1. Введение

Информация имеет первостепенное значение. Современное общество называют информационным.

В 1972 году американский специалист в области связи и вычислительной техники Роберт Фано говорил: «Стремление сохранить тайну предприятий и отдельных лиц – не единственный повод для поиска надежных средств обеспечения неприкосновенности информации, хранимой в вычислительных системах, а также для поиска средств контроля над ее применением. Такие средства требуются также для выполнения договорных обязательств, заключаемых между создателями программного обеспечения и банков данных, с одной стороны, и потребителями этой продукции, с другой. Следует иметь в виду и то, что бесконтрольный сбор, хранение и распределение информации неизбежно сопровождается «загрязнением» информационной среды – явлением, которое уже начало приводить если не к серьезным, то, во всяком случае, к тревожным последствиям. Наконец, соображения общественной безопасности диктуют необходимость надежного контроля над информацией, способной оказаться источником угрожающего положения, скажем вследствие распространения среди населения панических настроений либо вследствие потворствования незаконным действиям»

Проблема безопасности информационных технологий (ИТ) возникла на пересечении двух активно развивающихся направлений – безопасности технологий и информатизации.

Обеспечение собственной безопасности – задача первостепенной важности для любой системы независимо от ее сложности и назначения, будь то биологический организм или система обработки информации. Однако, когда средства нападения имеют форму информационных воздействий, необходимо разрабатывать и применять совершенно новые технологии, методы зашиты.

Научные и технические предпосылки кризисной ситуации.

Современные компьютеры приобрели гигантскую вычислительную мощь, но одновременно с этим стали и проще в эксплуатации.

Все большее количество новых (и неквалифицированных) людей получает доступ к компьютерам, что приводит к снижению средней квалификации пользователей. Большинство пользователей имеют личные компьютеры и осуществляют их администрирование самостоятельно. Они не в состоянии постоянно поддерживать безопасность своих систем на должном уровне, т.к. это требует соответствующих знаний, времени и средств. Распространение сетевых технологий объединило отдельные машины в локальные сети, совместные использующие общие ресурсы, а применение технологий клиент-сервер и кластеризации преобразовало такие сети в распределенные вычислительные среды.

Безопасность сети определяется защищенностью всех входящих в нее компьютеров и сетевого оборудования и достаточно нарушить работу только одного компьютера, чтобы скомпрометировать всю сеть.

Если компьютер, который является объектом атаки, подключен к глобальной вычислительной сети (Internet), то независимо от характера обрабатываемой в нем информации то не имеет значения, где он находится – в соседней комнате или на другом континенте.

Бурное развитие программного обеспечения

В настоящее время большинство операционных систем не отвечает требованиям безопасности, хотя в последнее время и осуществляют определенные усилия в этом направлении. Существует огромное количество различных недокументированных возможностей, обеспечивающих реализацию намеренных злоумышленных действий.

Развитие гибких и мобильных технологий привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов. Теперь любое развитое приложение не просто обрабатывает данные, а интерпретирует интегрированные в них инструкции специальных языков программирования, т.е. по сути дела является отдельной

машиной с привычной фон-неймановской архитектурой, для которых можно создавать средства нападения. Это увеличивает возможности злоумышленников и затрудняет задачу зашиты таких систем, т.к. наличие «вложенных» систем требует и реализации защиты для каждого уровня.

Несоответствие бурного развития средств обработки информации и медленного процесса разработки теории информационной безопасности привело к разрыву между теоретическими моделями, оперирующими абстрактными понятиями и реальными категориями современных информационных технологий. Кроме того, многие средства защиты (например, средства борьбы с компьютерными вирусами) и системы защиты корпоративных систем на данный момент вообще не имеют системной научной базы. Такое положение является следствием отсутствия общей теории защиты информации, комплексных моделей безопасности обработки информации, отсутствие средств, позволяющих эффективно промоделировать адекватность тех или иных решений в области безопасности. Сегодня нет даже общепринятой терминологии, адекватно воспринимаемой всеми специалистами в области безопасности.

Необходимость создания глобального информационного пространства и обеспечение безопасности протекающих в нем процессов потребовала разработки международных стандартов, следование которым может обеспечить необходимый уровень гарантий обеспечения ИБ. Причем в современных условиях важным является не только стандартизация требований безопасности, но и обоснование их применения, а также методов подтверждения адекватности реализованных средств защиты и корректности самой реализации.

Перед разработчиками современных ИС стоят следующие задачи:

- Обеспечение безопасности новых типов информационных ресурсов. Это означает, что системы защиты должны обеспечивать безопасность не отдельных документов, файлов или сообщений, а решать задачи ИБ на уровне информационных ресурсов (Например, гипертекст, мультимедиа).

Гипертекст – информационный массив, на котором заданы и автоматически поддерживаются ассоциативные и смысловые связи между выделенными элементами, понятиями, терминами или разделами.

Мультимедиа – комплексное представление информации – вывод данных в текстовом, графическом, видео, аудио, мультипликационном видах.

- Организация доверенного взаимодействия сторон.
- Защита от автоматических средств нападения – разрушающих программных средств (РПС) т.е. компьютерных вирусов, «троянских коней» программных закладок. Средства разграничения доступа не решают в полной мере этой проблемы.
- Интеграция защиты информации в процессе автоматизации ее обработки в качестве обязательного элемента. Это означает, что средства безопасности не должны вступать в конфликт с существующими приложениями и сложившимися технологиями обработки информации, а напротив, должны стать неотъемлемой частью этих средств и технологий.

Понятие «защищенная система»

Защищенная система обработки информации для определенных условий эксплуатации обеспечивает безопасность (конфиденциальность и целостность) обрабатываемой информации и поддерживает свою работоспособность в условиях воздействия на нее заданного множества угроз.

Защищенная система должна обладать следующими свойствами:

- Она должна автоматизировать процесс обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности.
- Успешно и эффективно противостоять угрозам безопасности.

Соответствовать требованиям и критериям стандартов информационной безопасности.
Наличие общепринятых стандартов позволяет согласовать подходы различных участников процесса создания защищенных систем (требования потребителей, технологии и методы производителей, критерии независимой экспертизы).

Информационная безопасность, актуальность ее обеспечения

Общее содержание проблемы информационной безопасности

Безопасность – это такое состояние рассматриваемой системы, при котором она с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – ее наличие и функционирование не создает угроз для элементов самой системы и внешней среды.

Меры безопасности системы:

- с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз. Степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования под воздействием дестабилизирующих факторов;
- с точки зрения отсутствия угроз для элементов системы и внешней среды. Степень (уровень) возможности (или отсутствия возможности) появления таких дестабилизирующих факторов, которые могут представить угрозу элементам самой системы или внешней среде.

Информация, как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т.е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой сама может быть источником большого числа разноплановых угроз как для элементов самой системы, так и для внешней среды.

Обеспечение информационной безопасности может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

- защиты находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз;
- защиты элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;
- защиты внешней среды от информационных угроз со стороны рассматриваемой системы.

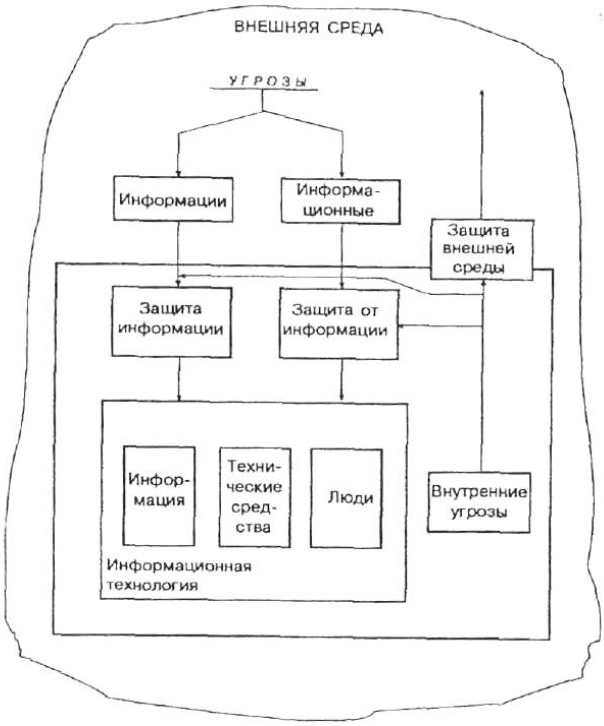

Рис. 1.1. Общая схема обеспечения информационной безопасности

Защита от информации заключается в использовании специальных методов и средств в целях предупреждения или нейтрализации негативного воздействия на элементы рассматриваемой системы (людей и технических комплексов) информации как имеющейся (генерируемой, хранимой, обрабатываемой и используемой) внутри системы, так и поступающей из внешней среды (защита системы от информации), а также предупреждение негативного воздействия выходной информации системы на элементы внешней среды (информационная экология).

Информация и информационные отношения. Субъекты информационных отношений

Информация – это сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной области, используемые (необходимые) для оптимизации принимаемых решений в процессе управления данными объектами.

Отношения между субъектами будем называть информационными отношениями, а самих участвующих в них субъектов - субъектами информационных отношений.

Автоматизированная система обработки информации (АС) – организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки в виде соответствующего программною обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- персонала и пользователей системы, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки информации (данных) с целью удовлетворения информационных потребностей субъектов информационных отношений.

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

Субъекты по отношению к определенной информации могут выступать в качестве:

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Для успешного осуществления своей деятельности по управлению объектами некоторой предметной области субъекты информационных отношений могут быть заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации;
- конфиденциальности определенной части информации;
- достоверности информации;
- защиты от навязывания им ложной информации;
- защиты части информации от незаконного ее тиражирования;
- разграничения ответственности за нарушения законных прав других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

Поэтому под безопасностью автоматизированной системы обработки информации (компьютерной системы) будем понимать защищенность всех ее компонентов (технических средств, программного обеспечения, данных и персонала) от подобного рода нежелательных для соответствующих субъектов информационных отношений воздействий.

Безопасность любого компонента (ресурса) АС складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента системы предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Ценность информации

Под ценностью информации понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте.

Среди подходов к построению моделей защиты ИС, основанных на понятии ценности информации наиболее известными являются: оценка, анализ и управление рисками, порядковые шкалы ценностей, модели решетки ценностей.

Пример

При оценке ценности информации в государственных структурах используется линейная порядковая шкала ценностей. Всю информацию сравнивают экспертным путем и относят к различным уровням ценности. В этом случае документам, отнесенным к некоторому уровню по шкале, присваиваются соответствующие грифы секретности. Сами грифы секретности образуют порядковую шкалу, например, (принятую почти всеми государствами): НЕСЕКРЕТНО <КОНФИДЕНЦИАЛЬНО <СЕКРЕТНО <СОВЕРШЕННО СЕКРЕТНО. Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

Рассматриваемая шкала хронологически была самой ранней и перестала удовлетворять требованиям ИТ, более детальной классификации. Разработка формализованных моделей информационных систем привело к разработке ценностной модели в виде решетки ценностей, которая является обобщением порядковой шкалы. Ее элементы представляют дискретную модель на базе введенной алгебры: с требованиями рефлексивности, транзитивности, антисимметричности, а также верхней и нижней грани.

Модель решетки ценностей

Пусть дано SC - конечное частично упорядоченное множество относительно бинарного отношения <, т.е. для каждых A, B, C выполняется

1) рефлексивность: A<A,

2) транзитивность: A<B, B<C==>A<C,

3) антисимметричность: A<B, B<A => A=B.

Определение 1.8. Для A, B$\in$SC элемент C=A$\oplus$B$\in$SC называется наименьшей верхней границей (верхней гранью), если

1) A<C, B<C;

2) A<D, B<D$\Rightarrow$C<D для всех D$\in$SC.

Элемент A$\oplus$B, вообще говоря, может не существовать. Если наименьшая верхняя граница существует, то из антисимметричности следует единственность.

Определение 1.9. Для A, B$\in$C элемент E=A$\otimes$B$\in$SC называется наибольшей нижней границей (нижней гранью), если

1) E<A, E<B;

2) D<A, D<B$\Rightarrow$D<E.

Эта граница также может не существовать. Если она существует, то из антисимметричности следует единственность.

Определение 1.10. (SC, <) называется решеткой, если для любых A, B$\in$SC существует A$\oplus$B$\in$SC и A$\otimes$B$\in$SC.

Лемма. Для любого набора S={A_1,...,A_n } элементов из решетки SC существуют единственные элементы,:

$\oplus$S=$A_1\oplus$...$\oplus A_n$ - наименьшая верхняя граница S;

$\otimes S=A_1\otimes...\otimes A_n$ - наибольшая нижняя граница S.

Для всех элементов SC в конечных решетках существует верхний элемент High = $\oplus$SC, аналогично существует нижний элемент Low = $\otimes$SC.

Определение 1.11. Конечная линейная решетка - это линейно упорядоченное множество, можно всегда считать {0, 1 ,..., n}=SC .

Для большинства встречающихся в теории защиты информации решеток существует представление решетки в виде графа. Рассмотрим корневое дерево на вершинах из конечного множества $X=\{X_1, X_2...X_n\}$с корнем в X_i. Пусть на единственном пути, соединяющем вершину X_1 с корнем, есть вершина X_j. Положим по определению, что $X_i<X_j$. Очевидно, что таким образом на дереве определен частичный порядок. Кроме того, для любой пары вершин X_i и X_j существует элемент $X_i\oplus X_j$, который определяется точкой слияния путей из X_i и X_j в корень. Однако такая структура не является решеткой, т.к. здесь нет нижней грани. Оказывается, что от условия единственности пути в корень можно отказаться, сохраняя при этом свойства частичного порядка и существование верхней грани. Например, добавим к построенному дереву вершину L, соединив с ней все концевые вершины. Положим i=l,...,n, $L<X_j$. Для остальных вершин порядок определяется как раньше. Построенная структура является решеткой.

Приведенный пример не исчерпывает множество решеток, представимых в виде графов, однако поясняет как связаны графы и решетки. Не всякий граф определяет решетку.
MLS решетка

Название происходит от аббревиатуры Multilevel Security и лежит в основе государственных стандартов оценки информации. Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X, т.е. (α,β), (α',β') -элементы произведения, $\beta,\beta'\in$L - линейная решетка, $\alpha,\alpha'\in$SC - решетка подмножеств некоторого множества X. Тогда

$(\alpha,\beta)<(\alpha',\beta')\Leftrightarrow\alpha\subseteq\alpha',\beta<\beta'$

Верхняя и нижняя границы определяются следующим образом:

$(\alpha,\beta)\oplus(\alpha',\beta')\Leftrightarrow(\alpha\cup\alpha',\max\{\beta,\beta'\})$,

$(\alpha,\beta)\otimes(\alpha',\beta')\Leftrightarrow(\alpha\cap\alpha',\min\{\beta,\beta'\})$.

Вся информация {объекты системы} отображается в точки решетки $\{(a,\beta)\}$. Линейный порядок, как правило, указывает гриф секретности. Точки множества X обычно называются категориями.

Свойства решетки в оценке информации существенно используются при классификации новых объектов, полученных в результате вычислений. Пусть дана решетка ценностей SC, множество текущих объектов O, отображение C: 0→S, программа использует информацию объектов $0_1,..,0_n$, которые классифицированы точками решетки $C(0_1),...,C(0_n)$. В результате работы программы появился объект O, который необходимо классифицировать. Это можно сделать, положив $C(0)= C(0_1)\oplus...\oplus C(0_n)$. Такой подход к классификации наиболее распространен в государственных структурах. Например, если в сборник включаются две статьи с грифом секретно и совершенно секретно соответственно, и по тематикам: первая - кадры, вторая - криптография, то сборник приобретает гриф совершенно секретно, а его тематика определяется совокупностью тематик статей (кадры, криптография).

Определение требований к защищенности информации

Исторически сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации - ее конфиденциальности (секретности). Требования же к обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что раз к информации имеет доступ только узкий круг доверенных лиц, то вероятность ее искажения (несанкционированного уничтожения) незначительна.

Если такой подход в какой-то степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации, то это вовсе не

означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

Во многих областях деятельности (предметных областях) доля конфиденциальной информации сравнительно мала. Для коммерческой и персональной информации, равно как и для государственной информации, не подлежащей засекречиванию, приоритетность свойств безопасности информации может быть иной. Для открытой информации, ущерб от разглашения которой несущественен, важнейшими могут быть такие качества, как доступность, целостность или защищенность от неправомерного тиражирования. К примеру, для платежных (финансовых) документов самым важным является свойство их целостности (достоверности, не искаженности). Затем, по степени важности, следует свойство доступности (потеря платежного документа или задержка платежей может обходиться очень дорого). Требований к обеспечению конфиденциальности отдельных платежных документов может не предъявляется вообще.

Попытки подойти к решению вопросов защиты такой информации с позиций традиционного обеспечения только конфиденциальности, терпят провал. Основными причинами этого, на наш взгляд, являются узость существующего подхода к защите информации, отсутствие опыта и соответствующих проработок в плане обеспечения целостности и доступности информации, не являющейся конфиденциальной.

Развитие системы классификации информации по уровням требований к ее защищенности предполагает введение ряда степеней (градаций) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности и защищенности от тиражирования. Пример градаций требований к защищенности:

- нет требований;
- низкие;
- средние;
- высокие;
- очень высокие.

Количество дискретных градаций и вкладываемый в них смысл могут различаться. Главное, чтобы требования к защищенности различных свойств информации указывались отдельно и достаточно конкретно (исходя из серьезности возможного наносимого субъектам информационных отношений ущерба от нарушения каждого из свойств безопасности информации).

В дальнейшем любой отдельный функционально законченный документ (некоторую совокупность знаков), содержащий определенные сведения, вне зависимости от вида носителя, на котором он находится, называется информационным пакетом.

К одному типу информационных пакетов будем относить пакеты (типовые документы), имеющие сходство по некоторым признакам (по структуре, технологии обработки, типу сведений и т.п.).

Задача состоит в определении реальных уровней заинтересованности (высокая, средняя, низкая, отсутствует) субъектов в обеспечении требований к защищенности каждого из свойств различных типов информационных пакетов, циркулирующих в АС.

Требования же к системе защиты АС в целом (методам и средствам защиты) должны определяться, исходя из требований к защищенности различных типов информационных пакетов, обрабатываемых в АС, и с учетом особенностей конкретных технологий их обработки и передачи (уязвимости).

В одну категорию объединяются типы информационных пакетов с равными приоритетами и уровнями требований к защищенности (степенью важности обеспечения их свойств безопасности: доступности, целостности и конфиденциальности).

Предлагаемый порядок определения требований к защищенности циркулирующей в системе информации представлен ниже:

1. Составляется общий перечень типов информационных пакетов, циркулирующих в системе (документов, таблиц). Для этого с учетом предметной области системы пакеты

информации разделяются по ее тематике, функциональному назначению, сходности технологии обработки и т.п. признакам.

2. На последующих этапах первоначальное разбиение информации (данных) на типы пакетов может уточняться с учетом требований к их защищенности.
3. Затем для каждого типа пакетов, выделенного в первом пункте, и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяются (например, методом экспертных оценок):

- перечень и важность (значимость по отдельной шкале) субъектов, интересы которых затрагиваются при нарушении данного свойства информации;
- уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т.п.) и соответствующий уровень требований к защищенности.
- при определении уровня наносимого ущерба необходимо учитывать:
- стоимость возможных потерь при получении информации конкурентом;
- стоимость восстановления информации при ее утрате;
- затраты на восстановление нормального процесса функционирования АС и т.д.

Если возникают трудности из-за большого разброса оценок для различных частей информации одного типа пакетов, то следует пересмотреть деление информации на типы пакетов, вернувшись к предыдущему пункту методики.

4. Для каждого типа информационных пакетов с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности по каждому из свойств информации (при равенстве значимости субъектов выбирается максимальное значение уровня).

Пример оценки требований к защищенности некоторого типа информационных пакетов приведен в таблице 1.1.

Таблица 1.1. Пример оценки требований к защищенности

Субъекты	Уровень ущерба по свойствам информации			
	конфиденциальность	целостность	доступность	защита от тиражирования
N1	Нет	Средняя	Средняя	Нет
N2	Высокая	Средняя	Средняя	Нет
Nm	Низкая	Низкая	Низкая	Нет
В итоге	Высокая	Средняя	Средняя	Нет

Критерии, условия и принципы отнесения информации к защищаемой.

Виды конфиденциальной информации.

Информация составляет служебную или коммерческую тайну в случае, если

- информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- к ней нет свободного доступа на законном основании;
- обладатель информации принимает меры к охране ее конфиденциальности.

Под служебной тайной (по аналогии с коммерческой тайной в негосударственных структурах) следует понимать служебную информацию в государственных структурах, имеющую коммерческую ценность. В отличие от коммерческой тайны (в коммерческих структурах) защищаемая государством конфиденциальная информация не ограничивается только коммерческой ценностью, поэтому служебная тайна является составной частью конфиденциальной информации. В государственных структурах еще может быть информация, имеющая политическую или иную ценность. Поскольку к служебной тайне она не относится, ей необходимо присваивать гриф “конфиденциально” или иной гриф.