста сложны; зачастую сложно правильно сконфигурировать и проверить эффективность установок . Средства, которые по ошибке неправильно сконфигурированы, могут привести к неавторизованному доступу.

Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения со стороны персонала должны рассматриваться руководством для принятия мер вплоть до увольнения.

Для ПИБ в Internet необходимо описание, с некоторой степенью детальности, нарушений , которые неприемлемы, и последствий такого поведения. Могут быть явно описаны наказания и это должно быть увязано с общими обязанностями сотрудников в организации. Если к сотрудникам применяются наказания, они должны координироваться с соответствующими должностными лицами и отделами. Также может оказаться полезным поставить задачу конкретному отделу в организации следить за соблюдением политики.