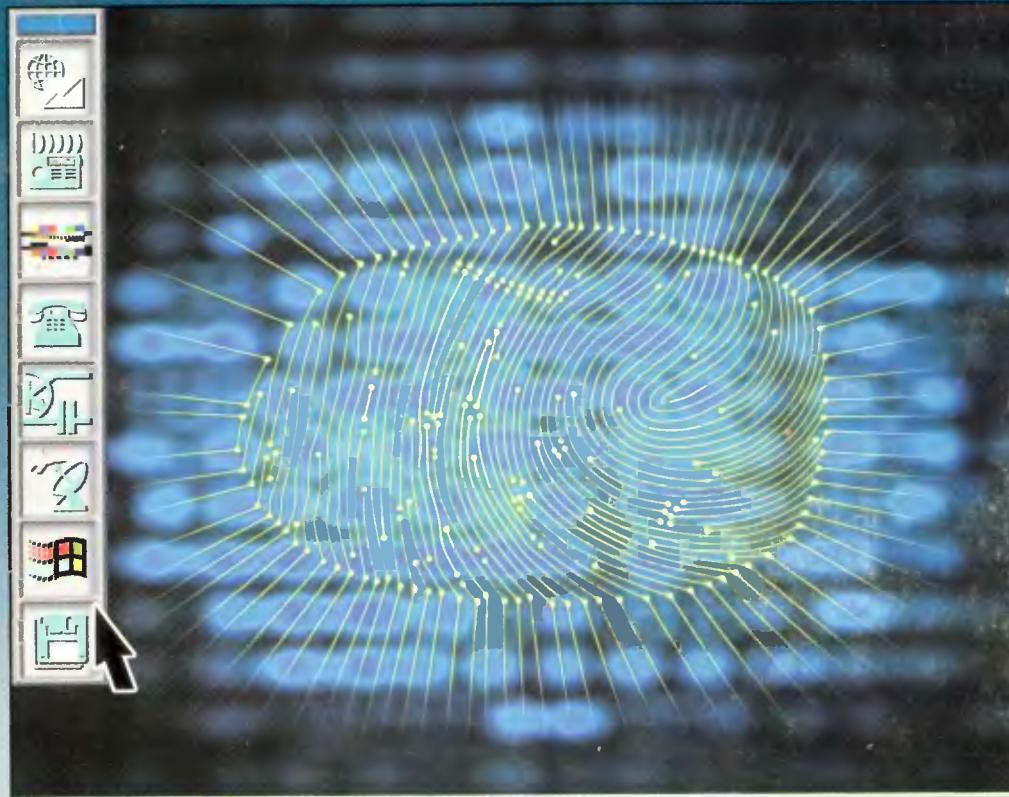


УЧЕБНОЕ ПОСОБИЕ

для высших учебных заведений

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Горячая линия-Телеком

А. А. Малюк

А.А. Малюк

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

*Допущено Министерством образования Российской Федерации
в качестве учебного пособия для студентов высших учебных
заведений, обучающихся по специальности 075400 —
«Комплексная защита объектов информации»*

**Москва
Горячая линия - Телеком
2004**

УДК 004.732.056(075.8)

М18

ББК 32.97

Рецензенты:

доктор техн. наук, профессор А. А. Стрельцов, доктор техн. наук М.П. Сычев,
кандидат техн. наук Ю.Н. Лаврухин

Малюк А. А.

M18 Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. - М: Горячая линия-Телеком, 2004. - 280 с. ил.

ISBN 5-93517-197-X

Изложены основы теории защиты информации, объединяющие широкий спектр проблем, связанных с обеспечением информационной безопасности в процессе генерирования, обработки, хранения и передачи информации в автоматизированных системах и на объектах информатизации. Анализируются различные подходы к моделированию систем и процессов защиты информации в условиях неполноты и недостоверности исходных данных. Особое внимание уделяется эвристической составляющей процесса поиска наиболее рациональных решений в различных ситуациях защиты информации.

Для студентов обучающихся по специальности «Комплексная защита объектов информатизации». Может использоваться при обучении по специальностям группы «Информационная безопасность», будет полезна разработчикам и пользователям комплексных систем обеспечения информационной безопасности.

ББК 32.97

Учебное издание

Малюк Анатолий Александрович

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:
КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ
ЗАЩИТЫ ИНФОРМАЦИИ**
Учебное пособие



Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований по проекту № 04-07-95002

Редактор А. Е. Павлов
Художник В. Г. Ситников
Подготовка оригинал-макета Ю. Н. Рысева

Лицензия ЛР № 071825 от 16.03.99 г.
Подписано к печати 02.04.2004. Формат 60x90 1/16.
Усл. печ. л. 17,5. Изд. № 197. Тираж 2000 экз.

ISBN 5-93517-197-X

© Малюк А.А., 2004
© Оформление издательства
«Горячая линия-Телеком», 2004

*Светлой памяти
доктора технических наук, профессора
Владимира Андреевича Герасименко
посвящается*

ПРЕДИСЛОВИЕ

Основную цель данной книги можно сформулировать следующим образом - обобщить имеющийся опыт теоретических исследований и практического решения задач защиты информации, сформировать на этой основе научно-методологический базис защиты и выработать рекомендации по практическим шагам в области интенсификации процессов обеспечения информационной безопасности.

В связи с тем, что процессы защиты информации подвержены сильному влиянию случайных факторов, методы классической теории систем оказываются практически непригодными для использования в качестве основы научно-методологического базиса решения проблем защиты. Таким образом, при формировании теории защиты возникает актуальная задача расширения арсенала классической теории систем за счет использования методов нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений. Причем, исключительно важное значение для решения современных проблем защиты приобретают методы экспертных оценок, эвристического программирования, «мозгового штурма» и психоинтеллектуальной генерации.

Основными результатами развития теории защиты информации являются введение понятия стратегий защиты и создание единого инструментально-методологического базиса их реализации - унифицированной концепции защиты информации. Унифицированная концепция фактически представляет собой последовательную цепь методологий оценки уязвимости информации, выработки требований по ее защите, определения кортежа концептуальных решений по защите, оценке факторов, влияющих на требуемый уровень защиты.

Все эти методологии, начиная с формирования полного множества угроз, представляют собой ярко выраженные неформализуемые проблемы.

Предисловие

В процессе развития теории и практики защиты информации сформировались три методологических подхода к их решению: эмпирический, теоретический и теоретико-эмпирический. Однако, для их эффективного использования необходимы исходные данные, систематизация и обобщение подавляющего большинства которых в настоящее время в России не организованы.

Таким образом, возникает задача серьезной корректировки организационной структуры обеспечения работ по защите информации, которая может проводиться путем создания специализированных центров защиты. В настоящее время идея создания таких центров практически реализована в виде сети учебно-научных центров по проблемам информационной безопасности в системе высшей школы.

Все перечисленные вопросы и составляют основное содержание этой книги, которое основано на материалах различных литературных источников, результатах исследований отечественных и зарубежных ученых и специалистов в области обеспечения информационной безопасности, авторских разработках в этой сфере.

Автор считает своим долгом особо отметить ценные замечания и предложения, сделанные профессором В.А. Герасименко на начальной стадии работы над книгой.

Автор выражает искреннюю благодарность рецензентам, доктору техн. наук, профессору А.А. Стрельцову, доктору техн. наук М. П. Сычеву и канд. техн. наук Ю.Н. Лаврухину.

ВВЕДЕНИЕ

В настоящее время общепризнанно, что удовлетворение все возрастающих потребностей современного общества при неуклонном увеличении народонаселения земного шара требует резкого повышения эффективности всех сфер общественной деятельности. При этом важнейшим и непременным условием такого повышения эффективности выступает адекватное повышение эффективности использования информационных ресурсов. Иными словами, для современного общества проблема информационного обеспечения всех сфер деятельности по своей значимости и актуальности превосходит проблему дальнейшей индустриализации производства, которая до недавнего времени считалась одной из центральных. Подчеркивая это обстоятельство, говорят, что современное общество вступает в постиндустриальный период своего развития, который по всеобщему мнению можно назвать информационным.

В связи с этим проблемы совершенствования систем информационного обеспечения считаются одними из наиболее актуальных и неотложных задач общества. В интересах их решения в последние годы ведутся весьма интенсивные и крупномасштабные исследования и разработки.

Вместе с тем интенсификация информационных процессов порождает ряд попутных и достаточно серьезных проблем, без решения которых вообще нельзя будет говорить об эффективности информатизации. Одной из наиболее острых проблем указанного плана выступает проблема надежной защиты информации, т.е. предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования и т.п. Особую остроту проблема защиты приобретает в связи с повсеместной и массовой компьютеризацией информационных процессов, широким внедрением информационно-вычислительных сетей с доступом к их ресурсам массы пользователей.

Вообще говоря, проблема защиты информации имеет многовековую историю. Однако, концентрируя внимание читателей на актуальных задачах сегодняшнего дня, мы ограничимся лишь тем периодом, который характеризуется регулярным применением для

хранения и обработки информации средств вычислительной техники (СВТ). Проблемы защиты информации в таких системах возникли практически одновременно с появлением самих систем, однако особо они обострились, когда СВТ стали применяться для обработки закрытой информации. Такое развитие событий в условиях общей закрытости и изолированности советского общества привело в нашей стране к положению, когда чуть ли не все содержание проблемы свелось к защите только секретной информации, хотя, как сегодня стало ясно всем, это составляет лишь одну из частей гораздо более общей задачи обеспечения защиты жизненно важных интересов личности, общества и государства в информационной сфере.

В более широкой постановке проблемы защиты информации в СССР стали открыто обсуждаться (сначала достаточно робко) чуть более двадцати лет назад после того, как в журнале «Зарубежная радиоэлектроника» был опубликован цикл из шести обзорных статей, подготовленных по данным зарубежной печати. Интенсивность обсуждения проблемы, исследований и разработок в этой области непрерывно росла, и к настоящему времени практически сформировалось самостоятельное научно-техническое направление. Создана также система подготовки профессиональных специалистов по защите информации. Иными словами, мы сегодня фактически имеем дело с новой важной сферой деятельности, в которой занято достаточно представительное число людей [1]. Основными задачами данной сферы являются:

организация практических работ по защите информации и управление ими на государственном, ведомственном, региональном и объектовом уровнях;

проведение научных исследований и разработок всех аспектов рассматриваемой проблемы;

разработка, производство и распространение средств защиты; подготовка кадров по защите информации.

Рассматривая общее содержание перечисленных задач мы можем отметить, что в плане организации работ по защите информации к настоящему времени на государственном уровне создана достаточно стройная и эффективная система управляющих органов [2]. Основу этой системы составляют Совет Безопасности Российской Федерации и комплекс силовых структур исполнительной власти.

Что касается объектового уровня, то в настоящее время практически на всех объектах (предприятиях, учреждениях, других организациях), деятельность которых связана с обработкой подлежащей защите информации, имеются штатные службы защиты, состав и

Введение

численность которых определяются объемом соответствующих задач. Общее содержание этих задач и организационно-правовой статус служб защиты достаточно детально рассмотрены в [3].

По общему признанию существующие службы решают свои задачи более или менее эффективно. Однако те изменения, которые происходят в понимании существа проблемы защиты информации, подходах, методах и средствах ее решения, предопределяют необходимость существенной корректировки организации и содержания их работы. В частности, расширение рамок комплексности защиты требует наличия в составе соответствующих служб высококвалифицированных специалистов по различным видам защиты информации, а непрерывный рост арсенала средств защиты, способов и методов их применения требует для получения наибольшего эффекта оптимального комплексирования всех средств и методов, т.е. создания комплексных (как по целям, так и по средствам) систем защиты и организации соответствующего управления ими. При этом отличительной особенностью этих систем является то, что они должны эффективно функционировать в условиях неопределенности, а зачастую и непрогнозируемости проявления дестабилизирующих факторов.

Кроме того, непрерывный рост количества объектов, нуждающихся в защите информации, но не имеющих возможностей содержать собственную полноценную службу защиты, делает все более актуальной задачу создания специализированных центров защиты информации, которые и оказывали бы соответствующие услуги названным выше объектам. Создание сети таких центров представляется главным методом организационного решения проблемы защиты информации на региональном и ведомственном уровне.

Анализируя результаты научных исследований и разработок в области защиты информации, следует отметить, что важным достижением теоретического характера на предшествующем этапе явились научные разработки новых средств защиты (технических, программно-аппаратных, криптографических) и способов построения на их основе комплексных механизмов и систем защиты. Результаты этих разработок достаточно представительно опубликованы в различных изданиях (и прежде всего на страницах журнала «Безопасность информационных технологий»). В последние годы стали появляться публикации монографического характера. Более или менее детальный анализ этих публикаций приведен в гл. 1 данного учебного пособия.

Основным результатом предшествующего этапа стало формирование основ теории защиты, в процессе которого введено поня-

Введение

тие стратегии защиты и обосновано базовое множество необходимых стратегий, предложена унифицированная концепция защиты информации (УКЗИ), обосновано полное множество задач, подлежащих решению в процессе защиты информации [3,31].

В настоящее время на базе анализа множества предпосылок доказана объективная необходимость перехода от экстенсивных к интенсивным способам защиты информации. В частности, дальнейшее совершенствование теории защиты связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества.

Во-первых, поскольку все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом, электронных) систем от разрушающего воздействия информации, то формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации. Различные аспекты этой задачи в предварительном плане обсуждены в [4].

Во-вторых, с самого начала регулярного использования автоматизированных технологий обработки информации актуальной стала задача обеспечения требуемого качества информации. Причем с течением времени актуальность данной задачи возрастает, а сама задача усложняется. Нетрудно показать, что в содержании задач обеспечения необходимого уровня качества информации и информационной безопасности много общего и аналогичного, что естественным образом наводит на мысль расширить унифицированность соответствующей концепции с учетом потребностей также задач обеспечения качества информации.

В-третьих, одним из серьезных достижений современной информатики следует признать разработку профессором Герасименко В.А. концепции информационного кадастра как высокоорганизованной совокупности данных, необходимых для эффективной деятельности соответствующего объекта (предприятия, учреждения, иной организации) [5]. Концепция информационного кадастра является ядром более общей концепции информационного обеспечения деятельности объектов. При этом, естественно, должны быть учтены и все задачи защиты информации, защиты от информации и обеспечения качества информации, которые необходимо решать как при формировании информационного кадастра, так и при его поддержке и использовании. Возникает обобщенное понятие управления информацией, объединяющее все упоминавшиеся выше понятия.

Введение

В-четвертых, серьезное внимание на новом этапе развития теории защиты информации должно быть уделено совершенствованию научно-методологического базиса и инструментальных средств, обеспечивающих решение любых возникающих задач на регулярной основе. В настоящей книге рассматриваются вопросы анализа всех этих задач с точки зрения их внутреннего содержания, в результате чего может быть определен набор необходимых и достаточных методов их решения и комплексов моделей для реализации этих методов. Все это и составляет так называемый методико-инструментальный базис решения задач защиты.

Углубленное изучение проблемы совершенствования научно-методологического базиса теории защиты информации привело к выводу, что уже в настоящее время (а тем более в перспективе) решение проблем защиты вне органической связи с решением более общих проблем (информационной безопасности, информационных технологий, информатизации общества) может привести к неадекватным результатам. Серьезность данного вопроса признана настолько основательной, что его решение должно вестись с использованием иных (по сравнению с прежними) интенсивных подходов. Все это говорит о необходимости обобщения накопленного опыта теоретических исследований и практического решения задач защиты информации в целях формирования на этой основе научно-методологического базиса защиты как краеугольного камня интенсификации процессов обеспечения информационной безопасности.

Третьей разновидностью деятельности в области защиты информации являются исследование, разработка и распространение средств защиты, которым всегда уделялось и продолжает уделяться повышенное внимание. Основное концептуальное требование к средствам защиты в условиях перехода к интенсивным способам решения задач защиты информации может быть сформулировано в терминах достаточности в том смысле, что в их арсенале должны быть средства для решения любой задачи и в любых потенциально возможных условиях. Подробно данные вопросы рассмотрены в соответствующих главах настоящего учебного пособия.

Что касается проблемы кадрового обеспечения информационной безопасности, то следует отметить, что данный вопрос к настоящему времени применительно к защите информации имеет достаточно серьезную практическую реализацию и некоторые теоретико-методологические обобщения. Справедливость сказанного можно подтвердить тем, что в настоящее время уже функционирует организованная система подготовки молодых и повышения ква-

Введение

лификации работающих специалистов по защите информации, основой которой являются учебно-методическое объединение вузов по образованию в области информационной безопасности и сеть региональных учебно-научных центров высшей школы.

Резюмируя, сегодня можно выделить следующие наиболее острые проблемы развития теории и практики обеспечения информационной безопасности:

создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);

разработка научно обоснованных нормативно-методических документов по обеспечению информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите;

стандартизация подходов к созданию систем защиты информации и рационализация схем и структур управления защитой на объектовом, региональном и государственном уровнях.

Решение спектра перечисленных задач имеет важное значение для реализации положений Доктрины информационной безопасности и Концепции национальной безопасности Российской Федерации.

Таким образом, основная цель данного учебного пособия состоит в ознакомлении читателей с современными взглядами на исследование путей и разработку методов интенсификации процессов обеспечения информационной безопасности на основе формирования научно-методологического базиса защиты и рационализации подходов к созданию систем защиты и управлению их функционированием.

В соответствии с этим в книге последовательно рассматриваются следующие вопросы:

место проблем информационной безопасности в общей совокупности информационных проблем современного общества;

подходы к защите информации и обоснование необходимости перехода в современных условиях к интенсивным способам защиты;

научно-методологические основы интенсификации процессов защиты информации;

угрозы и методология оценки уязвимости информации;

методы определения требований к защите информации с учетом факторов, влияющих на уровень защиты, и потенциально возможных условий функционирования защищаемых систем;

Введение

общеметодологические принципы построения систем защиты информации и управления процессами их функционирования;

практические рекомендации по интенсификации процессов защиты информации и формированию современных организационных структур, обеспечивающих эффективную реализацию комплексного подхода к обеспечению информационной безопасности.

Первая глава пособия посвящена рассмотрению общих аспектов проблемы безопасности как научной категории. Здесь определяется место информационной безопасности в обеспечении национальной безопасности государства, на основе привлечения достижений информатики и ретроспективного анализа развития подходов к защите информации как одной из основных составляющих обеспечения информационной безопасности формулируется современная постановка задачи защиты, суть которой состоит в переходе от экстенсивных к интенсивным методам решения проблем.

Во второй главе рассматриваются научно-методологические основы интенсификации процессов защиты информации, формируется научно-методологический базис решения задач защиты, рассматриваются проблемы расширения арсенала классической теории систем за счет использования методов, позволяющих адекватно моделировать процессы, существенно зависящие от воздействия трудно предсказуемых факторов, и решать задачи анализа, т.е. оценки защищенности (уязвимости) информации, и синтеза, т.е. оптимизации распределения ресурсов, выделяемых на защиту.

Третья глава рассматривает проблемы количественной оценки угроз защищаемой информации. В ней приводится системная классификация угроз и описывается модель определения показателей уязвимости информации.

В четвертой главе рассматриваются методы определения требований к защите информации, проблемы классификации множества вариантов потенциально возможных условий защиты и формирования на ее основе необходимого и достаточного набора типовых систем защиты информации.

Пятая глава посвящена методологическим принципам создания систем защиты информации и управления их функционированием. Здесь также рассматриваются вопросы типизации и стандартизации систем защиты.

В шестой главе рассматриваются обобщенные итоги и перспективы развития теории и практики защиты информации.

Глава первая

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества

Если рассматривать безопасность в качестве общенаучной категории, то она может быть определена как некоторое состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой - ее функционирование не создает угроз для элементов самой системы и внешней среды. При таком определении мерой безопасности системы являются:

с точки зрения способности противостоять дестабилизирующему воздействию внешних и внутренних угроз - степень (уровень) сохранения системой своей структуры, технологии и эффективности функционирования при воздействии 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 представлять угрозу элементам самой системы или внешней среде.

Чисто механическая интерпретация данных формулировок приводит к следующему определению информационной безопасности:

Информационная безопасность - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

Именно такое понятие информационной безопасности положено в основу Доктрины информационной безопасности и законодательства в сфере обеспечения информационной безопасности Российской Федерации (дословно - «Информационная безопас-

ность – это состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз»).

Приведенное определение представляется достаточно полным и вполне корректным. Однако, для того, чтобы служить более конкретным ориентиром в направлении поиска путей решения проблем информационной безопасности, оно нуждается в уточнении и детализации его основополагающих понятий. При этом отправной точкой может служить тот факт, что 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. Отсюда естественным образом вытекает, что обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

первая – защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;

вторая – защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;

третья – защита внешней среды от информационных угроз со стороны рассматриваемой системы.

В соответствии с изложенным общая схема обеспечения информационной безопасности может быть представлена так, как показано на рис. 1.1.

Естественно, что проблемы информационной безопасности являются производными относительно более общих проблем информатизации. Поэтому содержание проблем информационной безопасности должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к их решению должны взаимоувязываться с концепциями информатизации.

К основным концептуальным вопросам информатизации, на базе которых должны решаться и проблемы информационной безопасности, очевидно, могут быть отнесены:

сущность информатизации;

конечные результаты информатизации;

пути, средства и методы достижения основных результатов информатизации.

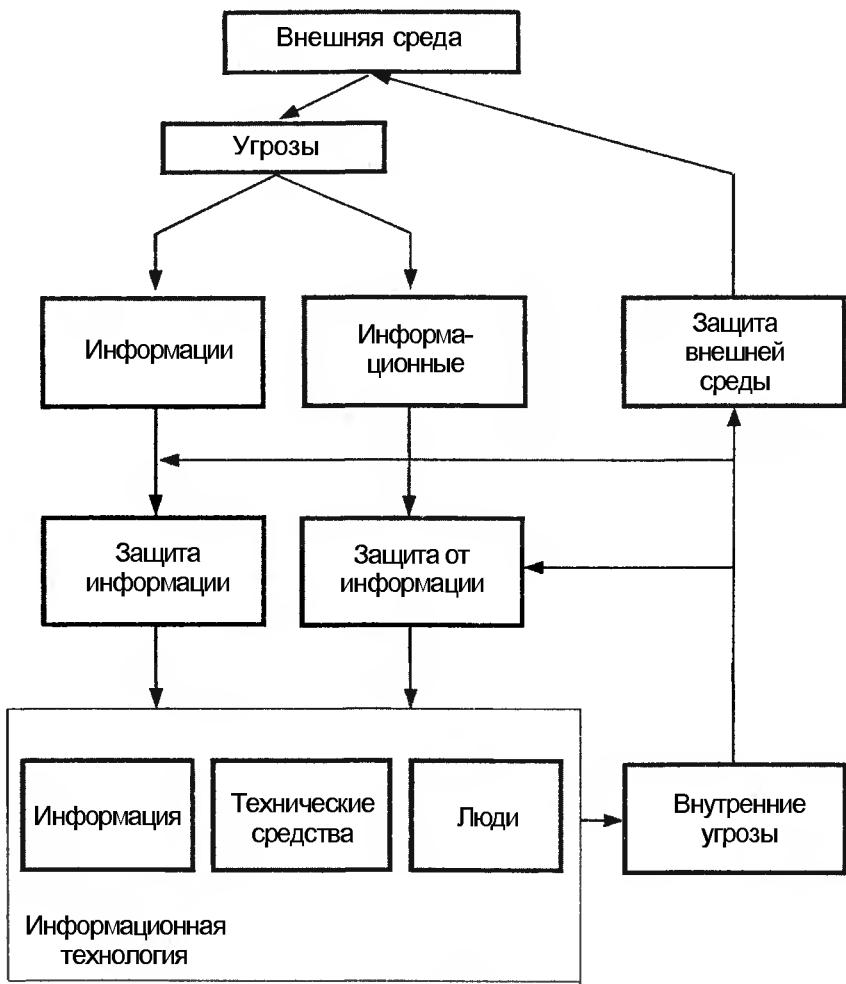


Рис. 1.1. Общая схема обеспечения информационной безопасности

Не вдаваясь в философские аспекты информатизации, а взяв за основу ее прагматическое значение, можно с полным основанием утверждать, что сущность информатизации заключается в формировании такой информационной среды, в которой имелись бы все объективные предпосылки, необходимые для наиболее рационального информационного обеспечения всех сфер деятельности современного общества. Создание такой среды естественно пред-

Проблемы обеспечения информационной безопасности

полагает всеобщую компьютеризацию, однако она представляет собой лишь компонент (хотя и один из важнейших) формирования общей инфраструктуры информационной среды.

В этих условиях производство, переработка и использование информации становятся важнейшей отраслью экономики, которая и получила общепризнанное название информационной индустрии. Таким образом, создание объективных предпосылок, необходимых для формирования информационной индустрии, и составляет основное содержание информатизации современного общества. При этом научно-методологическим базисом этого процесса служит такая отрасль науки, как информатика.

Перед информатикой фактически стоят две основные задачи: изучение информационных проблем общества и разработка путей, методов и средств наиболее рационального их решения. Изучение информационных проблем поставлено нами на первое место со всем не случайно. Этим однозначно определяется, что такое изучение является исходным базисом для реализации второй основной задачи информатики - разработки путей, методов и средств наиболее рационального решения этих проблем и прежде всего удовлетворения информационных потребностей общества в процессе его жизнедеятельности. Таким образом, пути, методы и средства информатизации должны разрабатываться исходя из информационных потребностей. Однако, в соответствии с законом об обратной связи, и информационные потребности общества должны максимально приспособливаться к возможностям их удовлетворения. Это означает, что информационные процессы в различных сферах деятельности должны быть целенаправленно подготовлены к переводу их на индустриальные методы осуществления.

Структурированные таким образом информационные потребности общества являются одной из основных предпосылок для разработки необходимого арсенала методов и средств информатизации. Основу этого арсенала должны составлять унифицированные методы и современные средства обработки информации. На их базе и должна разрабатываться концепция индустриализации переработки информации и необходимые для этого информационные технологии.

Объективные предпосылки индустриализации процесса информационного обеспечения различных сторон деятельности современного общества создаются совокупностью результатов, полученных в последнее время в рамках информатики. К ним прежде всего относятся:

системная классификация информации;
унификация структуры информационного потока;
унификация процедур (задач) обработки информации;
систематизация методов обработки информации;
унификация информационной технологии;
формирование концепции управления процессами обработки информации по унифицированной технологии.

Последний из приведенных здесь результатов носит многоаспектный характер. Причем одной из основных его составляющих является проблема обеспечения информационной безопасности.

Современное состояние изучения и практической разработки проблемы информационной безопасности может быть оценено следующим образом. Первая ее составляющая, т. е. проблема защиты информации, уже продолжительное время (свыше 30 лет) находится в центре внимания специалистов, и к настоящему времени достигнуты следующие результаты:

проблема получила практически всеобщее признание;
заложены основы разработки теории защиты;
налажено производство средств защиты;
организована планомерная подготовка и повышение квалификации специалистов соответствующего профиля;
создана государственная система защиты информации;
накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.

На основе перечисленных результатов справедливым будет утверждение, что проблема защиты информации имеет определенный базис для дальнейшего целенаправленного развития. При этом основные задачи дальнейшего развития могут быть сформулированы следующим образом.

Первая и самая неотложная - регулярный сбор и обработка статистических данных о составе и результатах функционирования реальных систем защиты. Полученные таким образом данные необходимы как для совершенствования методологии проектирования новых систем защиты и повышения эффективности их функционирования, так и для дальнейшего развития теории защиты, поскольку те основы, которые упоминались выше, носят по преимуществу вербальный характер. Развитая же теория должна содержать количественные методы анализа и синтеза систем защиты и управления ими в процессе функционирования.

Вторая задача заключается в создании организационных структур, обеспечивающих решение первой задачи. Такие организационные структуры могут, например, формироваться в виде специализированных региональных центров защиты, на базе которых можно было бы развернуть эффективную систему сбора и обработки статистических данных, а также обеспечить оказание широкого спектра услуг своим абонентам.

Третья задача - это дальнейшее развитие научно-методологического базиса как основы интенсификации процессов защиты [6]. Составляющими частями данной задачи выступают:

во-первых, формирование более общей (по сравнению с классической) теории систем, ориентированной не только на технические, но и на социальные системы;

во-вторых, разработка на основе вербальной теории строгой теории защиты, базисом которой должны служить общая теория систем и статистические данные о структуре и функционировании систем защиты информации, получаемые при решении первой сформулированной задачи;

в-третьих, разработка комплекса рабочих моделей, необходимых и достаточных для решения всех задач защиты информации.

Так в самом общем виде могут быть представлены состояние и основные направления развития защиты информации как первой составляющей общей проблемы информационной безопасности.

Рассматривая эти направления в качестве основных на сегодняшний день, мы не можем в то же время, хотя бы вкратце, не остановиться на состоянии дел с изучением и разработкой второй составляющей информационной безопасности - защиты от информации.

Дело в том, что наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне.

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

Глава 1

части общей проблемы информационной безопасности заключается в том, что информация способна оказывать такое воздействие на людей и технические комплексы, результаты которого могут носить не просто негативный, а трагический и даже катастрофический характер.

Информационное воздействие на человека может вызывать плохое настроение, ухудшение психического состояния, негативное поведение, неправильную ориентацию и т. п. Большие возможности имеются и для информационного воздействия на электронную технику. Например, если в ЭВМ заблаговременно ввести специальную аппаратную закладку, то по команде извне можно прервать работу ЭВМ, или, наоборот, несанкционированно ее инициировать, вывести из строя и т. п.

Уже того, что сказано здесь относительно защиты от информации, достаточно для утверждения о чрезвычайной важности данной проблемы для современного общества. В то же время, несмотря на практически всеобщее понимание (по крайней мере среди специалистов по информатике) важности проблемы, сколько-нибудь регулярные ее исследования и разработки на сегодняшний день практически не ведутся.

Справедливо ради надо отметить, что проблема защиты от информации существенно сложнее проблемы защиты информации в силу того, что информационные угрозы чрезвычайно многообразны, а их воздействие далеко не всегда очевидно. Предотвращение и нейтрализация информационных угроз требуют не столько технических решений, сколько организационно-правовых и политических, причем не только внутригосударственных, но и международных.

В постановочном плане представляется, что задача защиты от информации естественным образом делится на две составляющие: защита от информации технических средств и систем и аналогичная защита людей.

Анализ показывает, что применительно к первой составляющей, т.е. защите от информации технических средств и систем, основные положения рассматриваемой в данном учебном пособии унифицированной концепции защиты информации (УКЗИ) остаются адекватными без особой трансформации (с точностью до нюансов терминов). Что же касается защиты от информации людей, то здесь эта адекватность не является такой очевидной в силу широкого и разно-планового воздействия на них информации и разномасштабности постановки задачи обеспечения информационной безопасности.

Отличительная особенность проблемы защиты людей от информации, создающая дополнительные трудности, состоит в том, что ее решение будет носить преимущественно гуманитарный характер, в то время как решения по защите от информации технических средств и систем, так же как и по защите информации, носят технический характер и поддаются строгой структуризации.

1.2. Ретроспективный анализ развития подходов к защите информации

Работы по защите информации в автоматизированных системах у нас в стране ведутся непрерывно, начиная с того времени, когда электронная вычислительная техника стала сколько-нибудь регулярно использоваться для обработки закрытой информации. Естественно, это были прежде всего органы государственного и военного управления, специальные ведомства, оборонные отрасли промышленности и другие организации, имеющие дело преимущественно именно с такой информацией.

В связи с этим продолжительное время все работы в области защиты информации были, как правило, закрытыми, а специальные публикации были эпизодическими и носили фрагментарный характер. Таким образом, до последнего времени практически отсутствовали необходимые объективные предпосылки для формирования какой-либо общей методологии обеспечения безопасности информации.

В то же время в ведущих зарубежных странах (и прежде всего в США) публикации в открытой печати по рассматриваемым вопросам уже в 60 - 70-е гг. прошлого века приняли практически массовый характер, причем наряду с журнальными статьями стали появляться работы монографического характера, а в учебные планы ведущих вузов стали включаться самостоятельные дисциплины по защите информации.

В целях привлечения внимания к проблеме широкого круга заинтересованных специалистов и хотя бы общего ознакомления их с зарубежным опытом в 1975-1976 гг. по согласованию с соответствующими органами в журнале «Зарубежная радиоэлектроника» была опубликована серия из шести обзорных (по данным зарубежной печати) статей, объединенных тематически и дающих общее представление обо всей совокупности проблем защиты информации и о подходах к их решению. По некоторым соображениям авторы названных статей В.А.Герасименко и В.И.Герасимов опубликовали их под псевдонимами В.Герасимов и В.Владиславский. Статьи вызвали большой резонанс в среде специалистов и сыгра-

ли роль детонатора, инициировав существенное повышение интереса к проблеме, ее исследованиям и разработкам.

С конца 80-х годов все чаще стали публиковаться оригинальные статьи с изложением результатов исследований и разработок их авторов. Особенно интенсифицировался поток публикаций в последние годы, когда периодически стали издаваться специализированные журналы. О количестве журнальных статей можно судить уже по тому факту, что только в журнале «Безопасность информационных технологий» с 1994 г. (года его основания) и до настоящего времени помещено свыше 400 различных публикаций по проблемам защиты информации. Статьи по рассматриваемой тематике публикуются и в других периодических изданиях, причем в таких журналах, издаваемых в Санкт-Петербурге, как «Конфидент», «БДИ: безопасность, достоверность, информация» и «Проблемы информационной безопасности. Компьютерные системы», практически регулярно. Перечислить, а тем более проаннотировать все опубликованные статьи здесь не представляется возможным. Назовем только две журнальные публикации обобщающего характера. Первой такой публикацией был специальный выпуск журнала «Зарубежная радиоэлектроника» (1989 г., №12), в котором были опубликованы 11 статей.

Данные статьи охватывают практически все основные вопросы, связанные с защитой. Уместно также отметить, что в первой из указанных статей предпринята попытка периодизации развития подходов к защите информации, причем весь интервал этого развития разделен на три периода, охарактеризованные следующим образом:

1) попытки обеспечения надежной защиты информации чисто формальными механизмами, содержащими главным образом технические и программные средства, сосредоточение программных средств в рамках ОС и СУБД;

2) дальнейшее развитие формальных механизмов защиты, выделение управляющего компонента - ядра безопасности, развитие неформальных средств защиты, формирование основ системного подхода к защите;

3) дальнейшее развитие механизмов второго этапа, формирование взглядов на защиту как на непрерывный процесс, развитие стандартов на защиту информации, усиление тенденции аппаратной реализации функций защиты, формирование вывода о взаимосвязи защиты информации, архитектуры систем обработки данных и технологии их функционирования.

Второй журнальной публикацией обобщающего характера была статья В.А. Герасименко, которая охватывает всю совокупность основных вопросов, относящихся к защите информации, в том числе впервые затрагивает вопросы перспектив развития теории защиты (журнал «Зарубежная радиоэлектроника», №3, 1993 г.).

К настоящему времени уже опубликовано некоторое количество работ монографического характера, причем сначала публиковались переводы книг зарубежных авторов, а в последнее время и работы отечественных авторов. Из переводов следует отметить книги [7-9]. Первыми публикациями монографического характера отечественных авторов стали учебное пособие В. В. Шуракова [10] и книга А.Г. Мамиконова, В.В. Кульбы и А.Б. Шелкова [11].

Первая из названных книг была написана по данным зарубежной печати и представляла собою грамотный синтез перечисленных выше переводных книг и обзорных статей, опубликованных к тому времени в журнале «Зарубежная радиоэлектроника». Она была рекомендована в качестве учебного пособия для студентов вузов, обучающихся по специальностям, связанным с автоматизированной обработкой данных, однако использовалась значительно более широким кругом специалистов соответствующего профиля, а тираж в 13000 экз. разошелся в достаточно короткие сроки.

Авторами второй книги являются широко известные ведущие ученые Института проблем управления РАН. По уровню изложения и строгости доказательства всех формулируемых положений она относится к изданиям академического плана. Авторы данной книги защиту информации в традиционном плане (предупреждение несанкционированного получения) рассматривают в одном контексте с обеспечением сохранности программных модулей и информационных массивов, что, как будет показано ниже, согласуется с современной концепцией комплексной защиты.

В 1991 г. выпущена небольшая (94 стр.), но получившая большое распространение книга С. П. Растрогуева и Н. Н. Дмитриевского [12], в которой осуществлена систематизация основных подходов к организации защиты программного обеспечения от несанкционированного копирования и рассмотрены принципы и методы снятия такой защиты.

Следующей в хронологическом порядке была очень важная и в современных условиях очень нужная книга [13], изданная в 1992 г. О содержании книги говорит ее название («Защита информации в персональных ЭВМ»), она пользуется повышенным авторитетом у широкого круга соответствующих специалистов.

В 1993 г. вышла книга известного в среде специалистов по защите информации ученого С. П. Растворгева [14]. По стилю изложения она носит несколько элитарный характер. В связи с этим для продуктивного ее чтения требуются достаточно глубокие знания основ защиты информации, программирования, криптографии и математики.

В 1994 г. библиотека литературы по защите информации пополнилась двумя публикациями монографического характера: двухтомной книгой В.А. Герасименко [3] и книгой В. Ю. Гайковича и А. В. Першина [15].

В книге В. А. Герасименко впервые предпринята попытка систематизации всей совокупности основных вопросов, относящихся к проблематике защиты информации.

Книга В. Ю. Гайковича и А. В. Першина ориентирована прежде всего на работников служб безопасности и руководителей банковских учреждений, хотя она, безусловно, представляет значительный интерес и для более широкого круга специалистов соответствующего профиля.

С течением времени поток публикаций, естественно, рос, и в 1996 г. вышло уже несколько работ монографического характера.

Из этих работ несомненный интерес для широкого круга специалистов представляет книга А. А. Грушко и Е. Е. Тимониной [16]. Книга является как бы введением в теорию защиты информации, в ней наряду со строгими определениями и доказательствами содержится большое количество примеров из практической жизни, доходчиво иллюстрирующих основные теоретические положения, она безусловно станет важной составляющей формирующейся в настоящее время общей теории защиты информации.

В 1996 г. вышла также книга П. Д. Зегжды [17], посвященная современным проблемам безопасности компьютерных систем. В ней приведены классификация и примеры нарушения безопасности, намечены новые подходы к созданию защищенных систем. Книга содержит также уникальный справочный материал по анализу безопасности наиболее распространенных на отечественном рынке зарубежных систем.

В период с 1997 года по настоящее время появилось достаточно много интересных работ монографического характера таких известных специалистов, как Г.В. Емельянов, В.А. Минаев, А.А. Стрельцов, Л.М. Ухлинов, Д.С. Черешкин..

Есть все основания утверждать, что тенденция интенсивного роста числа публикаций (на примере периодической печати) со-

хранится и в обозримом будущем, порукой чему служит уже то обстоятельство, что журналы «Безопасность информационных технологий» и «Проблемы информационной безопасности. Компьютерные системы» находятся на восходящих траекториях своего развития.

Достойное место в ряду периодических изданий по защите информации безусловно займет и российско-белорусский журнал «Управление защитой информации», который начал выходить в 1998 году (до этого он издавался как журнал Республики Беларусь).

Основываясь на анализе приведенных выше публикаций, можно сформулировать следующие общие характеристики выделенных нами периодов развития подходов к защите информации.

Как уже отмечалось, первые попытки периодизации истории развития этих подходов относятся к 1989 г., когда было введено понятие этапа развития, причем по критерию используемых средств защиты и способов их применения было выделено три этапа: начальный, промежуточный и современный. Если в качестве основного критерия периодизации принять определяющий для конкретного этапа методологический подход к защите информации, то эти три периода могут быть названы соответственно эмпирическим, концептуально-эмпирическим и теоретико-концептуальным. Обобщенные характеристики выделенных периодов приведены в табл. 1.1.

Наиболее характерная особенность эмпирического подхода к защите информации заключается в том, что на основе анализа ранее проявлявшихся угроз информации и накапливаемого опыта защиты разрабатывались и внедрялись необходимые механизмы защиты. При этом под защитой понималось предупреждение несанкционированного получения информации лицами и процессами (программами), не имеющими на это полномочий, хотя традиционно применялись меры для обеспечения целостности информации, т. е. предупреждения несанкционированного ее уничтожения и искажения.

Следует отметить, что в это же время делались попытки и разработки строгих теоретико-вероятностных зависимостей для оценки угроз. Однако они оказались достаточно сложными, а в силу повышенного влияния на защиту информации случайных факторов и отсутствия достаточной выборки статистических данных практического применения не нашли.

Сущность и содержание **концептуально-эмпирического подхода** к защите информации заключались в том, что на основе опыта защиты информации, полученного на этапе эмпирического подхода,

Глава 1

удалось некоторым образом подойти к унификации используемого для решения задач защиты методико-инструментального базиса.

В качестве основы формирования соответствующей этому этапу концепции, естественно, была принята приведенная на рис. 1.2 схема организации защиты информации на основе эмпирического подхода.

Таблица 1.1

Обобщенные характеристики периодов развития подходов к защите информации

Характеристики периода	Обобщенное название и содержание периода		
	Эмпирический	Концептуально-эмпирический	Теоретико-концептуальный
Сущность подхода	1. Непрерывное слежение за появлением новых угроз информации 2. Разработка средств защиты от новых угроз 3. Выбор средств защиты на основе опыта	1. Формирование на основе опыта общей концепции защиты 2. Разработка и научное обоснование методов оценки уязвимости информации и синтеза оптимальных механизмов защиты 3. Появление унифицированных и стандартных решений по защите	1. Разработка основ теории защиты информации 2. Обоснование постановки задачи многоаспектной комплексной защиты 3. Введение понятия стратегии защиты 4. Унификация концепции защиты 5. Разработка методологий анализа и синтеза систем защиты и управления ими в процессе функционирования 6. Широкое развитие унифицированных и стандартных решений
Способы организации средств защиты	Функционально-ориентированные механизмы защиты	Единые системы защиты	Системы комплексной защиты. Ориентация на защищенные информационные технологии

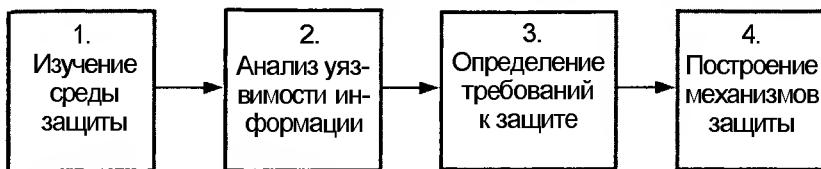


Рис. 1.2. Схема организации защиты информации на этапе эмпирического подхода

Трансформация приведенной схемы осуществлялась по следующим направлениям:

1) в целях создания предпосылок для построения адекватных моделей защищаемых информационных систем и технологий разработана методология их структуризации, для чего в концепции предусмотрен самостоятельный компонент;

2) для обеспечения объективной оценки уязвимости информации блок 2 представлен тремя компонентами: системой показателей уязвимости, системой угроз информации, методами и моделями определения и прогнозирования значений показателей уязвимости;

3) блок 4 преобразован в цепочку концептуальных решений по защите информации: определение функций защиты (однородных в функциональном отношении мероприятий, осуществляемых в интересах защиты информации), определение задач защиты в традиционной интерпретации этого понятия (решаемых в интересах осуществления функций защиты), выбор средств защиты (с помощью которых решаются задачи), построение системы защиты (организованной совокупности методов, средств и мероприятий, используемых для обеспечения защиты);

4) в целях повышения эффективности защиты предусмотрена обратная связь от концептуальных решений по защите к той среде, в которой она осуществляется.

Структура сформированной таким образом концепции защиты (в дальнейших публикациях она получила уже упоминавшееся нами название унифицированной) приведена на рис. 1.3.

К настоящему времени УКЗИ (с точностью до нюансов непринципиального характера) изложена в нескольких публикациях (см., например, [3]). Однако следует отметить, что и до сегодняшнего дня системная реализация всей совокупности положений УКЗИ сдерживается рядом серьезных трудностей, обусловленных следующими причинами:

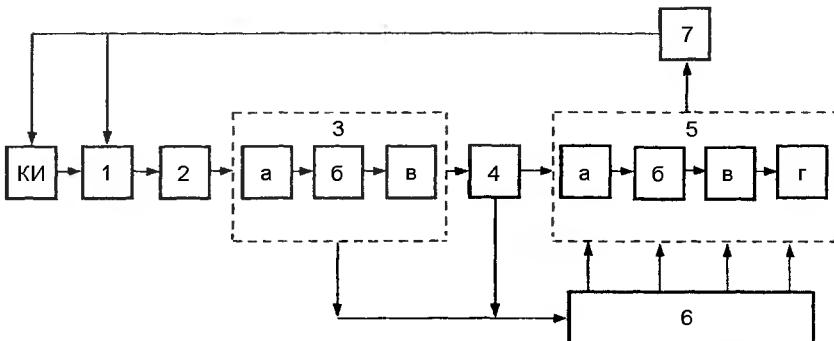


Рис. 1.3. Структура унифицированной концепции защиты информации:
 КИ - концепция информатизации; 1 - среда защиты; 2 - методология структуризации среды защиты; 3 - методология оценки уязвимости информации (а - система показателей уязвимости; б - система угроз безопасности информации; в - методы определения текущих и прогнозирования будущих значений показателей уязвимости); 4 - методология формирования требований к защите; 5 - система концептуальных решений по защите (а - функции защиты; б - задачи защиты; в - средства защиты; г - система защиты); 6 - требования к концептуальным решениям; 7 - условия, способствующие повышению эффективности защиты

1) значительным своеобразием систем и процессов защиты информации, связанным с повышенным влиянием случайных факторов, в силу чего методы классической теории систем далеко не всегда адекватны характеру моделируемой ситуации, методы же, которые могли бы в достаточной мере дополнить существующие, в необходимой степени не разработаны;

2) недостаточно четкой проработкой инструментальных средств решения задач анализа и синтеза систем и процессов защиты информации;

3) отсутствием значительной (если не подавляющей) части исходных данных, необходимых для обеспечения решения названных задач.

В указанных выше публикациях обсуждены возможные пути преодоления данных трудностей, однако конкретные разработки удалось произвести лишь частично, причем основной причиной этого оказалось отсутствие в период эмпирико-концептуального подхода целостной теории защиты.

Значительное развитие в рассматриваемом периоде получили средства защиты, причем оно шло по нескольким направлениям: увеличивался арсенал различных средств, расширялись их функциональные возможности за счет комплексирования различных средств в

многофункциональные механизмы защиты, наиболее удачные разработки получали сертификаты качества и даже принимались в качестве стандартов. Наибольшее развитие получили технические, программно-аппаратные и криптографические средства.

Технические средства классифицируются сегодня по четырем критериям: 1) функциональному назначению, т. е. по тем функциям защиты, которые они могут осуществлять (внешняя защита объекта, опознавание объектов и субъектов, внутренняя защита); 2) типу, указывающему на принцип работы их элементов (механические, электрические, оптические, электронные, комбинированные); 3) сложности средств защиты и практического их применения (простое устройство, блок, агрегат, автономная система); 4) стоимости приобретения, установки и эксплуатации (незначительная, средняя, большая и очень большая). Системное изложение сведений по техническим средствам содержится в [3, 18] и др.

Критерии классификации программных средств не так очевидны, как технических. Один из возможных вариантов классификации приведен в [3], где выбраны следующие критерии: решаемые задачи (опознавание объектов и субъектов, разграничение доступа и т. п.); расположение в защищаемой системе (операционная система, система управления базами данных и т. п.); уровень инициирования (физический, логический). Данный класс средств интенсивно развивается, описание программной защиты содержится во многих публикациях, например, [3, 13, 17, 19 - 22]. Программные средства используются как в «чистом виде» (программы регистрации запросов, программы опознавания пользователей и т. п.), так и в комплексных механизмах защиты (широко известная система защиты информации от несанкционированного доступа «Снег» состоит из четырех функциональных подсистем: 1) разграничения доступа, 2) регистрации и учета, 3) обеспечения целостности, 4) криптографической).

Криптографические средства в настоящее время составляют непременный компонент любой сколько-нибудь серьезной системы защиты информации, особенно в сетевых структурах, где они являются практически единственным средством надежной защиты. Имея многовековую историю развития, к настоящему времени криптографические средства достигли весьма высокого уровня совершенства, причем в настоящее время достаточно широко используются как традиционные системы секретного ключа, так и сравнительно новые, получившие название систем открытого ключа.

Учитывая высокую ответственность и сугубую специфику криптографических средств, соответствующие системы стараются доводить до уровня стандартов, гарантирующих высокий уровень защиты. В Российской Федерации в настоящее время есть стандарты на шифрование (ГОСТ 28147-89) и электронную цифровую подпись (ГОСТР 3410-94, ГОСТР 3411-94).

Достаточно полные сведения по криптографическим средствам приведены в [23].

Весьма интенсивно в рассматриваемый период развивались методы и средства защиты от так называемых разрушающих закладок (вредоносных программ), под которыми понимаются «тroyянские кони», «компьютерные вирусы», «бомбы», «ловушки» и т. п. Такие закладки появились чуть ли не одновременно с актуализацией самой проблемы защиты. Борьба с ними первоначально носила оборонительный характер: после обнаружения закладки (непрекращающееся уже после осуществления ее разрушающего воздействия) изучался ее характер, после чего разрабатывались методы и средства борьбы с нею. Учитывая, что количество различных закладок растет лавинообразно (в настоящее время оно исчисляется тысячами), стало совершенно очевидно, что оборонительный характер защиты от них не только недостаточно эффективен, но и чреват серьезными последствиями. В связи с этим усилия соответствующих специалистов были направлены на системные исследования проблемы в целях заблаговременного обнаружения закладок и унификации способов и средств борьбы с ними. Появился даже термин «компьютерная вирусология», причем одной из первых фундаментальных работ этого плана была отечественная монография [24]. Из других работ заслуживают упоминания [17, 20, 25] и др. К настоящему времени разработаны методы предупреждения заражения компьютера, лечения зараженного компьютера и технологии создания программ, устойчивых к заражению [25].

Отличительная особенность теоретико-концептуального подхода к защите информации состоит в том, что на основе достижений концептуально-эмпирического подхода предпринимаются попытки разработать основы целостной теории защиты и этим самым подвести под реализацию защиты прочную научно-методологическую базу. При этом теория защиты, как и любая другая теория, определяется как совокупность основных идей в данной области знания. Основное назначение теории защиты заключается в том, чтобы дать полное и адекватное представление о сущности и содержании про-

блемы защиты и обеспечить на основе научно-методологической базы эффективное решение всех задач защиты с использованием всех доступных инструментальных средств.

Объективной основой формирования теории защиты явилась унифицированная концепция защиты информации, которая в достаточно завершенном виде была сформулирована в предшествующий период и которая, вообще говоря, вобрала в себя весь накопленный к этому времени опыт защиты. На основе этого опыта были сформулированы следующие принципиальные выводы [26]:

1) проблемы обеспечения безопасности информации будут носить перманентный характер, вследствие чего необходима развитая и регулярно функционирующая система, обеспечивающая эффективное решение всей совокупности соответствующих задач;

2) обеспечение безопасности информации должно носить комплексный характер;

3) комплексность защиты информации может быть достигнута лишь при взаимосогласованном участии в решении соответствующих задач как профессиональных специалистов по защите информации, так и всех тех руководителей и специалистов, которые организуют и осуществляют процессы сбора, передачи, хранения, обработки и использования информации;

4) надежная защита информации может быть обеспечена лишь в том случае, если проблемы защиты будут решаться в тесной взаимосвязи с проблемами информатизации;

5) эффективное решение проблем защиты информации в современной их постановке возможно только при наличии развитого и адекватного научно-методологического базиса.

Формирование теории защиты идет в порядке ответа науки на объективные потребности практики. Однако до 1992 г. этот процесс осуществлялся стихийно. В середине 1992 г. существовавший в то время Государственный комитет Российской Федерации по высшему образованию организовал и финансировал межвузовскую программу по проблемам защиты информации, к выполнению которой было привлечено значительное число вузов.

Разработанные в процессе выполнения данной межвузовской программы основы теории защиты информации в последующие годы развивались и совершенствовались. Это дает основания для признания факта формирования к настоящему времени основ теории защиты информации. Основное содержание составляющих

частей этой теории с учетом концепции интенсификации процессов защиты будет рассмотрено в гл. 2.

1.3. Современная постановка задачи защиты информации

Задача защиты информации в последнее десятилетие практически повсеместно представляется как предупреждение несанкционированного ее получения в системах обработки, построенных на базе современных средств электронной вычислительной техники (ЭВТ). Такая интерпретация рассматриваемой задачи воспринимается как нечто само собой разумеющееся. Нисколько не отрицая важность задачи защиты в названной выше постановке и достигнутые успехи в ее решении, скажем однако, что к настоящему времени созрели и объективная необходимость, и объективные предпосылки для кардинального видоизменения этой постановки задачи и подходов к ее решению. Заметим, что необходимость своевременного видоизменения постановки задачи является одним из важнейших общеметодологических принципов развития науки.

Основные факторы, обуславливающие объективную необходимость названного видоизменения, заключаются в следующем.

Небывалое повышение значимости информации как общественного ресурса. Современное общество характеризуется как постиндустриальное в хронологическом плане и как информационное в плане основополагающих процессов. Интегральное толкование обеих характеристик сводится к тому, что по мере поступательного развития индустриального общества возникло и неуклонно усиливалось противоречие между индустриальным характером материального производства и характером управления этим производством, существенно зависящим от искусства управленческого персонала. В целях преодоления названного противоречия управление должно быть переведено на принципы и методы поточно-индустриального производства. Осуществление такого перевода составляет главную задачу постиндустриального общества. А поскольку всякое управление есть информационный процесс (второй закон кибернетики), то информация приобретает статус главного ресурса общества со всеми вытекающими из этого требованиями, предъявляемыми к обращению с ним.

Существенные изменения в организации информационных технологий. Современные информационные технологии характеризуются массовым насыщением сверхбыстро действующими

средствами ЭВТ и объединением их в глобальные сети, что обеспечивает расширение обработки огромных объемов информации в очень короткие сроки со всеми вытекающими последствиями.

Все возрастающие опасности злоумышленных действий над информацией и злоумышленного ее использования. О возможных злоумышленных действиях по отношению к информации можно судить по нашумевшему в свое время делу Владимира Левина. Возможности же злоумышленного использования информации достигли такого уровня, что уже практически ведутся информационные войны.

Объективные предпосылки видоизменения постановки задачи защиты информации создаются следующими обстоятельствами.

Наличие богатого опыта организации различных защитных процессов по отношению к информации как в традиционных, так и в автоматизированных технологиях ее обработки. Так, отработаны современные методологии обеспечения сохранности (целостности) информации, ее надежности, качества обработки и выдачи, регулирования использования (предупреждения несанкционированного доступа).

Значительные достижения в научном обеспечении названных выше процессов. Большое развитие получила теория надежности ([27], [28] и др.), теория обеспечения качества информации ([29], [30] и др.). В последние годы разработаны основы теории защиты информации ([31] и др.).

Возможности решения всех проблем организации защитных процессов по отношению к информации в рамках единой концепции. Такой концепцией может стать разрабатываемая в теории защиты информации упоминавшаяся унифицированная концепция защиты информации. Состав и содержание УКЗИ достаточно детально изложены в [31].

Основное содержание видоизменения постановки задачи защиты может быть сведено к совокупности следующих направлений:

1) интегральное представление понятия комплексности защиты информации в целевом и инструментальном планах;

2) расширение рамок защиты от обеспечения компьютерной безопасности до защиты информации на объекте и защиты информационных ресурсов региона и государства;

3) комплексное организационное построение систем защиты информации;

4) организация не только защиты информации, но и защиты от нее;

5) обеспечение условий наиболее эффективного использования информации;

6) переход к так называемой упреждающей стратегии осуществления защитных процессов.

Нетрудно видеть, что при таком подходе проблема защиты информации перерастает в более общую проблему управления информационными ресурсами.

Рассмотрим основное содержание видоизмененной постановки задачи по каждому из названных направлений.

1. Интегральное представление понятия комплексности защиты информации. Данное представление чаще других встречается в работах по защите информации, чем подтверждается тезис о том, что при решении любых проблем защиты требуется системный подход, поскольку сумма даже высокоеффективных независимых решений основных вопросов защиты совсем не гарантирует эффективной защиты в целом. Поэтому если, например, о комплексной защите говорят специалисты по ПЭВМ, то надо понимать защиту только в пределах отдельно взятого компьютера, а когда говорят специалисты по антивирусной борьбе, то только защиту от вирусов. Но в настоящее время, когда средства ВТ (и прежде всего ПЭВМ) получили массовое распространение, а требования к надежности обеспечения различных видов защиты информации (обеспечение физической и логической целостности, предупреждение несанкционированных получения, модификации и размножения) и к рациональному использованию выделенных на эти цели ресурсов неизмеримо возрастают, само понятие комплексности защиты должно быть комплексным. Суть такого интегрального понимания комплексности показана на рис. 1.4. Нетрудно заключить, что интегральному представлению понятия комплексности соответствует правый нижний элемент представленной классификации.

2. Расширение рамок защиты информации. Данный аспект видоизменения постановки задачи защиты информации определяется двумя самыми последними шагами, осуществленными в этой области. Первый - это переход от компьютерной безопасности к проблеме комплексной защиты в автоматизированных системах и второй - это организация решения соответствующих задач в масштабе региона и государства в целом. Таким образом, масштаб проблемы защиты информации представляется в виде трехуровневой структуры: компьютерная безопасность, защита информации на объекте, защита информации в регионе (государстве).

Без дополнительных обоснований, очевидно, можно утверждать, что при переходе от первого уровня ко второму и от второго к третьему происходит не только количественный рост задач защиты, но и появление качественно новых, более сложных задач.

ЦЕЛИ ЗАЩИТЫ	МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ		
	Только одного вида	Нескольких видов	Всех имеющихся видов
ОДНА	Локальная защита информации		
НЕСКОЛЬКО		Полукомплекс- ная защита информации	
ВСЕ			Комплексная защита информации

**Рис. 1.4. Классификация возможных подходов
к защите информации**

Так, при организации защиты информации на объекте дополнительно существенно расширяется круг разновидностей типовых структурных компонентов (ТСК), в которых должна быть обеспечена защита.

Дополнительно к тем разновидностям, которые в общем случае имеют место в автоматизированных системах, (см., например, [31]), добавляются традиционные организационные структуры объекта: контрольно-пропускные пункты (они являются, с одной стороны, частью системы защиты, а с другой - объектами защиты); подразделения традиционного делопроизводства; коллективы и рабочие помещения функциональных подразделений; вспомогательные подразделения и т.п. Для обеспечения надежности защиты информации особое значение имеет предупреждение возникновения условий, благоприятствующих порождению угроз безопасности информации, отсюда существенно повышается значимость законодательных, организационно-психологических и морально-

Глава 1

этических средств защиты. Таким образом, внимание сосредотачивается на системных вопросах защиты информации, а именно:

- 1) формировании и обосновании общей политики защиты;
- 2) подборе и расстановке кадров с учетом требований защиты;
- 3) обучении кадров (руководителей объекта и его функциональных подразделений, сотрудников функциональных подразделений) вопросам защиты в современных условиях;
- 4) системотехническом проектировании комплексной системы защиты информации на объекте;
- 5) четкой организации технологии функционирования системы защиты во всех режимах и условиях деятельности объекта;
- 6) сборе, накоплении и аналитико-синтетической обработке данных о функционировании системы защиты информации.

При переходе же на региональный (а тем более - государственный) уровень рассмотрения проблемы все более превалирующее значение приобретают задачи стратегического плана - создание и преумножение информационных ресурсов, их сбережение и использование в соответствии с экономическими и политическими потребностями развития, включая и потребности обеспечения информационной безопасности. Все это уже означает не просто защиту информации в процессе ее обработки и защиту от информации в процессе ее циркуляции, а системную увязку задач обеспечения информационной безопасности с остальными задачами решения информационных проблем общества.

Само собою разумеется, что все вопросы, связанные с информационной безопасностью вообще, и с защитой информации в частности, будут решаться в рамках унифицированной информационной технологии. Но поскольку эта технология предполагает массовое применение, то она по определению должна обеспечивать высокоеэффективное информационное обеспечение деятельности современных объектов (предприятий, учреждений, иных организаций) и быть экономной с точки зрения расходования ресурсов на ее разработку, тиражирование и эксплуатацию. Достижение этих целей возможно лишь при тщательном системном учете всех факторов, которые оказывают влияние на структуру, содержание и организацию функционирования информационной технологии. Совершенно очевидно, что проблемы обеспечения информационной безопасности (т. е. защиты информации и защиты от информации) относятся к числу существенно значимых факторов, поэтому на современном этапе они должны решаться не сами по себе, а как составляющая часть общей проблемы информатизации.

Есть еще один очень важный аспект рассматриваемого вопроса.

Как известно, любое индустриальное производство предполагает непрерывное и непрерывное управление перерабатываемыми на индустриальной основе ресурсами. В индустриальных информационных технологиях на индустриальной основе обрабатывается информация, чем предопределяется необходимость управления информацией по всем законам современной науки управления. Отсюда следует, что вопросы защиты информации должны решаться как составная часть задачи управления информацией.

3. Комплексное организационное построение систем защиты информации. Прежде всего заметим, что примерно до середины XX столетия у нас в стране в плане защиты информации специализированные органы создавались только для защиты секретной информации, обобщенно они назывались режимно-секретными органами. Данные структуры обеспечивали соблюдение правил работы с секретными данными, правил секретного документооборота и функционирования режимных объектов. В итоге сложилась довольно стройная и эффективно функционирующая система организационной защиты. К этому следует добавить, что в тот же период по мере расширения возможностей технической разведки все более угрожающей становилась опасность утечки информации по техническим каналам. Пересяжение технических каналов возможно лишь специфическими методами и с широким использованием специальных технических средств, что могут осуществить лишь специалисты, имеющие фундаментальную инженерно-техническую подготовку. Для решения этой задачи были созданы специальные органы противодействия технической разведке. Стойкую организационную структуру названные органы приобрели с созданием в 1973 г. Государственной технической комиссии (Гортехкомиссии) с развитой системой региональных органов.

Когда для обработки секретной информации стали регулярно применяться средства ЭВТ, возникли новые задачи обеспечения ее защищенности в автоматизированных системах. Поскольку для решения этих задач необходимы знания методов автоматизированной обработки, то для их решения стали создаваться самостоятельные подразделения, состоящие из специалистов соответствующего профиля. С течением времени образовалась система органов защиты информации в автоматизированных системах, причем обозначилась и на практике реализуется тенденция объединения их с органами противодействия технической разведке. В настоящее же время, особенно под воздействием массового распространения персональных ЭВМ, актуальной стала задача объединения всех названных органов в единую комплексную структуру органов защиты информации.

При этом создание такой единой структуры не должно быть сведено к механическому объединению рассмотренных выше трех видов органов. В итоге объединения должна быть создана такая структура, которая могла бы реализовать комплексную интенсивную защиту в полном соответствии с современными потребностями и возможностями.

4. Организация защиты от информации. Выше уже отмечалось, что, помимо защиты информации второй составляющей обеспечения информационной безопасности является защита от информации, т. е. защита электронных информационно-управляющих систем и людей (отдельно взятого человека, коллектива людей, населения региона) от разрушающего воздействия информации. Важность и актуальность данной проблемы в настоящее время является общепризнанной. Что же касается уровня ее изучения и научной разработки, то системно-концептуальные подходы к проблеме находятся только в зародышевом состоянии. Объективная причина такого положения заключается в необычности проблемы, чрезвычайной ее сложности, многоаспектности и высоком уровне неопределенности. Существует и субъективная причина, заключающаяся в отсутствии до последнего времени общегосударственной востребованности серьезного решения этой проблемы. Положение здесь должно существенно улучшиться в связи с принятием Доктрины информационной безопасности Российской Федерации.

В средствах массовой информации время от времени появляются публикации по отдельным вопросам и конкретным фактам злоумышленного использования информации как средства противоборства при силовом решении политических, социальных и экономических проблем. Наиболее серьезные исследования проблем информационной борьбы выполнил профессор Н. А. Костин (см. его статью в журнале «Безопасность информационных технологий», №4, 1996 г.). Имеются и другие публикации, заслуживающие внимания. Однако системные теоретико-концептуальные исследования проблемы защиты от информации еще ждут своего осуществления.

В § 1.1 уже упоминалась возможность трансформации в этих целях основных положений унифицированной концепции защиты информации и использования их для решения задачи защиты от информации. Основанием реальности такого подхода служат два обстоятельства: сравнительно тесная родственная связь обеих задач и высокий уровень разработки и научной обоснованности УКЗИ. Как показывает практика использования основных положе-

ний УКЗИ при создании реальных систем защиты информации, она применима для обеспечения эффективной защиты информации в любых системах ее обработки и на всех трех уровнях защиты: компьютерном, объектовом, региональном (государственном). На этой основе сделан фундаментальный вывод о том, что полномасштабная реализация УКЗИ создает все необходимые объективные предпосылки для повсеместного перехода от экстенсивных к интенсивным способам защиты информации. Такой переход обеспечит высокую, полностью управляемую надежность защиты и существенное снижение расходов на ее организацию. Пути и проблемы интенсификации процессов защиты информации являются основным предметом следующих глав данной книги.

1.4. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации

В энциклопедических изданиях понятие «интенсивный» определяется как напряженный, усиленный, дающий высокую производительность. В соответствии с этим интенсификация определяется как усиление, увеличение напряженности, производительности, действенности. Применительно к производству интенсификация конкретизируется как его развитие на основе применения все более эффективных средств и технологических процессов, использования передовых методов организации труда, достижений научно-технического прогресса. Альтернативным интенсивному способу является способ экстенсивный, при котором рост объема производства достигается за счет количественного увеличения вовлекаемых в производство ресурсов без качественных изменений производственных процессов.

Приведенные выше общие положения полностью соответствуют процессам, происходящим в последнее время в области защиты информации. При этом преобладавший до недавнего прошлого экстенсивный подход к защите информации в его чистом виде означает независимую организацию защиты на каждом объекте. Интенсивный же подход предполагает организацию защиты информации на всех объектах в соответствии с некоторой единой, научно обоснованной концепцией.

В более развернутом виде переход к интенсивным способам защиты означает целенаправленную реализацию всех достижений теории и практики, которые в концентрированном виде отражены в УКЗИ. При этом можно выделить следующие основные положения унифицированной концепции, практическая реализация которых и будет означать переход к интенсивным способам защиты информации.

Непременное (перед решением вопросов защиты) структурированное описание среды защиты. Такое описание представляет структуру защищаемого объекта и технологию обработки информации на нем в виде направленного графа, вершины которого отображают структурные компоненты объекта, а дуги - направления циркуляции информации в процессе его функционирования. В целях создания условий для унификации методов такого представления введены понятия типового структурного компонента и типового состояния компонента.

Всесторонний и количественный (хотя бы приближенный, оценочный, рамочный) анализ степени уязвимости информации на объекте. Такой анализ необходим прежде всего для возможно более объективной оценки реальных угроз информации и необходимых (достаточных, но оправданных) усилий и расходов на ее защиту. При нынешних масштабах работ по защите информации суммарный эффект от оптимизации расходов на защиту будет огромным. В основах теории защиты информации (см., например, [31]) разработана довольно развитая методология оценки уязвимости информации, состоящая из трех элементов: системы показателей уязвимости, системы угроз информации и системы моделей определения текущих и прогнозирования ожидаемых значений показателей уязвимости. Эта методология создает объективные предпосылки для научно обоснованного решения данной задачи. Однако практическая реализация разработанной методологии сопряжена с преодолением больших трудностей, связанных с формированием баз исходных данных, необходимых для обеспечения моделей оценки уязвимости. Подходы к преодолению этих трудностей будут рассмотрены ниже.

Научно обоснованное определение (и желательно в количественном выражении) требуемого уровня защиты на каждом конкретном объекте и в конкретных, вообще говоря, изменяющихся условиях его функционирования. Трудности решения этой задачи определяются тем, что на требуемый уровень защиты оказывает влияние большое количество разноплановых факторов. В силу этого до сих пор требуемый уровень защиты оценивался качественными показателями. В [31] рассмотрен подход к более объективному определению требуемого уровня защиты, основанный на структуризации факторов, влияющих на этот уровень, и количественных оценках этих факторов. Указанные оценки определяются экспертным путем. Есть основания утверждать, что реализация предложенной методики позволит решить поставленную задачу.

Решение всех задач, связанных с созданием и организацией систем защиты информации на объекте, должно осуществляться на основе единой унифицированной методологии, обеспечивающей построение оптимальных систем защиты с количественными оценками получаемых решений. При этом оптимизация систем защиты понимается в одной из двух постановок: первая - при имеющихся ресурсах, выделенных на защиту, обеспечить максимально возможный уровень защиты информации; вторая - обеспечить требуемый уровень защиты информации при минимальном расходовании ресурсов. Для достижения указанных целей в УКЗИ предложен так называемый кортеж концептуальных решений по защите информации, состоящий из следующей последовательности: функции защиты - задачи защиты - средства защиты - система защиты. Основное назначение кортежа заключается в создании объективных предпосылок для синтеза оптимальных систем защиты информации с количественными оценками достигаемого уровня защиты. Детальное описание взаимодействия компонентов кортежа приведено в упоминавшейся выше книге [31]. В конспективном виде оно заключается в следующем.

По требуемому уровню защиты информации определяется требуемый уровень надежного осуществления каждой из полного множества функций защиты (условия полноты и состав полного множества функций приведены в [31]).

2) Заблаговременно должны быть составлены различные варианты наборов задач, решением которых могут осуществляться функции защиты. Из всех потенциально возможных наборов выбираются те, которые обеспечивают требуемый уровень надежного осуществления каждой из функций наименьшим числом решаемых задач.

3) Заблаговременно для каждой задачи должны быть составлены различные наборы возможных средств, которыми могут быть решены эти задачи. В каждом конкретном случае из всех потенциально возможных наборов выбираются те, которые обеспечивают решение всех выбранных на предыдущем этапе задач при минимальном расходовании ресурсов.

4) Все выбранные средства защиты информации объединяются в единую систему защиты по всем канонам построения систем организационно-технологического типа (принципы и методы организации и обеспечения функционирования систем защиты информации достаточно детально рассмотрены в [31]).

Рассмотрим теперь более подробно проблемы, связанные с преодолением трудностей, возникающих при практической реализации приведенного кортежа решений по защите информации.

Наиболее серьезной проблемой здесь является формирование баз исходных данных для моделей УКЗИ. Задача эта, во-первых, весьма трудоемкая, а во-вторых, не имеющая строго формальных методов решения.

О трудоемкости задачи можно судить по тому количеству данных (величин), которые надо определять. Так, для обеспечения исходными данными моделей оценки уязвимости информации необходимы значения вероятностей: 1) доступа нарушителей различных категорий в те зоны объекта защиты, в которых могут осуществляться злоумышленные действия; 2) проявления в зонах различных каналов несанкционированного получения информации (КНПИ) в различных структурных компонентах защищаемого объекта; 3) доступа нарушителей различных категорий, находящихся в зоне, к проявившимся там КНПИ; 4) наличия в проявившемся КНПИ защищаемой информации в момент доступа к нему нарушителя. Если учесть, что (см. [31]) число категорий потенциальных нарушителей равно 10, зон злоумышленных действий - 5, типовых структурных компонентов - 25, КНПИ - 100, то общее число необходимых для обеспечения моделей величин $N = 10 \times 5 + 100 \times 25 + 100 \times 10 + 100 \times 25 = 6050$.

Для определения требуемого уровня защиты информации необходимы также показатели важности каждого влияющего на него фактора. В [31] выделено 67 таких факторов, объединенных в 5 групп по характеру их происхождения, характеру обрабатываемой информации, архитектуре объекта защиты, условиям функционирования объекта, технологии обработки информации, организации работы объекта.

Из приведенного выше краткого описания кортежа концептуальных решений по защите информации следует, что реализация всех потенциально возможных кортежей может быть осуществлена лишь при наличии следующих данных:

вероятности надежного осуществления функций защиты при решении каждого из потенциально реальных наборов задач;

надежности решения каждой из задач защиты каждым из наборов средств защиты;

стоимости используемых средств защиты.

Трудности формирования указанных баз исходных данных помимо традиционных трудностей решения сложных задач большого объема усугубляются еще весьма высоким уровнем неопределенности, которая обуславливается непредсказуемостью поведения злоумышленников. Углубленные исследования данного аспекта проблемы в процессе формирования теории защиты информации

неминуемо приводят к выводу, что единственным выходом из этого положения является широкое применение для решения задач подобного характера, так называемых неформально-эвристических методов: экспертных оценок, мозгового штурма и психоинтеллектуальной генерации. Следовательно, мы приходим к безальтернативному выводу о том, что переход на интенсивные методы защиты информации возможен лишь при широком применении неформально-эвристических методов, особенно методов экспертных оценок.

Однако эффективность указанных методов существенно зависит от представительности тех выборок, на которых они осуществляются. Кроме того, с учетом непрерывного изменения условий защиты, возможностей злоумышленного доступа к защищаемой информации, а также возможностей ее защиты эксперты оценки должны быть не просто перманентными, а практически непрерывными. Всем этим требованиям можно удовлетворить лишь при наличии стройной и целенаправленной организации системы сопровождения работ по защите информации. Наиболее полным и наиболее адекватным решением этой проблемы было бы создание сети специализированных центров защиты информации (ЦЗИ), каждый из которых представлял бы собою самостоятельное научно-производственное предприятие, укомплектованное высококвалифицированными специалистами и специализирующееся на аккумулировании всех новейших достижений в области защиты, формировании научно-методологического и инструментального базиса для решения соответствующих задач на интенсивной основе (включая и базы необходимых исходных данных) и оказании широкого спектра услуг абонентам соответствующего центра. Концепция создания и организации работы ЦЗИ к настоящему времени разработана достаточно полно, наиболее детально она изложена в [34]. В соответствии с этой концепцией в настоящее время в системе высшей школы уже созданы более 20 региональных учебно-научных центров.

Одной из весьма важных функций ЦЗИ должна стать непрерывно проводимая экспертиза в целях формирования рассмотренных выше баз исходных данных. Формами экспертизы могут быть:

- обследование конкретных объектов, являющихся абонентами соответствующего ЦЗИ;
- непрерывное наблюдение за процессами функционирования действующих систем защиты информации;
- традиционные экспертные оценки;
- организация сеансов мозгового штурма;
- организация сеансов психоинтеллектуальной генерации.

В качестве экспертов могут выступать сотрудники ЦЗИ (которые по определению должны быть высококвалифицированными специалистами), компетентные специалисты служб защиты информации на объектах, сотрудники организаций, занимающиеся вопросами защиты, профессорско-преподавательский состав, научные сотрудники и аспиранты вузов, готовящих соответствующих специалистов.

Нетрудно видеть, что при достаточно развитой сети ЦЗИ (а создание именно развитой сети центров является объективной необходимостью) будет решена (и весьма эффективно) задача массовой экспертизы, в чем и заключается центральная идея данного мероприятия.

Второй важной составляющей объективных предпосылок успешного решения обсуждаемой проблемы являются значительные теоретические достижения в исследовании проблем защиты информации и богатый опыт их практического решения.

Один из дискуссионных вопросов, поднимаемых в процессе обсуждения проблемы организации массовой экспертизы, заключается в чрезвычайно большом разнообразии условий защиты информации на современных объектах и невозможности выразить единым значением ту или иную характеристику, общую для всех объектов. Ведь, например, при прочих равных условиях вероятности доступа злоумышленника к некоторым КНПИ существенно зависят даже от того этажа, на котором расположены средства обработки защищаемых данных. Игнорировать это обстоятельство никак нельзя. Но уже сейчас можно назвать, по крайней мере, два выхода из этого объективно сложившегося положения, первый из которых заключается в проведении экспертизы по методу синтеза, второй - по методу анализа.

Экспертиза по методу синтеза заключается в формировании соответствующих данных каждым ЦЗИ для конкретных объектов - абонентов центра. Полученные данные могут подвергаться всесторонней аналитико-синтетической обработке в целях получения обобщенных оценок любого уровня обобщения.

Экспертиза по методу анализа может осуществляться следующим образом. Сначала формируется возможно более полный перечень факторов, влияющих на защиту информации, выбираются возможные значения каждого из факторов и экспертно определяются относительные веса групп факторов, различных факторов в пределах группы и значения каждого фактора в общей их совокупности. По этим данным можно сформировать поле потенциально возможных условий защиты (как всевозможных сочетаний одного

значения каждого из факторов) и определить вес каждой точки в этом поле. Затем методами кластерного анализа поле потенциально возможных условий может быть разделено на некоторое число классов, каждый из которых будет объединять однородные (сходные) в некотором смысле условия. После этого необходимые данные могут определяться отдельно для каждого класса. Данный подход формирования и классификации поля потенциально возможных условий защиты информации детально изложен в [31] и является предметом самостоятельного рассмотрения в последующих главах данной книги.

В заключение обратим внимание еще на одно весьма важное обстоятельство. Нетрудно видеть, что в деле перевода процессов защиты информации на интенсивные способы заинтересованы практически все специалисты по защите и все руководители тех объектов, на которых должна осуществляться защита. Для широкого распространения сведений о достижениях в этом плане и обсуждения вопросов заинтересованными специалистами необходимо организовать регулярное их освещение в периодической печати.

Краткие выводы

1. Возрастание роли информации, информационных ресурсов и технологий в жизни граждан, общества и государства в XXI веке выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности. «Укрепление информационной безопасности» названо в Концепции национальной безопасности Российской Федерации в числе важнейших долгосрочных задач.

Под информационной безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. В соответствии с этим определением общая схема обеспечения информационной безопасности может быть представлена двумя параллельными процессами: защитой информации и защищкой от информации.

2. Проблемы защиты информации являются производными относительно более общих проблем информатизации, поэтому концептуальные подходы к их решению должны взаимоувязываться с концепцией информатизации, ключевым звеном которой является формирование информационной индустрии, базирующейся на современных средствах и унифицированных методах обработки информации.

3. Ретроспективный анализ развития подходов к решению проблем защиты информации показывает, что их история может быть довольно четко разделена на три периода, которые названы соответственно эмпирическим, концептуально-эмпирическим и теоретико-концептуальным. Сущность подходов к защите в течение этих периодов изменилась от выбора средств защиты на основе опыта через все более настоятельные попытки разработки и научного обоснования методов оценки уязвимости информации и синтеза оптимальных механизмов защиты к разработке в настоящее время основ теории защиты информации, постановке задачи многоаспектной комплексной защиты и формированию унифицированной концепции защиты. Изменялись и применяемые средства защиты от функционально ориентированных механизмов до системы комплексной защиты и создания изначально защищенных информационных технологий.

4. Современный взгляд на защиту информации как на комплексную проблему неминуемо приводит к возрастанию значимости системных вопросов, связанных с процессом защиты. Среди них: формирование и обоснование общей политики защиты, оптимизация процессов проектирования и функционирования комплексных систем защиты, подбор, обучение и расстановка соответствующих кадров специалистов, сбор и аналитико-синтетическая обработка данных о функционировании реальных систем защиты информации.

Таким образом, возникают необходимые объективные предпосылки для перехода к новому этапу в решении задач защиты - этапу интенсификации процессов защиты информации.

5. Переход от экстенсивных к интенсивным способам защиты информации означает целенаправленную реализацию всех достижений теории и практики защиты, которые в концентрированном виде отражены в унифицированной концепции защиты информации, а именно: структурированное описание среды защиты, всесторонний количественный анализ степени уязвимости информации на объекте, научно обоснованное определение требуемого уровня защиты на каждом конкретном объекте и в конкретных условиях его функционирования, построение оптимальных систем защиты на основе единой унифицированной методологии.

Реализация всех этих требований возможна лишь при наличии стройной и целенаправленной организации системы сопровождения работ по защите информации. Наиболее полным и адекватным решением этой проблемы является создание сети специализированных центров информационной безопасности.

Глава вторая

ОСНОВЫ ТЕОРИИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Особенности и состав научно-методологического базиса решения задач защиты информации

Наиболее полное и адекватное описание любого изучаемого фрагмента объективного мира (процесса, явления) может быть получено на основе научно-методологического базиса, в качестве которого выступает некоторая теория, представляющая собой совокупность основных идей и дающая целостное представление о закономерностях и существенных связях действительности. Сказанное, естественно, в полной мере относится и к такому фрагменту объективного мира, как защита информации. Поэтому задача разработки целостной теории защиты является одним из главных направлений работ в области создания методов и технических средств обеспечения безопасности информации.

В процессе исследований по этому направлению на сегодняшний день созданы основы достаточно полной и стройной теории защиты, которые изложены в ряде журнальных статей (в основном, в журнале «Безопасность информационных технологий»), отражены в брошюре [35] и включены в учебник по защите информации [31] в качестве самостоятельной главы (гл. 2, с. 55-117). Первоначальный вариант основ теории защиты информации носил сугубо вербальный (описательный) характер, в последующем удалось сформировать ее структуру в аксиоматическом представлении.

На содержание теории существенное влияние оказало то обстоятельство, что процессы защиты информации носят ярко выраженный стохастический и в значительной мере непредсказуемый характер. В силу этого методология и методы классической теории систем оказались не вполне адекватными для описания и моделирования процессов защиты информации. Возникла необходимость широкого привлечения методов, основанных на использовании эвристических способностей человека.

Дадим определение и сформулируем основные понятия теории защиты информации.

Глава 2

Теория защиты информации определяется как система основных идей, относящихся к защите информации в современных системах ее обработки, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся и развивающаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

В приведенном определении уже содержатся общие сведения о задачах теории защиты, в более же развернутом виде теория защиты должна:

- 1) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты;
- 2) полно и адекватно отображать структуру и содержание взаимосвязей с родственными и смежными областями знаний;
- 3) аккумулировать опыт предшествующих исследований, разработок и практического решения задач защиты информации;
- 4) ориентировать в направлении наиболее эффективного решения основных задач защиты и предоставлять необходимые для этого научно-методологические и инструментальные средства;
- 5) формировать научно обоснованные перспективные направления развития теории и практики защиты информации.

Сформулированным целевым назначением теории защиты предопределяется ее состав и общее содержание. Составляющими частями ее, очевидно, должны быть:

- 1) полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;
- 2) систематизированные результаты ретроспективного анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты, полно и адекватно отображающие наиболее устойчивые тенденции в этом развитии;
- 3) научно обоснованная постановка задачи защиты информации, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;
- 4) общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;
- 5) методы, необходимые для наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные приложения;

6) методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;

7) научно обоснованные предложения по организации и обеспечению работ по защите информации;

8) научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Приведенный перечень составных частей даже при таком очень общем представлении их содержания свидетельствует о многоаспектности теории защиты, что, естественно, порождает значительные трудности ее формирования. Эти трудности усугубляются еще тем, что по мере развития исследований, разработок и практической их реализации появляются новые аспекты, защита информации представляется все более комплексной и все более масштабной проблемой. Существенное влияние оказывает также неординарность проблемы защиты, наиболее существенным фактором которой является повышенное влияние на процессы защиты случайных трудно предсказуемых событий. Всем изложенным предопределается настоятельная необходимость выбора и обоснования методологических принципов формирования самой теории защиты.

Общеметодологические принципы формирования теории, методы решения задач и методологический базис в совокупности составляют научно-методологическую основу теории защиты информации. Структура и содержание названных компонентов этой основы рассматриваются в следующих параграфах данной главы.

2.2. Общеметодологические принципы формирования теории защиты информации

Всю совокупность общеметодологических принципов удобно разделить на две группы: общетеоретические и теоретико-прикладные.

Основные принципы общетеоретического характера могут быть сформулированы следующим образом.

1) Четкая целевая направленность исследований и разработок, причем цели должны быть сформулированы настолько конкретно, чтобы на любом этапе работ можно было предметно оценить степень их достижения. Применительно к теории защиты информации целевой установкой может являться приведенный в предыдущем параграфе перечень составляющих ее компонентов.

2) Неукоснительное следование главной задаче науки, которая заключается в том, чтобы видимое, лишь выступающее в явлении

движение свести к действительному внутреннему движению, которое, как правило, скрыто. Названный принцип ориентирует на поиск научно обоснованных решений изучаемой проблемы, которые в общем случае существенно эффективнее эмпирических. Для рассматриваемых в книге проблем перехода к интенсивным способам защиты информации данное обстоятельство особенно важно, поскольку до настоящего времени пока превалируют эмпирические подходы к их решению.

3) Упреждающая разработка общих концепций, на базе которых могли бы решаться все частные вопросы. Нетрудно видеть, что данный принцип является дальнейшим развитием предыдущего, его требования заключаются в том, чтобы все получаемые научно обоснованные решения образовывали единую систему. Применительно к защите информации и ее интенсификации такая концепция будет рассмотрена ниже.

4) Формирование концепций на основе реальных фактов, а не абстрактных умозаключений. Сущность этого принципа очевидна, следуя ему, выше были приведены результаты ретроспективного анализа фактографических данных о развитии подходов к защите информации.

5) Учет всех существенно значимых связей, относящихся к изучаемой проблеме. Практическая очевидность данного принципа в дополнительной аргументации не нуждается и дает достаточно оснований рассматривать его в качестве одного из основных принципов общетеоретического характера.

6) Строгий учет диалектики взаимосвязей количественных и качественных изменений. Для рассматриваемых здесь проблем перехода от экстенсивных к интенсивным способам защиты информации данный принцип имеет прямое действие, конкретное содержание которого будет изложено при обосновании следующего принципа.

7) Своевременное видоизменение постановки изучаемой проблемы или решаемой задачи. Сущность данного принципа заключается в том, что назревшие качественные изменения, подготовленные изменениями количественными в процессе предшествующего развития изучаемого явления (а они в области развития способов и методов защиты информации, как отмечалось выше, налицо), должны быть актуализированы путем видоизменения самой постановки решаемой задачи.

С учетом современного этапа развития теории и практики защиты информации приведенные общетеоретические принципы могут быть интерпретированы так, как представлено в табл. 2.1.

Основы теории защиты информации

Что касается второй группы принципов, содержащих концентрированно выраженные рекомендации, относящиеся к самому процессу изучения сложных проблем, содержанию и практической реализации результатов изучения, то указанная группа представляется следующими четырьмя принципами.

Таблица 2.1

Интерпретация общеметодологических принципов развития науки применительно к современным проблемам защиты информации

№ п/п	Формулировки принципов	Интерпретация
1	<i>Строгая целевая направленность.</i>	Главная цель - формирование научно-технических предпосылок, необходимых для перехода от экстенсивных способов решения проблем защиты информации к интенсивным, т.е.: дальнейшее развитие основ теории защиты; формирование регулярных методологий анализа степени уязвимости информации, обоснование целесообразного уровня защиты; создание методологии синтеза систем защиты, опимальных по всей совокупности существенно значимых критериев, и оптимального управления системой в процессе ее функционирования.
2	<i>Неукоснительное следование главной задаче науки - за внешними проявлениями вскрыть внутренние движения.</i>	Необходимо: подвергнуть тщательной аналитико-синтетической обработке всю совокупность статистических данных, относящихся к защите информации; выявить устойчивые тенденции в эволюционном развитии теории и практики защиты информации; осуществить прогноз наиболее вероятных направлений развития выявленных тенденций.
3	<i>Упреждающая разработка общих концепций</i>	Уточнение и строгое научное обоснование предложенной унифицированной концепции защиты информации. Формирование на базе кортежа концептуальных решений по защите информации единой методологии создания, организации и обеспечения функционирования систем защиты информации, соответствующих заданным требованиям к защите.

Глава 2

№ п/п	Формулировки принципов	Интерпретация
4	<i>Формирование концепций на основе реальных фактов</i>	<p>Формирование структуры и содержания информационного кадастра по защите информации. Организация систематического и целенаправленного сбора и накопления всех данных, относящихся к защите информации.</p> <p>Регулярная обработка всех накопленных данных в целях обновления и пополнения информационного кадастра по защите информации.</p> <p>Периодический анализ данных информационного кадастра в целях выявления новых фактов относительно различных аспектов защиты информации</p>
5	<i>Учет всех существенно значимых факторов, влияющих на изучаемую проблему</i>	<p>Рассмотрение защиты информации как комплексной проблемы в целевом, инструментальном и организационном аспектах.</p> <p>Рассмотрение проблемы комплексной защиты как составляющей части более общей проблемы управления информацией.</p> <p>Рассмотрение проблемы управления информацией как составляющей части глобальной проблемы информатизации современного общества</p>
6	<i>Строгий учет диалектики взаимосвязей количественных качественных изменений в развитии изучаемых явлений</i>	<p>Необходимо предметно обосновать, что к настоящему времени в развитии проблем защиты информации произошли (накоплены) такие количественные изменения (масштабы работ, объемы расходуемых ресурсов, арсеналы используемых средств), на основе которых вполне созрела необходимость качественных изменений в подходах к организации и обеспечению защиты в общегосударственном масштабе</p>
7	<i>Своевременное видоизменение постановки задачи</i>	<p>Интерпретация требований данного принципа заключается в разработке и обосновании необходимости, сущности и содержания перехода от экспансивных к интенсивным способам решения всех проблем защиты информации</p>

1. Построение адекватных моделей изучаемых систем и процессов. В общепостановочной части данный принцип общепризнан и понятен. До недавнего времени, пока в центре внимания специалистов были преимущественно технические, т.е. строго

формальные системы, не было никаких недоразумений также в плане построения моделей, строго адекватных моделируемым системам и процессам. Однако по мере того, как росла необходимость моделирования систем социально-экономических, подверженных повышенному влиянию случайных и даже трудно предсказуемых факторов, построение адекватных моделей натолкнулось на трудности принципиального характера: методы классической теории систем оказались недостаточно приспособленными для этого. Попытки построения моделей указанных систем с использованием традиционных методов чаще всего приводили к такой трансформации постановки задачи, что в итоге создаваемые модели оказывались неадекватными моделируемым системам. Стало совершенно ясно, что имеющиеся методы моделирования нуждаются в существенном расширении и дополнении.

2. Унификация разрабатываемых решений. Содержание названного принципа специалистам практически очевидно. Заметим только, что он детализирует в известной мере один из аспектов общеметодологического принципа упреждающей разработки общих концепций, поскольку любое унифицированное решение есть своего рода концепция.

3. Максимальная структуризация изучаемых систем и разрабатываемых решений. Структуризация может быть определена как процесс формирования такой архитектуры разрабатываемых систем и технологических схем их функционирования, которая наилучшим образом удовлетворяет всей совокупности условий их разработки, эксплуатации и усовершенствования. В более общей постановке структуризация может рассматриваться как одно из направлений расширения научно-методологического базиса классической теории систем.

4. Радикальная эволюция в реализации разработанных концепций. Результатом изучения сложных проблем, как правило, являются предложения и решения (концепции) по более или менее кардинальному совершенствованию архитектуры соответствующих систем или процессов организации и обеспечения функционирования. Естественно, при этом возникает вопрос о способах практического претворения в жизнь разработанных концепций. Крайними вариантами будут: слева - выбросить (убрать, демонтировать) прежние решения и заново построить систему в строгом соответствии с новыми концепциями, справа - отказаться от новых концепций во имя сохранения прежних решений. В реальной жизни эти крайние варианты если и будут разумными, то лишь в каких-то не-

ординарных ситуациях, в подавляющем же большинстве ситуаций рациональным будет какой-то промежуточный вариант. Для ориентации в подобных ситуациях В.М. Глушков еще в 70-х годах XX века сформулировал принцип так называемой радикальной эволюции, суть которого, как следует из самого названия, сводится к тому, что надо стремиться к радикальным совершенствованиям, но реализовывать их эволюционным путем.

Так в самом общем виде могут быть представлены состав и содержание первой составляющей теории защиты - общеметодологические принципы. Вторая составляющая этой теории - инструментально-методологический базис рассматривается ниже.

2.3. Методологический базис теории защиты информации

Методологический базис как второй компонент теории защиты информации составляют совокупности методов и моделей, необходимых и достаточных для исследования проблемы защиты и решения тех или иных практических задач в этой области.

На формирование названных методов большое влияние оказывает тот факт, что, как отмечалось выше, процессы защиты информации подвержены сильному влиянию случайных факторов, особенно связанных со злоумышленными действиями людей-нарушителей защищенности. В то же время методы классической теории систем, которые на первый взгляд могли бы быть здесь с успехом использованы, разрабатывались применительно к потребностям создания, организации и обеспечения функционирования технических, т. е. в основе своей формальных систем. Попытки применения этих методов к системам с высоким уровнем стохастичности, аналогичным системам защиты информации, показали их недостаточность для решения подобных задач для данных систем. В силу сказанного возникла актуальная задача расширения комплекса методов классической теории систем, которое позволило бы адекватно моделировать процессы, существенно зависящие от воздействия трудно предсказуемых факторов. Наиболее подходящими для указанных целей могут оказаться методы нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений.

Методы теории нечетких множеств применяются для описания систем, элементы которых принадлежат тем или иным множе-

ствам лишь с некоторой вероятностью. К таким элементам могут, например, относиться те или иные каналы несанкционированного получения информации, те или иные средства защиты, с помощью которых может быть эффективно перекрыт тот или иной КНПИ и т. п. Указанные элементы принадлежат соответствующим множествам лишь с некоторой вероятностью, что естественно приводит к заключению о возможности использования для описания процессов защиты информации теории нечетких множеств. Для читателей, интересующихся более подробным изложением этой теории, можно назвать некоторые известные нам работы, которые в той или иной степени полезны для решения проблем защиты информации. К ним относятся статья И. Г. Перфильевой [36] и монография под редакцией Р. Р. Ячера [37]. Основные положения теории нечетких множеств, имеющие принципиальное значение для решения задач защиты информации в современной их постановке, достаточно подробно изложены также в монографии В.А.Герасименко [3].

Методы теории лингвистических переменных используются для построения моделей больших систем, основывающихся на неформальных суждениях и умозаключениях эксперта-аналитика, формируемых им, исходя из накопленного опыта и решения аналогичных проблем. Интерес к этим методам в последние годы значительно возрос в связи с особой актуальностью задач анализа и синтеза человеко-машинных систем, процессы функционирования которых в решающей степени определяются так называемым человеческим фактором.

Поскольку системы защиты информации относятся именно к таким системам, то целесообразность использования методологии теории лингвистических переменных при решении проблем защиты информации не вызывает никаких сомнений.

Исходным базисом теории лингвистических переменных служит совокупность трех посылок [3]:

1) в качестве меры характеристик изучаемых систем вместо числовых переменных (или в дополнение к ним) используются лингвистические переменные;

2) простые отношения между переменными в лингвистическом измерении описываются с помощью нечетких высказываний, которые имеют следующую структуру: «из А следует В», где А и В - переменные в лингвистическом измерении;

3) сложные отношения между переменными в лингвистическом измерении описываются нечеткими алгоритмами.

Пример построения нечеткого алгоритма сложного отношения между переменными «надежность компонентов системы защиты информации» и «интенсивность контроля хранилища носителей защищаемой информации» желающие могут найти в монографии [3] и учебнике [31].

Этот, а также другие примеры аналогичного рода, которые может легко предложить сам читатель, говорят о том, что аппарат теории лингвистических переменных эффективен в ситуациях, когда строгое описание систем и их функционирования или невозможно, или даже нецелесообразно в силу самого характера решаемой задачи. Совершенно очевидно, что в указанных выше случаях отсутствуют необходимые данные как для строгого определения уязвимости информации, так и для оценки эффективности применяемых средств и методов ее защиты.

Можно привести и примеры, когда попытки построить строго количественные алгоритмы решения проблемы являются вредными. К их числу относится на сегодня и выработка общей стратегии защиты информации. Построение строгого алгоритма в этом случае требует принятия таких допущений, что его адекватность становится весьма сомнительной.

Вообще же различного рода нестрогие алгоритмы (на основе теории нечетких множеств или теории лингвистических переменных) целесообразно использовать когда реализация строгого алгоритма, даже, если такой найден, является трудоемкой, а время на нее крайне ограничено, когда множество анализируемых ситуаций слишком велико по сравнению с возможностью их рассмотрения, или, наконец, когда имеющаяся исходная информация такого качества, что результаты реализации строгого алгоритма неминуемо будут сомнительными.

В связи с тем, что методы нечетких множеств или лингвистических переменных в значительной степени используют эвристическую составляющую, эффективное решение с их помощью тех или иных проблем может быть обеспечено только рациональными действиями людей (экспертов-аналитиков). Таким образом, организация функционирования систем с высоким уровнем неопределенности, к которым мы с полным правом относим системы защиты информации, должна включать в себя (и притом в качестве важнейшего атрибута) подготовку персонала к решению соответствующих задач с использованием рассматриваемых методов.

Неформальные методы оценивания. В процессе исследования больших человеко-машинных систем постоянно приходится

оценивать значения их различных параметров. При этом нередки случаи, когда значения этих параметров не удается получить традиционными методами (непосредственно измерить или вычислить по известным аналитическим зависимостям, определить путем статистической обработки их значений, зафиксированных в процессе наблюдения, или по аналогии с уже известными значениями других, схожих параметров). Такая ситуация особенно характерна для систем с высоким уровнем неопределенности, не имеющих достаточной предыстории функционирования. Именно такими являются рассматриваемые здесь системы защиты информации. Зачастую при исследовании этих систем отсутствуют данные, необходимые для определения таких параметров, как вероятности проявления угроз безопасности информации в различных условиях функционирования той или иной системы, вероятности успешной реализации этих угроз злоумышленником, показатели эффективности функционирования различных средств защиты и многих других. В таких случаях естественно приходится пользоваться эвристическими методами, основанными на оценках специалистов-экспертов в соответствующей области.

Из таких неформальных методов оценивания наиболее известными являются методы экспертных оценок. Достоинства указанных методов общеизвестны. Это прежде всего возможность их использования для широкого класса объектов исследования, относительная простота и нетребовательность к качеству исходной информации. Эксперт, будучи опытным специалистом в конкретной предметной области, как бы располагает персональным, уникальным фондом информации, аккумулирующим не только его собственный, но и весь известный ему чужой опыт по данной проблеме. Он широко использует при работе не только простые логические построения и умозаключения, но также интуитивные представления и творческую фантазию.

Вместе с тем, методы экспертных оценок не лишены существенных недостатков. В их числе - субъективность оценок, основанных на интуитивном мнении экспертов, трудная сопоставимость мнений ввиду преимущественно качественного характера оценок, а также необходимость постоянного привлечения группы высококвалифицированных специалистов, что делает процесс прогнозирования достаточно сложным и трудоемким с организационной точки зрения. Как правило, такой процесс поддается лишь очень слабой автоматизации.

На все это до последнего времени мало обращали внимания,

поскольку методам экспертной оценки в области прогнозирования параметров угроз безопасности информации и процессов защиты информации долгое время не было разумной альтернативы. Да и в настоящее время, как следует из приведенного выше анализа, ситуация кардинальным образом не изменилась.

Достаточно подробное изложение основных положений метода экспертных оценок можно найти в книге В.А. Герасименко [3], а также в учебнике [31], к которым мы и адресуем читателя.

Здесь же отметим, что среди множества проблем методов экспертных оценок основной является задача конкретного определения и учета компетентности эксперта как в смысле его профессиональной пригодности к оценке и прогнозированию, так и его индивидуальной способности высказывать конкретные, убедительные суждения о текущем и будущем состоянии объекта исследования. Опыт и квалификация эксперта проявляются в его умении критически оценивать имеющуюся информацию. Однако человеческая психика и мышление в значительной степени консервативны и инертны, что зачастую заставляет эксперта скептически относиться к слишком радикальным оценкам и особенно к прогнозам, тем самым упуская из поля зрения «парадоксы», дающие, как известно, новые знания об исследуемой системе.

Частично избежать присущего эксперту прогнозированию субъективизма суждений помогает использование методов коллективной экспертной оценки с использованием различных процедур и методов обработки мнений экспертов, а также использование в дополнение к экспертной оценке методов математического и имитационного моделирования.

Анализ выполненных на сегодняшний день исследований позволяет выделить две группы математических методов, которые могут применяться для решения рассматриваемых нами задач: метод многофакторного анализа и метод параметрического прогнозирования.

В основе многофакторных статистических методов лежит использование процедур корреляционно-регрессионного анализа. Основным из этой группы методов является метод многошагового регрессионного анализа. Сущность его, как известно, заключается в расчете линейных регрессионных уравнений, описывающих зависимость прогнозируемых характеристик от некоторой совокупности важнейших показателей системы. Другими вариантами использования процедур регрессионного анализа являются метод сегментной регрессии и метод главных компонент.

Параметрические методы прогнозирования дают дополнительные возможности углубленного математико-статистического анализа динамики численных значений изучаемых показателей, а также расширяют возможности моделирования и прогнозирования в условиях достаточно часто наблюдающегося недостатка соответствующей количественной информации по основным показателям ситуации, влияющей на уровень безопасности информации.

Опыт использования приведенных математических методов прогнозирования свидетельствует, что надежность отдельных из них существенно зависит от периода или глубины прогнозирования. Наиболее надежным следует признать метод многошагового регрессионного анализа. При прогнозировании он хорошо сочетается с другими разновидностями методов регрессионного анализа, а также параметрическими методами. Последние имеют ряд чрезвычайно важных преимуществ, главным из которых является невысокая трудоемкость разработки на их базе прогноза и возможность полной автоматизации всего прогностического процесса. Однако, надежные результаты прогнозирования параметрические методы, как показывает опыт, обеспечивают лишь при глубине прогнозирования не более двух шагов, что делает абсолютно нецелесообразным их использование для целей долгосрочного прогнозирования. Основной недостаток методов параметрического типа состоит в их повышенной инертности, вследствие чего базирующиеся на этих методах прогнозы плохо «отрабатывают» вариации временного ряда, содержащие высокочастотные компоненты.

Из приведенного анализа следует, что важнейшим направлением повышения надежности прогнозирования уровня безопасности информации является синтез и «взаимопроникновение» методов экспертных оценок и методов математического моделирования. Такой синтез может быть осуществлен в виде некоторой человеко-машинной системы, формализующей знания эксперта (в том числе и интуитивные) в конкретной предметной области путем проведения вычислительного эксперимента с комплексом математических моделей.

Подробнее эти проблемы будут рассмотрены ниже в § 2.4.

Неформальные методы поиска оптимальных решений. Завершим изложение методологического базиса теории защиты информации рассмотрением неформальных методов поиска оптимальных решений. Назовем оптимальными такие решения проблем защиты информации, которые при заданных затратах ресурсов обеспечивают максимальную защищенность информации или

обеспечивают достижение заданной защищенности при минимальных затратах ресурсов.

Поиск оптимальных решений является наиболее сложной процедурой, осуществляющейся при разработке и обеспечении функционирования больших систем. В настоящее время известно достаточно большое число различных методов оптимизации. Если рассматривать их применение для решения проблем защиты информации, то основные трудности здесь связаны с наличием в постановке оптимизационных задач значительных неопределенностей. В связи с этим особый интерес для формирования научно-методологического базиса защиты информации представляют развивающиеся в последние годы неформальные методы поиска оптимальных решений, суть которых состоит либо в сведении сложной неформальной задачи к формальной постановке и дальнейшем использовании уже реализованных формальных методов, либо в изначальной организации неформального поиска оптимального решения, т. е. в непосредственной реализации процедуры поиска.

Классификационная структура этих методов, заимствованная нами из монографии [3], может быть представлена схемой, приведенной на рис. 2.1.

Остановимся на важнейших характеристиках неформальных методов оптимизации, которые имеют принципиальное значение для их использования в качестве инструментальных средств решения задач защиты информации.

Сведение неформальной задачи к формальной постановке заключается в формировании строго выраженных исходных условий, т. е. определяемых переменных, ограничений, которым они должны удовлетворять, и целевой функции, экстремальное значение которой и соответствует оптимальному решению. Процедура такого преобразования неформальной задачи может быть реализована с использованием рассмотренных выше методов теории нечетких множеств, эвристического программирования и эволюционного моделирования.

В первом случае могут быть получены аналитические выражения для количественных оценок нечетких условий защиты информации с точки зрения проявления тех или иных угроз безопасности информации. Тем самым постановки неопределенных задач сводятся к строго определенным. Далее могут быть использованы соответствующие конечные методы, которые, как известно, гарантируют получение оптимальных решений.

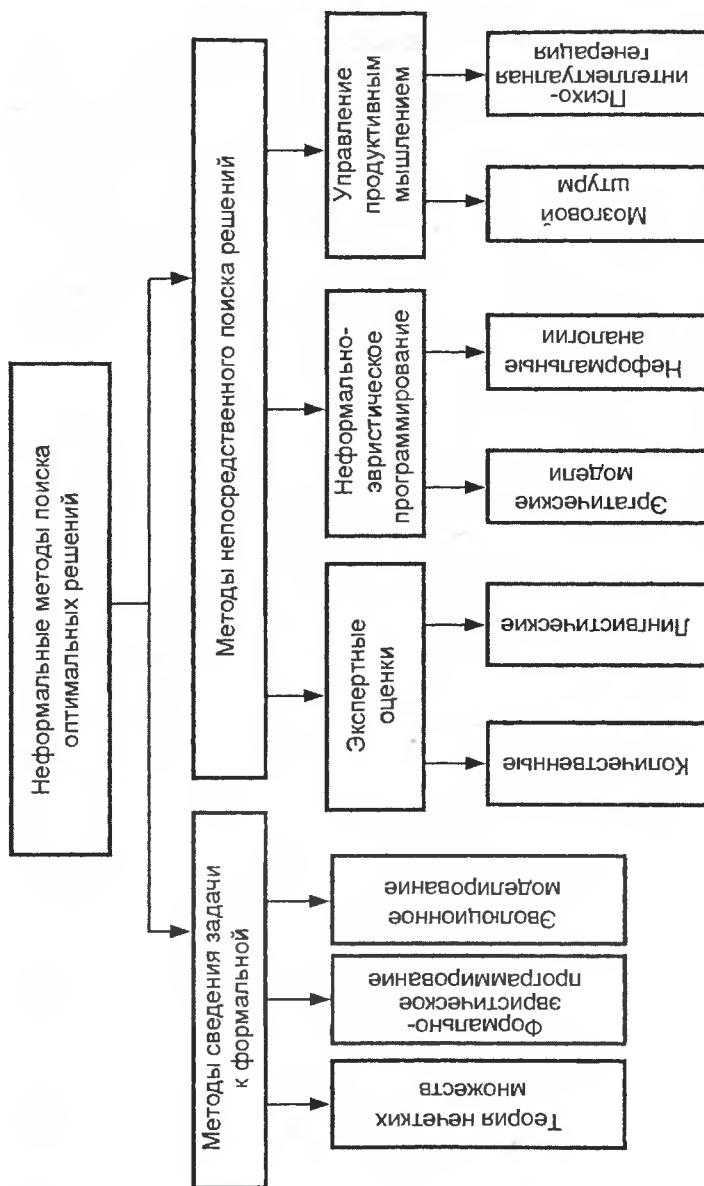


Рис. 2.1. Классификационная структура неформальных методов поиска оптимальных решений

Эвристическое программирование, основу которого составляют формализованные (т. е. представленные в виде конечного алгоритма) эвристики, требует для своего осуществления последовательной реализации следующих процедур: изучения содержания соответствующего класса слабоструктуризованных задач, изучения приемов решения задач данного класса человеком, выявления закономерностей в решении человеком задач рассматриваемого класса, формализации выявленных закономерностей, приемов и правил и построении на этой основе модели решения задач данного класса, алгоритмической реализации построенной модели. Таким образом, с помощью эвристического программирования фактически реализуется задача построения некоторой экспертной системы, формализующей знания эксперта-аналитика в соответствующей предметной области.

Принципиальным моментом, который следует учитывать при решении вопроса об использовании этого метода в составе научно-методологического базиса защиты информации, является то, что эвристическое программирование вовсе не гарантирует получение строго оптимальных решений. В данном случае лучше использовать термин «рациональное» решение, поскольку эвристическое программирование позволяет гарантировать, что найденное решение будет лучшим среди известных альтернативных решений.

Следует отметить, что теория построения эвристических моделей находится еще в стадии разработки. Это понятно, поскольку для формирования такой теории необходимо создать модель продуктивного мышления человека, для которого при решении задач оптимизации характерно, с одной стороны, сужение поля поиска (области допустимых решений) за счет исключения из рассмотрения заведомо непригодных решений, а с другой - расширение поля поиска за счет генерирования новых альтернатив. В отличие от этого при использовании строго формальных методов поле поиска (область допустимых решений) остается неизменным, а сам процесс решения состоит в направленном или случайном преоборе возможных решений. Практически на сегодняшний день говоря об эвристических моделях имеют в виду так называемые лабиринтные и концептуальные эвристики.

В первой из них задача представляется в виде лабиринта возможных путей поиска решения, ведущих как бы от начальной площадки (условий задачи) к конечной (условиям завершения задачи). Естественно при этом предполагается, что эксперт способен достаточно быстро отсечь неперспективные варианты движения по

лабиринту и оставить только те, которые с большей вероятностью приведут к конечной площадке.

Механизм реализации концептуальной эвристики состоит в генерировании множества таких путей решения задачи, которое с большой вероятностью содержит и результативный путь. При этом эксперт-аналитик как бы строит структурированную модель проблемной ситуации, формируя на основе анализа исходной информации обобщенные элементы и отношения между ними, которые получили название концептов. Согласно концептуальной теории [38] универсальному набору концептов соответствуют присущие человеку механизмы вычисления, трансформации и формирования отношений, а сам процесс реализации концептуальной эвристики представляется в виде мысленного эксперимента с структурированной моделью ситуации. Фактически такой процесс представляет собой не что иное, как автоформализацию знаний эксперта, которую мы рассмотрим более подробно в следующем параграфе.

Эволюционное моделирование [39] является фактически некоторой модификацией статистического моделирования, в котором статистически совершенствуется (эволюционирует) сам алгоритм имитации процессов функционирования моделируемых систем.

Блок неформальных методов непосредственного поиска оптимальных решений представлен на рис. 2.1 в составе методов экспертных оценок, неформально-эвристического программирования, а также методов, основанных на управлении продуктивным мышлением человека в процессе решения задачи.

Методы экспертных оценок были рассмотрены нами выше. Использование их естественным образом может быть распространено и на задачи поиска оптимальных решений, выраженных простой оценкой.

Неформально-эвристическое программирование фактически представляет собой разновидность эвристического программирования, когда роль эксперта расширяется, включая непосредственное участие его не только в процессе составления моделей для поиска решений, но также и в процессе непосредственного решения конкретных задач. К разновидностям неформально-эвристического программирования относятся и так называемые неформальные аналогии, когда поиск решения осуществляется на основе precedентов решения аналогичных задач.

Последняя группа представленных на рис. 2.1 неформально-эвристических методов включает методы, основанные на управлении продуктивным мышлением эксперта в процессе самого поиска опти-

мальных решений. Наибольшее распространение получили две разновидности такого управления интеллектуальной деятельностью - метод «мозгового штурма» и метод психоинтеллектуальной генерации.

Первый из них направлен на получение новых решений в результате коллективного творчества группы экспертов, организованного по определенным правилам. Принципиальной особенностью «мозгового штурма» является абсолютное исключение в процессе его проведения критики и вообще какой-либо оценки высказываемых идей. Сущность метода, и это надо особо подчеркнуть, состоит в принципиальном разделении во времени решения двух задач - генерирования новых идей и анализа (оценки) этих идей. Практически при использовании этого метода создаются две разные группы экспертов - генераторов идей и аналитиков.

В отличие от «мозгового штурма» метод психоинтеллектуальной генерации напротив основан на критике и суждениях, высказываемых экспертом. Он реализуется в виде целенаправленной беседы-дискуссии двух непременных участников - ведущего и решающего. Первый ставит вопросы (проблемы), по которым последний высказывает свои суждения. Таким образом, завязывается дискуссия, направляемая ведущим на возможно более полное и глубокое рассмотрение проблемы. Дополнительно в помочь ведущему могут привлекаться оппонент и эксперты. Оппонент определяет слабые места в суждениях решающего и формирует возражения и критические замечания, побуждающие его к энергичной дискуссии. Задача экспертов - помочь ведущему оценивать высказываемые суждения и определять последовательность и содержание дальнейшего обсуждения проблемы.

Подробнее с описанием данных методов можно познакомиться в [3,31].

2.4. Принципы автоформализации профессиональных знаний эксперта-аналитика

Из предыдущего изложения следует, что в задачах оценки состояния и прогнозирования уровня безопасности информации стратегия поиска решения, а также большинство этапов интерпретации результатов должны строиться в основном на неформальных знаниях эксперта и применяемых им интуитивных методах. В связи с этим в исследовательских процедурах такого уровня сложности рассматриваемые неформальные алгоритмы будут существенно различаться не только от одной задачи к другой, но и в рамках одной задачи у разных экспертов-аналитиков.

Таким образом, единственным реальным способом создания моделей исследуемой ситуации на основе формализации алгоритмов аналитической деятельности в этих условиях может быть только автоформализация знаний эксперта, т. е. возникает проблема разработки технологии формализации экспертом своих профессиональных знаний.

В ряде работ Г.Р. Громова (см., например, [40]) предлагается форма автоформализации знаний, основанная на проведении вычислительного эксперимента с моделями, описывающими конкретные объекты предметной области и построенными самими экспертами. Результатом автоформализации в этом случае являются как те новые сведения, которые эксперт получил в ходе эксперимента, так и сами модели, отражающие его глубинные представления о структуре исследуемого объекта и присущих ему качественных и количественных зависимостях.

Последовательность и взаимосвязь этапов автоформализации знаний при таком подходе к проблеме показаны на структурной схеме, приведенной на рис. 2.2.

Если распространить этот подход на задачу анализа процессов защиты информации и оценки уровня безопасности информации, то ее постановку можно формализовать в виде четверки:

$$Z = \langle R_o, R_n, K, U \rangle, \quad (2.1)$$

где R_o - исходное состояние защищаемой системы, определяемое имеющимися в наличии данными;

R_n - прогнозируемое состояние системы, соответствующее ее потенциальным возможностям противостоять угрозам безопасности информации;

K - знания о системе (элементарные и сложные модели, взаимосвязь между ними, ограничения на отдельные параметры и т.п.);

U - функция полезности системы, соразмеряющая эффективность функционирования и затраты на его обеспечение.

Таким образом, исследование проблемы обеспечения безопасности информации можно рассматривать как формальную систему, представляющую выражением (2.1). Функциональная структура процесса принятия решения, отвечающая этому представлению, имеет вид, приведенный на рис. 2.3.

Дадим формализованное описание процесса принятия решения, опирающееся на приведенную функциональную структуру.

Установим, что принятие решений сводится к определению эффективных точек в пространстве состояний системы обеспечения

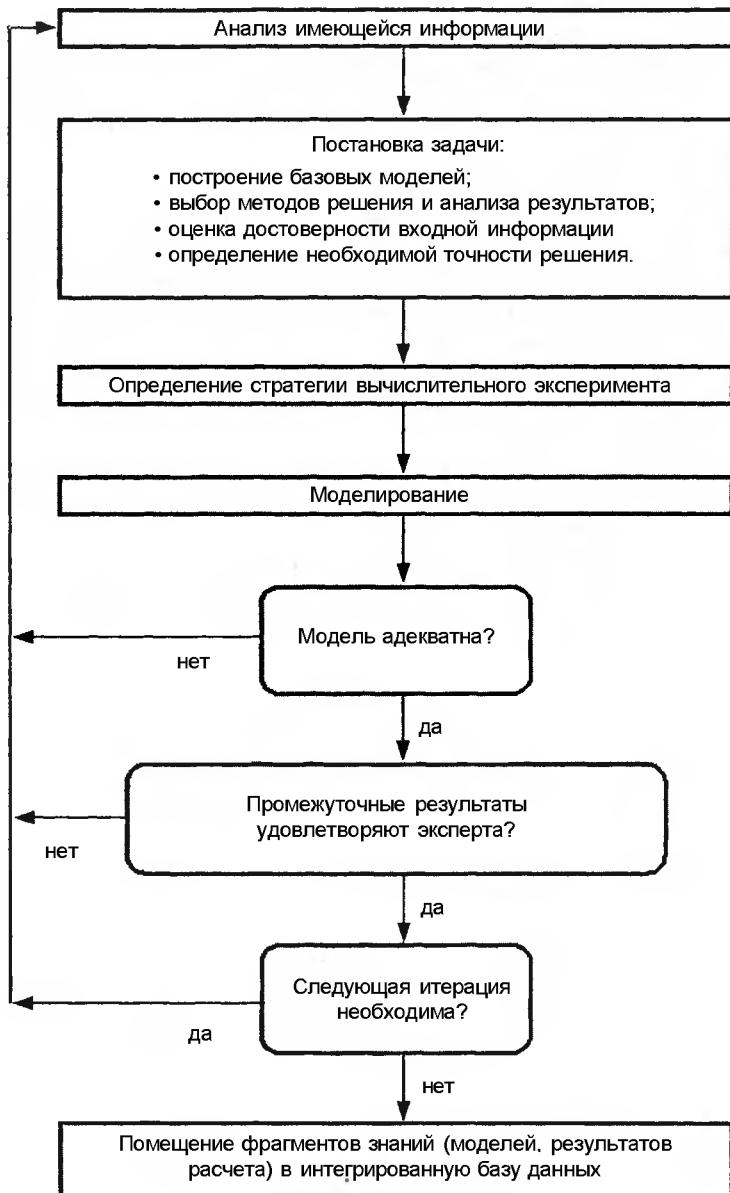


Рис. 2.2. Последовательность этапов автоформализации знаний

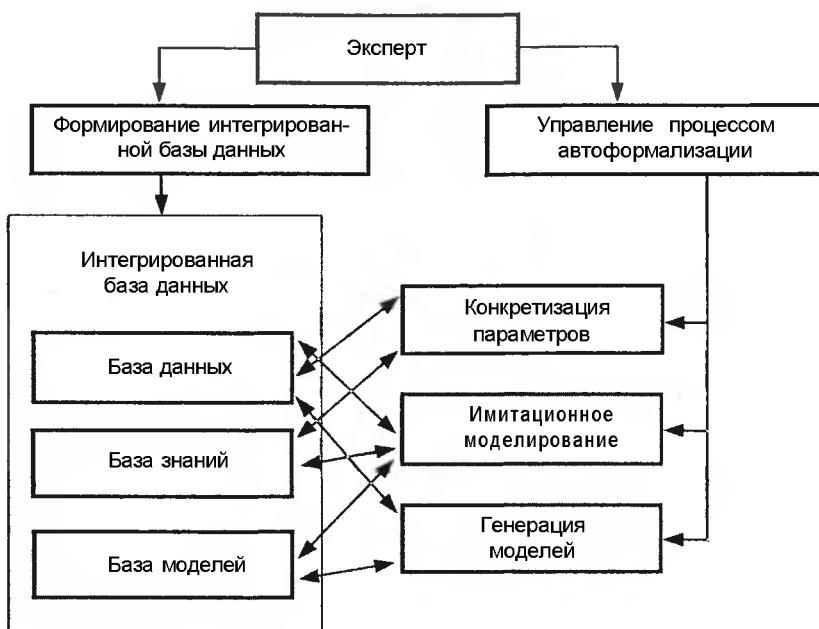


Рис. 2.3. Функциональная структура процесса принятия решения

безопасности информации, соответствующих ее потенциальным возможностям, на базе вычислительного эксперимента с имитационной моделью. Таким образом, выходом процесса является набор параметров системы при максимизации ее функции полезности. Процесс принятия решения включает этапы конкретизации параметров и имитационного моделирования.

Конкретизация параметров представляет собой формирование их исходных значений. Основой конкретизации являются знания K , неявно задающие ориентированный граф без циклов $G = \langle X, \Gamma(X) \rangle$, где X - множество вершин G , а $\Gamma(X) \subseteq X^* X$. Среди вершин X выделяются множества объективных P и функциональных F вершин ($F \cap P = \emptyset$ и $F \cup P = X$). Объективные вершины P соответствуют множеству априорно заданных и вычисляемых параметров, а функциональные F - способам расчета одних параметров через другие. Конкретизация параметров заключается в поиске пути на графе G от определяемого параметра к априорно заданным параметрам и проведении расчетов по полученной схеме. Каждая функциональ-

ная вершина $f \in F$ определяет макропроцедурный механизм, реализуемый через ряд процедур с заданными приоритетами их применения.

Имитационное моделирование осуществляется на основе исходного состояния системы R_0 , целевой функции полезности U и моделей элементов $Q \in K$. В результате моделирования строится решение R_n , соответствующее потенциальным возможностям системы. Формирование R_n осуществляется на основе построения дерева вывода, каждая новая вершина $(R_{t,j})$ которого порождается применением к предыдущему состоянию $(R_{t-1,j})$ некоторого преобразования, определяемого моделью $Q_j \in Q$.

Генерация моделей является ключевой в реализации процесса автоформализации знаний. С ее помощью эксперт формализует свои представления о структуре исследуемого объекта и взаимосвязях отдельных элементов в виде системы динамических моделей K , позволяющей ему в дальнейшем проводить с ее помощью вычислительный эксперимент (имитационное моделирование).

Наиболее сложными проблемами в реализации описываемых процедур, связанными со спецификой задач оценки состояния и прогнозирования уровня обеспечения безопасности информации, являются проблемы формирования базы данных и базы моделей.

При формировании базы данных необходимо учитывать, что вся работа по исследованию состояний безопасности информации априори опирается на систему неполных и неточных исходных данных. Во-первых, достоверность их в сильной степени зависит от точности и надежности источника информации и методики ее получения. Во многих случаях достоверность "окрашивается" интуитивным представлением эксперта об объекте и его субъективным отношением к источнику. Во-вторых, не исключена возможность проведения потенциальными злоумышленниками целенаправленной дезинформации с задачей усложнения адекватной оценки их конкретных намерений при проведении тех или иных мероприятий по осуществлению несанкционированного доступа к защищаемой информации.

Перечисленные моменты вынуждают осуществлять разработку методов, которые позволяли бы корректировать в зависимости от поступающих новых сведений достоверность исходных данных, используемых для прогнозных оценок уровня безопасности информации, а также оценивать степень достоверности получаемых на основе этих данных прогнозов.

В постановочном плане проблема учета недоопределенностей в системах математического моделирования неоднократно рассматривалась в различных работах, посвященных построению моделей тех или иных систем. Однако предлагаемые в них подходы требуют для получения необходимых практических результатов предварительного решения фундаментальной проблемы создания аппарата функций от недоопределенных переменных и аппарата многозначных логик. В то же время продвижение в этой области возможно и при использовании для оценки достоверности некоторых эвристических методов и приемов, опирающихся на известную теорему Байеса. Такой подход представляется даже более целесообразным и перспективным с точки зрения построения практических человеко-машинных систем анализа и прогнозирования. При этом следует иметь в виду принципиальную невозможность получения в полном объеме всей объективной информации, необходимой для успешного применения тех или иных математических моделей. Поэтому в такие модели неминуемо вносятся субъективные допущения и догадки их создателей, а эксперт должен иметь возможность конструировать собственные модели, создавая базы моделей и проигрывая на них воображаемые ситуации в интерактивном режиме.

Сложность формирования базы моделей для оценки состояния и прогнозирования уровня безопасности информации заключается в структуризации и формализации самого этого понятия. В терминах системного анализа оптимальный уровень безопасности информации может быть отождествлен с глобально не улучшаемым эффективным вариантом построения системы защиты информации, нацеленным на максимальное удовлетворение потребностей защиты при естественных бюджетных ограничениях, накладываемых на ресурсы. Точки в многомерном пространстве состояний системы, отвечающие критерию эффективности при такой постановке проблемы, можно формально выявить, решая задачу максимизации функции полезности системы защиты информации, которая определяется на множестве частных функций полезности отдельных ее подсистем. При этом формирование математических моделей отдельных подсистем обычно не представляет большого труда (эти вопросы подробно изложены в многочисленных работах по проблемам систем защиты информации, в том числе, в уже неоднократно упоминавшейся нами книге В.А. Герасименко [3]), тогда как установление связи между функциями полезности отдельных подсистем и системы в целом оказывается задачей не формаль-

ной. Речь здесь может идти лишь о некоторых гипотезах, на основе которых удается построить формальную модель такой связи. Одна из них приводит к функции полезности типа энтропии физической системы, которая применительно к данному классу задач будет рассмотрена в постановочном плане в следующем параграфе данного учебного пособия.

2.5. Моделирование процессов защиты информации

Из содержания предыдущих параграфов данной главы совершенно очевидно, что модели процессов защиты информации являются одним из основных элементов научно-методологического базиса защиты. Следует отметить, что, так как процессы защиты информации в значительной степени определяются случайными факторами, то применяемые для их анализа и прогнозирования модели неминуемо должны иметь стохастический характер.

На сегодняшний день проблема моделирования систем и процессов защиты информации нашла довольно серьезное отражение в ряде учебных и научных изданий. Наиболее системное изложение эта проблема получила, на наш взгляд, в монографии [3] и учебнике [31], к которым мы и отсылаем читателя, желающего познакомиться с ней более подробно.

Главным результатом анализа и системной классификации моделей, приведенной в [3, 31], является разработка обобщенной модели процессов защиты информации, осуществленная под руководством профессора В.А. Герасименко. Учитывая важнейшее значение этой модели для решения стратегических проблем защиты и формирования перспективных планов организации соответствующих работ, мы сочли необходимым включить ее описание и в состав данного учебного пособия.

В соответствии с упомянутым назначением рассматриваемой модели в ней отражаются те процессы, которые должны осуществляться в самой системе защиты. А поскольку центральным решением стратегического характера является оценка объема ресурсов, необходимых для обеспечения требуемого уровня защиты, и оптимальное их распределение, то в этой модели определяющими должны быть именно процессы распределения ресурсов. Основой для ее построения являются общие цели (задачи) защиты информации и условия, в которых осуществляется защита.

Цели защиты информации в самом общем виде могут быть сформулированы как построение оптимальных систем защиты ин-

формации и организация оптимального их функционирования. При этом понятие оптимальности интерпретируется в соответствии с общими постановками оптимизационных задач: при заданных ресурсах обеспечить достижение максимального результата или обеспечить достижение заданного результата при минимальном расходовании ресурсов. Таким образом, в любом случае речь идет о наиболее рациональном использовании ресурсов, выделяемых или необходимых для защиты информации.

Защищенность информации определяется некоторыми показателями, которые в свою очередь определяются параметрами системы и внешней среды. Всю совокупность параметров, определяющих значения показателей защищенности информации, в самом общем случае можно разделить на три вида: 1) управляемые параметры, т. е. такие, значения которых полностью формируются системой защиты информации; 2) параметры, недоступные для такого однозначного и прямого управления, как параметры первого вида, но на которые система защиты может оказывать некоторое воздействие; 3) параметры внешней среды, на которые система защиты информации никаким образом воздействовать не может.

Тогда модель процесса защиты информации в самом общем виде может быть представлена так, как показано на рис. 2.4, на котором приняты следующие обозначения: $\{K\}$ - множество показателей защищенности (уязвимости) информации; $\{P^{(c)}\}$ - множество параметров внешней среды, оказывающих влияние на функционирование системы; $\{R^{(c)}\}$ - множество ресурсов системы, участвующих в обработке защищаемой информации; $\{P^{(y)}\}$ - множество внутренних параметров системы, которыми можно управлять непосредственно в процессе обработки защищаемых данных; $\{P^{(e)}\}$ - множество внутренних параметров системы, не поддающихся непосредственному управлению, но поддающихся воздействию (например, в процессе реорганизации или совершенствования компонентов системы); $\{S^{(y)}\}$ и $\{R^{(y)}\}$ - множества средств и ресурсов текущего управления; $\{S^{(e)}\}$ и $\{R^{(e)}\}$ - множества средств и ресурсов воздействия; $\{R^{(o)}\}$ - множество общих ресурсов управления.

Тогда для решения задач анализа, т.е. для определения значений показателей защищенности (уязвимости) информации можно использовать следующее обобщенное выражение:

$$\{K\} = F_k [\{P^{(y)}\}, \{P^{(e)}\}, \{R^{(c)}\}, \{P^{(c)}\}], \quad (2.2)$$

Задачи синтеза в общем виде могут быть представлены следующим образом:



Рис. 2.4. Обобщенная модель процессов защиты информации

1) найти такие $\{R^{(y)}\}$ и $\{R^{(e)}\}$ ($\{R^{(y)}\} + \{R^{(e)}\} \leq \{\bar{R}^{(o)}\}$, $\{\bar{R}^{(o)}\}$ - заданные ресурсы), чтобы при заданных $\{P^{(c)}\}$ и $\{P^{(e)}\}$ выполнялось условие $\{K\} \rightarrow \max$;

2) выбрать такие $\{R^{(y)}\}$ и $\{R^{(e)}\}$, чтобы при заданных $\{R^{(c)}\}$ и $\{P^{(c)}\}$ условие $\{K\} \geq \{\bar{K}\}$ ($\{\bar{K}\}$ - заданный уровень защищенности) выполнялось при

$$\{R^{(o)}\} = \{R^{(y)}\} + \{R^{(e)}\} \rightarrow \text{т.п.}$$

Таким образом, задачи управления сводятся к оптимизации распределения $\{R^{(y)}\}, \{S^{(y)}\}, \{R^{(e)}\}, \{S^{(e)}\}$.

Нетрудно видеть, что возможны следующие модификации обобщенной модели:

1) блоки 1, 2 и 3 - модель функционирования системы при отсутствии управления защитой информации (такая модель позволяет лишь определять значения показателей защищенности информации, т. е. решать задачи анализа);

2) блоки 1, 2, 3, 4а и 5а - модель текущего управления защитой информации, основу которого составляет оптимизация использования средств защиты, непосредственно включенных в состав системы (такое управление может быть оперативно-диспетчерским и календарно-плановым);

3) блоки 1, 2, 3, 4а, 5а и 6а - модель управления ресурсами, выделенными на защиту информации, которая дополнительно к предыдущим задачам позволяет оптимизировать процесс формирования средств для текущего управления защитой информации;

4) блоки 1, 2, 3, 4б и 5б - модель управления средствами воздействия на параметры, не допускающие текущего управления, но поддающиеся воздействию;

5) блоки 1, 2, 3, 4б, 5б и 6б - модель управления ресурсами, выделенными на развитие системы;

5) все блоки - полная модель защиты, которая дополнительно ко всем возможностям, рассмотренным выше, позволяет оптимизировать использование всех ресурсов, выделенных на защиту информации.

Отметим, что приведенная модель в принципе позволяет решать все задачи моделирования систем и процессов защиты информации. Однако, чтобы воспользоваться этой обобщенной моделью, должны быть известны функциональные зависимости значений показателей защищенности от всех обозначенных на рис. 2.4 параметров и зависимость самих параметров от размеров ресурсов, вкладываемых в отображаемые ими процессы.

Так как на практике из-за отсутствия необходимых статистических данных не удается строго выполнить эти условия, то рассмотренная модель может применяться только в совокупности с неформальными методами анализа и прогнозирования, в частности, с использованием рассмотренного выше алгоритма автоформализации знаний эксперта-аналитика.

Рассмотрим еще один вариант построения модели системы защиты информации, который может оказаться весьма полезным при решении задачи оптимизации.

В предыдущем параграфе нами было отмечено, что для оценки функции полезности системы обеспечения безопасности информации может быть использован энтропийный подход.

Сформулируем описание системы обеспечения безопасности информации как системы с максимальной полезностью, под которой понимается наиболее полное использование ресурсов для целей защиты информации.

Пусть x_1, x_2, \dots, x_n - некоторые показатели, характеризующие деятельность отдельных подсистем системы обеспечения безопасности информации, достижение которых сопряжено с удельными затратами r_1, r_2, \dots, r_n , при этом суммарные затраты системы ограничиваются величиной соответствующего бюджета I . Для оценки обеспечиваемого при этом уровня безопасности информации необходимо максимизировать функцию полезности

$$u = u(x_1, x_2, \dots, x_n), \quad I), \quad (2.3)$$

соответствующую принятой концепции и структуре системы безопасности информации, при бюджетном ограничении

$$\sum_{i=1}^n x_i r_i = I. \quad (2.4)$$

Определим Лагранжиан L

$$L = u(x_1, x_2, \dots, x_n, I) + \lambda (I - \sum_i r_i x_i), \quad (2.5)$$

где λ - множитель Лагранжа, связанный с уравнением (2.4).

Проводя теперь обычным способом максимизацию, получаем, что значения параметров системы обеспечения безопасности информации определяются из решения системы уравнений

$$\frac{\partial L}{\partial x_i} = \lambda r_i . \quad (2.6)$$

Это решение может быть записано в виде

$$x_i = x_i (r_1, r_2, \dots, r_n, I) . \quad (2.7)$$

Можно показать также, что при заданном уровне полезности

$$\left. \frac{\partial I}{\partial r_i} \right|_{u=\bar{u}} = x_i . \quad (2.8)$$

Таким образом, уравнения (2.3) - (2.8) описывают систему обеспечения безопасности информации как систему с максимальной полезностью.

Покажем, что задача максимизации функций полезности такой системы может быть сведена к максимизации ее энтропии.

Вильсон А.Дж. [41] применил максимизацию энтропии при решении проблемы оптимизации транспортных потоков в городских системах. Он показал, что энтропия в этом случае связана с распределением вероятностей:

$$(2.9) \quad - \sum p_{ij} \ln p_{ij},$$

где $p_{ij} = T_{ij} / T^i$ может интерпретироваться как распределение вероятностей (T_{ij} - число поездок из зоны i в зону j , T - полное число поездок, которое является фиксированной величиной).

Рассмотрим возможность применения данного выражения для определения энтропии системы обеспечения безопасности информации как системы с максимальной полезностью. В этом случае необходимо решить проблему соизмерения значений частных функций полезности отдельных ее подсистем. Чтобы аналог выражения (2.9) интерпретировался как энтропия системы обеспечения безопасности информации, должны быть введены некоторые относительные единицы, связывающие количественные характеристики деятельности отдельных подсистем с подходящей фиксированной величиной. В качестве последней может быть использована величина бюджета I . Тогда такая относительная единица будет представлена в виде

$$y_i = \frac{x_i r_i}{I} . \quad (2.10)$$

Теперь система с максимальной полезностью может быть описана в терминах y_i следующим образом:

$$u = u\left(\frac{y_1 I}{r_1}, \frac{y_2 I}{r_2}, \dots, \frac{y_n I}{r_n}, I\right) \rightarrow \max, \quad (2.11)$$

$$\sum_{i=1}^n y_i = 1. \quad (2.12)$$

Функция Лагранжа имеет вид

$$L = u + \lambda \left(1 - \sum_i y_i\right). \quad (2.13)$$

Дифференцирование ее по y_i приводит к следующей системе уравнений:

$$\frac{du}{dy_i} = \lambda, \quad i = 1, 2, \dots, n, \quad (2.14)$$

откуда

$$y_i = y_i(r_1, r_2, \dots, r_n, I) \quad (2.15)$$

и

$$\left. \frac{dI}{dr_i} \right|_{U=\bar{U}} = \frac{y_i I}{r_i} \quad (2.16)$$

Легко проверяется, что уравнения (2.11) - (2.16) описывают ту же систему, что и уравнения (2.3) - (2.8).

Предположим теперь, что для анализа этой системы используется принцип максимизации энтропии

$$S = - \sum_{i=1}^n y_i \ln y_i \quad (2.17)$$

при известном ограничении (2.12).

Ограничения по другим видам ресурсов сформулируем следующим образом:

$$f_j(y_1, y_2, \dots, y_n) = g_j, \quad j = 1, 2, \dots, k, \quad (2.18)$$

где для удобства все члены, содержащие y_i , входят в f_i , а все остальные (константы) в g_i .

Функция Лагранжа в этом случае имеет вид

$$L = S + \lambda (1 - \sum_{i=1}^n y_i) + \sum_{j=1}^k \mu_j (g_j - f_j), \quad (2.19)$$

где λ и μ - множители Лагранжа, связанные соответственно с уравнениями (2.12) и (2.18).

Дифференцируя выражение (2.19) по y_i , получим систему уравнений, решая которую совместно с уравнениями (2.12) и (2.18), в итоге имеем

$$\ln y_i = -\lambda - \sum_{j=1}^k \mu_j \frac{df_j}{dy_i}. \quad (2.20)$$

Из анализа выражения (2.20) следует, что задача максимизации энтропии формально эквивалентна максимизации функции полезности, записанной в виде:

$$u = S + \sum_{j=1}^k \mu_j (g_j - f_j), \quad (2.21)$$

при ограничении (2.12) и очевидном условии, что параметры $\mu_j < 1$, а число ограничений k меньше числа переменных n .

Таким образом, и при максимизации энтропии, и при анализе системы с максимальной полезностью в конце концов будет получен один и тот же результат. Однако максимизация энтропии имеет принципиально важные для решения специфической задачи исследования состояний безопасности информации преимущества перед статистическим подходом, так как позволяет учитывать априорную информацию об отдельных ограничениях, накладываемых на y_i , а также делает возможной индивидуальную интерпретацию ограничений. Кроме того, этот подход оказывается полезным при построении динамических моделей.

Сформулируем теперь на основе рассмотренного энтропийного подхода соответствующую модель системы обеспечения безопасности информации. Пусть состояние x_i системы характеризуется некоторым ресурсом (эффектом) $f(x_i)$. Под состоянием x , будем понимать некоторый i -ый набор средств защиты информации. При этом справедливо ограничение

$$\sum_i p_i f(x_i) = E[f(x)] \leq U, \quad (2.22)$$

где p_i - вероятность состояния x_i ; U - лимит на ресурс, либо ограничение на полезный эффект.

Тогда задача поиска оптимального (с точки зрения максимизации уровня обеспечения безопасности информации) распределения величины x , формально записывается в виде:

$$S \rightarrow \max, \quad (2.23)$$

$$\sum_i p_i f(x_i) = U, \quad (2.24)$$

$$\sum_i p_i = 1, \quad (2.25)$$

где $S = - \sum_i p_i \ln p_i$ - энтропия системы.

Решение данной задачи методом неопределенных множителей Лагранжа имеет вид:

$$p_i = \exp[-\lambda - \mu f(x_i)], \quad (2.26)$$

где λ и μ - множители Лагранжа.

С учетом условия (2.25) получаем

$$e^\lambda = \sum_i \exp[-\mu f(x_i)] \quad (2.27)$$

При этом, искомое оптимальное распределение представляется в виде распределения Больцмана:

$$p_i = \frac{\exp[-\mu f(x_i)]}{\sum_i \exp[-\mu f(x_i)]} \quad (2.28)$$

Таким образом, макросостояние системы обеспечения безопасности информации задается функцией $f(x_i)$, имеющей в нашем случае смысл ресурса (эффекта), и некоторым параметром μ , аналогом температуры ($T=1/\mu$) в физических системах. Вводя так называемую статистическую сумму

$$Z = \sum_i \exp[-\mu f(x_i)], \quad (2.29)$$

а также величину $F = -(1/\mu) \ln Z$ - аналог свободной энергии в физических системах, получим, имея в виду известное соотношение Г. Гельмгольца для свободной и связанной энергии:

$$F = U - \frac{1}{\mu} S,$$

$$S = - \frac{dF}{d(1/\mu)},$$

$$U = F - \frac{1}{\mu} \frac{dF}{d(1/\mu)} = \frac{d}{d\mu} (\mu F) = - \frac{d(\ln Z)}{d\mu}. \quad (2.32)$$

К этим соотношениям добавляется условие монотонности возрастания U и S при положительном μ и $f(x_i) \neq \text{const}$.

Таким образом, макросостояние системы обеспечения безопасности информации можно задать четырьмя взаимосвязанными характеристиками U , F , μ и S . Их интерпретация зависит от постановки решаемой задачи, а также от особенностей конкретной исследуемой системы. В частности, F может интерпретироваться как суммарные прямые издержки системы на создание определенного

уровня обеспечения безопасности, а $\frac{1}{\mu} S$ - как косвенные затраты

на поддержание этого уровня.

Обобщение задачи поиска оптимального распределения на случай задания более одного вида ограничений на ресурсы формально записывается в виде:

$$S = - \sum_i p_i \ln p_i \rightarrow \max, \quad (2.33)$$

$$\sum_i p_i f_r(x_i) = E[f_r(x)], r = 1, 2, \dots, n, \quad (2.34)$$

$$\sum_i p_i = 1. \quad (2.35)$$

Аналогично (2.29) строится функция

$$Z(\mu_1, \mu_2, \dots, \mu_m) = \sum_i \exp \left[- \sum_{r=1}^m \mu_r f_r(x_i) \right]. \quad (2.36)$$

Тогда

$$p_i = \exp \left\{ - \sum_{r=1}^m [\lambda + \mu_r f_r(x_i)] \right\}, \quad (2.37)$$

где $\lambda = \ln Z$.

Остальные множители Лагранжа определяются из ограничений (2.34) и (2.35), записываемых в виде:

$$E[f_r(x)] = - \frac{d}{d\mu_r} \ln Z. \quad (2.38)$$

Можно вычислить максимальное значение энтропии:

$$S_{\max} = \lambda + \sum_{r=1}^m \mu_r E[f_r(x)] \quad (2.39)$$

и возможные флуктуации, рассчитывая дисперсию распределения

$$\Delta^2 f_r(x) = E[f_r(x)]^2 - \{E[f_r(x)]\}^2 = \frac{d^2}{d\mu_r^2} \ln Z. \quad (2.40)$$

Если задана зависимость f_r не только от x , но и от независимых параметров α_j ($j = 1, 2, \dots, L$), то можно оценить значение ее производных по максимуму энтропии

$$E \left(\frac{df_r}{d\alpha_j} \right) = \frac{d}{d\alpha} \ln Z. \quad (2.41)$$

Предположим, что функции ограничений $f_r(x)$ можно менять независимым образом для всех r и i . Допустим также независимое изменение средних значений f_r . Тогда

$$\delta\lambda = \delta \ln Z = - \sum_{r=1}^m \{\delta\mu_r E[f_r(x)] + \mu_r E[\delta f_r(x)]\}, \quad (2.42)$$

и, воспользовавшись (2.39), получим

$$\delta S = \sum_{r=1}^m \mu_r \{ \delta E[f_r(x)] - E[\delta f_r(x)] \} = \sum_{r=1}^m \mu_r \delta G_r, \quad (2.43)$$

где параметр G_r определяется соответствующим видом ограничений и является r -ым видом «теплоты», если пользоваться терминологией термодинамики, соотношения которой мы и положили в основу всех наших рассуждений. Таким образом, μ_r - весовой коэффициент при G_r , является, следовательно, r -тым видом «температуры».

Из уравнения (2.43) легко может быть получен его частный случай

$$dS = \mu dE[f(x)] + \mu \sum_k \bar{x}_k dx_k, \quad (2.44)$$

где \bar{x}_k - среднее значение обобщенной силы, действующей на внешнюю координату x_k .

Это выражение является аналогом второго закона термодинамики и описывает процесс релаксации системы обеспечения безопасности информации в равновесное состояние, определяющее ее потенциальные возможности.

Для практического применения предложенных энтропийных методов моделирования необходимо увязать макропараметры системы U, F, μ, S с конкретными характеристиками отдельных ее подсистем и элементов, что может выполнить эксперт-аналитик.

2.6. Основное содержание теории защиты информации

Изложенная нами выше постановка задачи защиты информации, сформированная на основе анализа современных концепций информационного обеспечения деятельности в различных сферах и ретроспективного анализа развития подходов к защите, представляет собой как бы концентрированное выражение объективных потребностей в защите. Рассмотренные в § 2.2 - 2.5 принципы, методы и модели являются суммой научно-методологических предпосылок, на основе которых могут быть построены системы для удовлетворения этих потребностей. Далее с учетом этого могут быть сформулированы и научно обоснованы проблемы, составляющие основное содержание теории защиты информации. В их числе:

- 1) принципиальные подходы к защите информации;
- 2) методы и средства, необходимые для эффективного решения всего комплекса задач защиты;
- 3) методы организации и обеспечения функционирования создаваемых механизмов защиты;

4) условия, соблюдение которых необходимо или желательно для эффективного решения задач защиты;

5) перспективы развития подходов, методов и средств защиты.

К настоящему времени содержание основ теории защиты сводится к следующему:

в целях четкого обоснования принципиальных подходов к защите введено понятие стратегии защиты;

в целях создания единого инструментально-методологического базиса, обеспечивающего решение на регулярной основе названных выше в пп. 2, 3 и 4 проблем, разработана так называемая унифицированная концепция защиты информации;

в целях создания предпосылок целенаправленного развития концепции защиты исследованы перспективные (необходимые и возможные) способы, методы и средства решения проблем защиты.

Рассмотрим более подробно сущность перечисленных частей теории защиты.

Стратегии защиты информации. Обобщая определения, приводимые в различных источниках, можно сказать, что стратегия - это общая, рассчитанная на перспективу руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов.

Таким образом, стратегическая установка на защиту информации, очевидно, может быть сформулирована следующим образом: вся совокупность мероприятий по защите информации должна быть такой, чтобы во все время функционирования системы уровень защиты соответствовал требуемому, а выделяемые для этих целей ресурсы расходовались бы наиболее рациональным способом.

Однако, современная практика показывает, что в различных ситуациях требования к защите и условия защиты могут существенно отличаться, поэтому, очевидно, одной стратегической установкой не удастся охватить и содержательно выразить общую направленность защиты для всех систем и всех возможных условий их функционирования. Отсюда следует, что для системного решения всей совокупности вопросов защиты во всем множестве потенциально возможных условий необходимы несколько различных стратегий защиты, каждая из которых соответствовала бы некоторой подобласти общей области условий. А отсюда, в свою очередь, следует, что основой для формирования множества возможных стратегий должны служить результаты системного анализа потенциально

возможных условий, в которых будет или может осуществляться защита информации.

Организация защиты информации в самом общем виде может быть определена как поиск оптимального компромисса между потребностями в защите и необходимыми для этих целей ресурсами.

Потребности в защите обусловливаются прежде всего важностью и объемами защищаемой информации, а также условиями ее хранения, обработки и использования. Эти условия определяются уровнем (качеством) структурно-организационного построения защищаемой системы или объекта, уровнем организации технологических схем обработки информации, местом и условиями расположения компонентов системы, а также некоторыми другими параметрами.

Размер ресурсов на защиту информации может быть ограничен определенным пределом, либо определяться условием обязательного достижения требуемого уровня защиты. В первом случае защита должна быть организована так, чтобы при выделенных ресурсах обеспечивался максимально возможный уровень защиты, а во втором так, чтобы требуемый уровень защиты обеспечивался при минимальном расходовании ресурсов. О подобной постановке задач речь уже шла выше в § 2.5.

Нетрудно видеть, что сформулированные задачи есть не что иное как прямая и обратная постановки оптимизационных задач, которые достаточно детально изучены в современной теории систем, информатике и прикладной математике. Поэтому, если бы были четко определены функциональные зависимости между объемом затрачиваемых ресурсов и достигаемым уровнем защиты, то каждая из сформулированных выше задач могла бы быть строго решена известными методами в каждом конкретном случае. Однако, указанные выше функциональные зависимости и в настоящее время, и в обозримом будущем могут быть получены с какой-то степенью достоверности только с использованием технологии автоформализации знаний (см. § 2.4). Основная причина этого обстоятельства заключается в том, что процессы защиты информации сильно зависят от большого числа случайных и даже трудно предсказуемых факторов, а среди средств защиты весьма заметное (если не определяющее) место занимают организационные меры и нормативно-правовые акты. Более того, сам процесс защиты с точки зрения классической теории систем выглядит не совсем определенным: например, уровень защищенности информации может быть повышен не только использованием специальных

средств защиты, но более четким построением защищаемой системы, упорядочением технологических схем обработки информации и т. п. В целях создания условий для ориентации в таких неопределенных ситуациях и введено понятие стратегии защиты, причем под стратегией понимается общий взгляд на сложившуюся ситуацию и общий подход к принятию наиболее рационального решения в этой ситуации. При этом количество различных стратегий должно быть небольшим (в противном случае будет трудно ориентироваться в самих стратегиях), но в то же время оно должно достаточно полно и адекватно отображать всю гамму потенциально возможных ситуаций.

В целях обоснования числа и содержания необходимых стратегий используем два критерия - требуемый уровень защиты и степень свободы действий при организации защиты.

Значения первого критерия лучше всего было бы выразить количественно, например, в виде вероятности надежной защиты информации. Но поскольку, как уже отмечалось выше, это не представляется возможным, то выразим его множеством тех угроз, относительно которых должна быть обеспечена защита, причем выберем следующие значения:

- 1) защита от уже известных (ранее проявлявшихся) угроз;
- 2) защита от наиболее опасных потенциально возможных угроз;
- 3) защита от всех потенциально возможных угроз.

Для защиты от известных угроз, очевидно, необходимо организовать регулярный сбор и обработку данных о проявлениях угроз и их последствиях и иметь арсенал проверенных средств эффективнойнейтрализации каждой из угроз.

Защита от всех потенциально возможных угроз возможна только в случае знания всего их множества. Формирование этого множества представляет собою достаточно сложную научно-техническую и организационную проблему. Один из наиболее разработанных к настоящему времени подходов к ее решению достаточно детально рассмотрен в [3].

Общая интерпретация второго критерия (степени свободы действий при организации защиты) сводится к тому, что организаторы и исполнители процессов защиты имеют относительно полную свободу распоряжаться методами и средствами защиты и некоторую степень свободы вмешательства в архитектурное построение защищаемой системы или объекта, а также в организацию и обеспечение технологии их функционирования. По этому последнему аспекту удобно выделить три различных степени свободы следующего содержания:

- 1) никакое вмешательство в систему не допускается;
- 2) к архитектурному построению системы и технологии ее функционирования допускается предъявлять требования неконцептуального характера;
- 3) требования любого уровня, обусловливаемые потребностями защиты информации, принимаются в качестве обязательных условий при построении системы, организации и обеспечении ее функционирования.

Если суммировать сказанное выше, то декартово произведение трех значений каждого из двух критериев дает в общем случае девять различных стратегических подходов к защите информации. Однако совершенно очевидно, что при защите от известных угроз вряд ли будет целесообразным вмешательство в систему на концептуальном уровне, а защита от всех потенциально возможных угроз может быть достигнута лишь при создании изначально защищенной информационной среды, что не может быть достигнуто без вмешательства в архитектуру системы и технологию ее функционирования.

На основе анализа всех девяти стратегических подходов могут быть выделены три основных стратегии защиты: оборонительная, наступательная и упреждающая. Их содержание может быть представлено так, как показано на рис. 2.5.

Анализ сущности условий, способствующих эффективной реализации различных стратегий защиты (см., например, [3], кн. 2, с. 39-77), приводит к следующему выводу: кардинальное повышение эффективности защиты информации (равно как и эффективности обеспечения качества информации и информационной безопасности) не может быть достигнуто в рамках существующих концепций автоматизированной обработки информации. Необходимы принципиально иные концепции, построение которых требует существенного видоизменения постановки задачи развития и использования вычислительной техники, а также в целом взглядов на процесс совершенствования информационного обеспечения различных сфер деятельности.

В рамках современной информатики, рассматриваемой как фундаментальное научное направление, основные цели которого заключаются в изучении информационных проблем современного общества и разработке способов, методов и средств наиболее рационального их удовлетворения, получены такие результаты, которые создают объективные предпосылки построения названных концепций.

Глава 2

		Способ реализации стратегии		
		Отдельные механизмы защиты	Системы защиты	Защищенные информационные технологии
Учитываемые угрозы	Все потенциально возможные			УПРЕЖДАЮЩАЯ
	Наиболее опасные потенциально возможные		НАСТУПАТЕЛЬНАЯ	
	Все известные	ОБОРОНИТЕЛЬНАЯ		
		Отсутствует	Частичное	Полное
Влияние на среду защиты				

Рис. 2.5. Стратегии защиты информации

Сформулируем кратко основные из этих результатов.

1. Процессы, осуществляемые в каждой сфере деятельности, могут быть представлены в виде строго определенной совокупности функций.

2. Содержание и последовательность осуществления каждой из функций могут быть представлены в виде четко сформулированной концепции.

3. Информационные процессы, имеющие место в любой сфере деятельности, могут быть представлены некоторой совокупностью процедур (задач) трех классов: информационно-поисковых, логико-аналитических, поисково-оптимизационных. Небезынтересно отметить, что в такой классификации содержится глубинный смысл, так как при решении информационно-поисковых задач обработка ин-

формации осуществляется преимущественно на синтаксическом, логико-аналитических - на семантическом, поисково-оптимизационных - на прагматическом уровнях.

4. Для решения задач каждого из названных выше унифицированных классов может быть разработан полный арсенал методов и средств, причем полнота интерпретируется здесь в том смысле, что любая задача в любых потенциально возможных условиях может быть решена рациональным образом.

5. Информационный поток, циркулирующий в любой системе или на любом объекте в процессе их функционирования, может быть представлен как частный случай некоторой унифицированной схемы.

Перечисленные результаты создают объективные предпосылки для построения унифицированной технологии автоматизированной обработки информации (УТАОИ). Впервые эта задача была поставлена профессором В.А.Герасименко в монографии [5]. В его интерпретации УТАОИ представляется как высокоорганизованный конвейер автоматизированной обработки информации, построенный применительно к унифицированной структуре информационного потока и с оптимальным использованием методов и средств решения задач унифицированных классов.

Один из принципов построения такой унифицированной технологии заключается в максимальном использовании задач унифицированных классов и стандартных средств их решения. Это создает возможности постепенной стандартизации все больших фрагментов технологических участков обработки информации. По мере решения этой задачи создаются все более полные предпосылки для построения эталонной информационной технологии, в которой не только наилучшим образом реализуются потенциальные возможности УТАОИ, но все основные реквизиты которой могут быть сертифицированы по всей совокупности существенно значимых показателей. Нет необходимости доказывать, какими широкими возможностями обладает эталонная технология в плане совершенствования информационного обеспечения деятельности и экономии расходуемых на эти цели средств. Само собой разумеется, что эталонная технология может быть сертифицирована также по показателям защищенности информации, причем может быть предусмотрено несколько версий технологии по уровню защищенности информации.

Далее, естественно предположить, что по мере совершенствования эталонной информационной технологии ее основные компо-

ненты (и прежде всего программные) будут совершенствоваться до такой степени, что смогут удовлетворять всем требованиям стандартных решений. А поскольку они к тому же по самой постановке задачи будут в высокой степени унифицированными, то создаются все необходимые предпосылки для аппаратной реализации процедур обработки информации, чем и определяются возможности создания защищенной информационной среды.

Унифицированная концепция защиты информации. Унифицированной концепцией защиты информации, уже упоминавшейся в гл. 1, будем называть инструментально-методологическую базу, обеспечивающую практическую реализацию каждой из рассмотренных выше стратегий защиты (оборонительной, наступательной, упреждающей), причем реализацию оптимальным образом, на регулярной основе и при минимальных затратах.

Структура УКЗИ приводилась на рис. 1.3. Ниже дается общее содержание выделенных на рисунке компонентов концепции.

1. Концепции, задающие ситуацию защиты. В настоящее время довольно четко обозначается тенденция формирования объективных предпосылок для оптимального информационного обеспечения деятельности систем и объектов на регулярной основе. Представляется, что основными путями решения данной задачи являются формирование на каждом объекте информационного кадастра, построение унифицированной технологии автоматизированной обработки информации и разработка методологии организации информационного обеспечения деятельности объектов. Итогом реализации этой методологии будет система решения основных задач объекта, связанных с использованием информации, на принципах и методах поточно-индустриального производства.

2. Методология описания ситуации защиты. В классической теории систем под описанием любой ситуации подразумеваются строго формальные представления архитектуры и процессов функционирования соответствующей системы. К этому необходимо стремиться и при описании ситуаций защиты. Однако, как уже отмечалось, одна из наиболее характерных особенностей ситуаций, возникающих в процессе решения задач защиты, заключается в повышенном влиянии случайных факторов. Это обстоятельство существенно затрудняет формальное их описание. В качестве выхода из положения понятие формализации в методологии системного анализа расширяется до уровня структуризации, причем под структуризацией ситуации понимается представление структуры в виде совокупности взаимодействующих элементов, а при опреде-

лении характеристик элементов и систем в целом, а также процессов их функционирования наряду с количественными допускается использование лингвистических переменных.

3. Система показателей уязвимости (защищенности) информации. Под показателем уязвимости информации понимается мера потенциально возможного негативного воздействия на защищаемую информацию. Величина, дополняющая меру уязвимости до максимально возможного значения представляет собой меру защищенности информации. Поскольку современные системы и объекты, а также технологические схемы их функционирования могут быть чрезвычайно сложными, то не удается одним каким-либо показателем удовлетворить потребности решения всех задач защиты, необходимо некоторое (как оказалось, достаточно большое) число таких показателей. Однако при независимом их формировании и использовании неизбежна путаница и другие неудобства. Чтобы избежать этого, все показатели должны быть объединены в некоторую упорядоченную систему.

4. Система дестабилизирующих факторов, влияющих на уязвимость (защищенность) информации. Под дестабилизирующим фактором понимается событие или явление, содержащее в себе потенциальную возможность такого негативного воздействия на информацию, результатом которого может быть увеличение значений каких-либо показателей уязвимости защищаемой информации и соответственно уменьшение показателей ее защищенности. Как и в случае показателей уязвимости (защищенности) информации, речь идет о формировании упорядоченной и полной системы дестабилизирующих факторов, т.е. угроз информации, что предопределяется потребностями решения задач защиты. В самом деле, если для реализации оборонительной стратегии защиты достаточно иметь сведения об уже известных угрозах, то для наступательной стратегии необходимы сведения и о наиболее опасных угрозах, которые пока не проявились, но являются потенциально возможными. Для реализации же упреждающей стратегии дополнительно к предыдущему необходимы сведения обо всех потенциально возможных угрозах информации. Совершенно очевидно, что формирование полной в указанном выше смысле системы угроз представляет собою весьма сложную и неординарную задачу.

5. Методология оценки уязвимости (защищенности) информации. В соответствии с изложенным выше, данная методология должна содержать методы, модели и инструментальные средства определения текущих и прогнозирования будущих значе-

ний каждого из системы показателей уязвимости (защищенности) информации под воздействием каждой из потенциально возможных угроз и любой их совокупности. С точки зрения классической теории систем подобные задачи выделены в класс задач анализа, и для их решения разработан весьма представительный арсенал методов, рассчитанных как на системы детерминированного, так и стохастического характера. Однако в силу очень высокого влияния на процессы защиты информации случайных факторов, для многих из которых к тому же неизвестны (по крайней мере в настоящее время) законы распределения и числовые их характеристики, указанные методы лишь частично могут быть использованы для решения рассматриваемых задач. Для системного их решения необходимы методы, существенно выходящие за рамки классической теории систем.

6. Методология определения требований к защите информации. Данный компонент унифицированной концепции защиты информации в решающей степени предопределяет подходы, средства и методы практической организации защиты. В классической теории систем предполагается, что требования к любым параметрам создаваемых систем определяются в количественном выражении. Однако, в силу повышенной неопределенности процессов защиты информации, предложить строго формальную и адекватную методику определения требуемого уровня защиты не удается (по крайней мере в настоящее время). Таким образом, приходится довольствоваться эвристическими и теоретико-эмпирическими методами. А поскольку требованиями к защите фактически предопределяется построение соответствующей системы защиты и технология ее функционирования, то решать рассматриваемую задачу оказалось целесообразным во взаимосвязи с задачей оптимизации и стандартизации систем защиты информации.

7. Система концептуальных решений по защите информации. Под концептуальным понимается такое решение, которое создает объективные предпосылки для формирования инструментальных средств, необходимых и достаточных для эффективного решения всей совокупности соответствующих задач на регулярной основе и в соответствии с требованиями, которые, в свою очередь, определяются целями функционирования соответствующей системы. Отсюда следует, что концептуальные решения должны быть научно обоснованными и оптимальными с точки зрения сочетания объективных требований к решению соответствующих задач и

объективных предпосылок их решения. А отсюда, в свою очередь, следует, что должны быть механизмы оценки оптимальности решения задач на основе концептуальных решений. Приведенные положения целиком и полностью относятся также к принятию концептуальных решений по защите информации. Как следует из рис. 1.3, указанные концептуальные решения сводятся к формированию взаимосвязанной цепочки: функции защиты - задачи защиты - средства защиты - система защиты.

Из теории управления известно, что принятие такого рода решений относится к числу слабоструктуризованных задач, реализация которых в значительной мере основывается на эвристических методах. Особенno важна доля эвристической составляющей в методиках принятия решений в условиях существенной неопределенности, что и имеет место при организации защиты информации.

8. Система требований к концептуальным решениям. Содержание данного компонента концепции защиты заключается в обосновании таких требований к каждому из концептуальных решений, которые обеспечивали бы достижение целей их принятия наиболее рациональным образом.

9. Условия, способствующие повышению эффективности защиты информации. Основное назначение и содержание данного компонента концепции защиты информации заключается в том, чтобы сформировать и обосновать перечень и содержание тех условий, соблюдение которых будет существенно способствовать повышению уровня защиты при ограничении объема выделенных для этих целей средств или расходованию возможно меньшего объема средств для обеспечения требуемого уровня защиты. Иными словами, указанная система условий выступает в качестве обратной связи от концептуальных решений по защите информации к ситуации, порождающей саму проблему защиты, т. е. к первому компоненту рассматриваемой здесь концепции защиты.

Отсюда следует, что унифицированная концепция защиты представляет собою кибернетическую систему с обратной связью, что и создает объективные предпосылки для оптимального решения задач защиты.

Перспективы и проблемы развития теории и практики защиты информации. Прогноз перспектив развития теории и практики защиты информации создает базу для упреждающей разработки перспективных методов и средств защиты. В то же время прогнозирование любых процессов относится к числу наиболее сложных задач, требующих достаточно репрезентативной выборки

статистических данных о развитии и функционировании различных систем защиты информации.

Сбор таких данных пока что организован неудовлетворительно, что существенно усложняет прогнозирование перспектив развития теории и практики защиты информации. Уместным будет также отметить, что даже в рамках классической теории систем, изучающей формальные системы, прогнозирование представляется весьма сложной задачей.

Таким образом, с учетом всего изложенного можно сделать вывод, что наиболее подходящей исходной платформой для решения задачи интенсификации процессов защиты информации может быть предложенная в работах В.А. Герасименко унифицированная концепция, поскольку именно в ней наиболее полно сконцентрирован и систематизирован весь опыт развития теории и практики защиты.

Краткие выводы

1. Переход от экстенсивных к интенсивным способам защиты информации требует формирования научно-методологического базиса, представляющего собой теорию защиты информации.

В основу формирования теории защиты информации положены фундаментальные общеметодологические принципы, такие как четкая целевая направленность исследований и разработок, неукоснительное следование главной задаче науки - за внешними проявлениями вскрыть внутренние движения, упреждающая разработка общих концепций, формирование концепций на основе реальных фактов, учет всех существенно значимых факторов, влияющих на изучаемую проблему, строгий учет диалектики взаимосвязей количественных и качественных изменений в развитии изучаемых явлений, своевременное видоизменение постановки задачи.

Данные принципы носят общетеоретический характер. Что касается самого процесса изучения сложных проблем защиты информации и практической реализации результатов этого изучения, то основой здесь могут явиться следующие четыре принципа: построение адекватных моделей изучаемых систем и процессов, унификация разрабатываемых решений, максимальная структуризация изучаемых систем и разрабатываемых решений, радикальная эволюция (принцип В.М. Глушкова) в реализации разработанных концепций.

2. Так как процессы защиты информации подвержены сильному влиянию случайных факторов, методы классической теории систем оказываются практически непригодными для решения задач создания, организации и обеспечения функционирования систем защиты информации. В связи с этим возникает актуальная задача расширения арсенала классической теории за счет использования методов, позволяющих адекватно моделировать процессы, существенно зависящие от воздействия труднопредсказуемых факторов. Наиболее подходящими для формирования методологического базиса теории защиты информации оказываются методы нечетких множеств, лингвистических переменных (нестрогой математики), неформального оценивания, неформального поиска оптимальных решений.

Исследование особенностей названных методов применительно к задачам интенсификации процессов защиты информации, а также практически полное отсутствие на сегодняшний день систематизированных статистических данных функционирования реальных систем защиты, выдвигают на передний план эвристическую составляющую методологического базиса теории защиты информации. Отсюда исключительно важное значение для решения проблем обеспечения информационной безопасности приобретают методы экспертных оценок, эвристического программирования, «мозгового штурма» и психоинтеллектуальной генерации, интегрированные в технологию автоформализации профессиональных знаний.

3. Принципиальным моментом практической реализации теоретико-прикладных принципов теории защиты информации является построение адекватных моделей изучаемых систем и процессов. Целенаправленное решение этой проблемы базируется на обобщенной модели, состоящей из блоков, различные комбинации которых позволяют определять значения показателей защищенности информации, оптимизировать использование средств защиты, управлять ресурсами, выделенными на защиту информации и, наконец, оптимизировать использование всех ресурсов, участвующих в решении проблемы защиты информации.

4. Основными результатами развития теории защиты информации являются введение понятия стратегий защиты и создание единого инструментально-методологического базиса их реализации - унифицированной концепции защиты информации.

С учетом требуемого уровня защиты и степени свободы действий при ее организации целесообразно выделить три вида базовых

Глава 2

стратегий защиты информации: оборонительную, наступательную и упреждающую. Каждая из этих стратегий может быть оптимальным образом реализована в рамках унифицированной концепции защиты информации, представляющей собой взаимосвязанную цепочку: функции защиты - задачи защиты - средства защиты - система защиты.

В унифицированной концепции защиты информации наиболее полно сконцентрирован и систематизирован накопленный на сегодняшний день опыт развития теории и практики защиты информации. Вследствие этого данная концепция является собой наиболее подходящую исходную платформу для дальнейшего развития теории защиты информации и решения проблемы перехода от экстенсивных к интенсивным способам ее организации.

Глава третья

УГРОЗЫ И ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИИ

3.1. Понятие угрозы безопасности информации. Ретроспективный анализ подходов к формированию множества угроз

Под угрозой безопасности информации будем понимать возникновение такого явления или события, следствием которого могут быть негативные воздействия на информацию: нарушение физической целостности, логической структуры, несанкционированная модификация, несанкционированное получение, несанкционированное размножение.

К настоящему времени специалистами фиксируется очень большое количество разноплановых угроз различного происхождения. На протяжении всего периода существования проблемы защиты информации предпринимались попытки классифицировать источники угроз безопасности информации и сами угрозы с целью дальнейшей стандартизации средств и методов, применяемых для защиты. Различными авторами предлагается целый ряд подходов к такой классификации [3, 7, 13, 14, 21, 42, 43, 44]. При этом в качестве критерии деления множества угроз на классы используются виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Рассмотрим эти подходы более подробно.

В достаточно известной монографии Л. Дж. Хоффмана «Современные методы защиты информации» [7] были выделены 5 групп различных угроз: хищение носителей, запоминание или копирование информации, несанкционированное подключение к аппаратуре, несанкционированный доступ к ресурсам системы, перехват побочных излучений и наводок.

В книге «Защита информации в персональных ЭВМ» [13] предпринята попытка классификации угроз, причем в качестве критерия классификации выбран тип средства, с помощью которого может быть осуществлено несанкционированное получение информации. Авторами было выделено три типа средств: человек, аппаратура и программа. К группе угроз, в реализации которых основную роль

играет человек, отнесены хищение носителей, чтение информации с экрана дисплея, чтение информации с распечаток; к группе, где основным средством выступает аппаратура, - подключение к устройствам и перехват излучений; к группе, где основным средством является программа, - несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Аналогичный подход предлагается и группой авторов учебных пособий по защите информации от несанкционированного доступа [21, 42]. Ими выделены три класса: природные (стихийные бедствия, магнитные бури, радиоактивное излучение); технические (отключение или колебания электропитания, отказы и сбои аппаратно-программных средств, электромагнитные излучения и наводки, утечки через каналы связи); созданные людьми (непреднамеренные и преднамеренные действия различных категорий лиц).

В руководящем документе Гостехкомиссии России [43] введено понятие модели нарушителя в автоматизированной системе обработки данных, причем в качестве нарушителя здесь рассматривается субъект, имеющий доступ к работе со штатными средствами системы. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами. В документе выделяются четыре уровня этих возможностей:

- 1) самый низкий - возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;
- 2) первый промежуточный - дополнительно к предыдущему предусматривает возможности создания и запуска собственных программ с новыми функциями обработки информации;
- 3) второй промежуточный - дополнительно к предыдущему предполагает возможности управления функционированием системы, т.е. воздействия на базовое программное обеспечение и на состав и конфигурацию ее оборудования;

- 4) самый высокий - определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав системы собственных технических средств с новыми функциями обработки информации.

Предполагается, что нарушитель на своем уровне является специалистом высшей квалификации, знает все о системе, в том числе и о средствах защиты.

Еще один вид источников угроз безопасности информации, связанный с ее хищением, достаточно подробно классифицирован в монографии С.П. Расторгуева «Программные методы защиты информации в компьютерах и сетях» [14]. Автор выделяет четыре способа хищения информации:

1) по каналам побочных электромагнитных излучений;

2) посредством негласного копирования, причем выделено две разновидности копирования: «ручное» (печать с экрана на принтер или вывод из памяти на принтер или экран) и «вирусное» (например, вывод из памяти на принтер, на экран или передача информации с помощью встроенной в компьютер радиозакладки);

3) хищение носителей информации;

4) хищение персонального компьютера.

В монографии В.А. Герасименко [3] введены понятия дестабилизирующих факторов, источников их проявления и причин нарушения защищенности информации. Предложены подходы к формированию относительно полных множеств указанных причин и приведена структура этих множеств применительно к нарушению физической целостности информации и несанкционированному ее получению.

Достаточно детальный анализ угроз несанкционированного получения информации проведен также в учебном пособии В.Ю. Гайковича и Д.В. Ершова [44], причем концептуальные подходы анализа перекликаются с подходами, изложенными в [3].

Своеобразный вид угроз представляют специальные программы, скрытно и преднамеренно внедряемые в различные функциональные программные системы, которые после одного или нескольких запусков разрушают хранящуюся в них информацию и/или совершают другие недозволенные действия. К настоящему времени известно несколько разновидностей таких программ: электронные вирусы, компьютерные черви, троянские кони и др.

Вредоносные программы представляют достаточно большую опасность для современных автоматизированных систем. Детальный анализ этих угроз и методов борьбы с ними приведен в учебном пособии Б.И. Скородумова [45] и др.

Нетрудно видеть, что в процессе формирования множества угроз достаточно четко проявилась тенденция перехода от эмпирических подходов к системно-концептуальным, научно обоснованным подходам. В этой связи интересной представляется классификация угроз безопасности информации по способам их возможного негативного

воздействия. Такая классификация предусматривает подразделение угроз на информационные, программно-математические, физические и организационные.

Информационные угрозы реализуются в виде:

нарушения адресности и своевременности информационного обмена, противозаконного сбора и использования информации;

осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

хищения информационных ресурсов из банков и баз данных;

нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

разработки и распространения программ, нарушающих нормальное функционирование информационных систем или систем защиты информации.

Физические угрозы реализуются в виде:

уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

хищения программных или аппаратных ключей и средств криптографической защиты информации;

перехвата информации в технических каналах связи и телекоммуникационных системах;

внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы реализуются в виде:

невыполнения требований законодательства в информационной сфере;

противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи,

3.2. Системная классификация угроз безопасности информации

Из предыдущего изложения следует, что на сегодняшний день предложен целый ряд подходов к классификации угроз безопасности информации. При этом в качестве критерии деления множества угроз на классы авторы этих подходов используют виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Все многообразие предлагаемых классификаций с помощью подходов, предложенных В А Герасименко [3], на основе методов системного анализа может быть сведено к некоторой системной классификации, приведенной в табл. 3.1.

Дадим краткий комментарий к использованным в этой таблице параметрам классификации, их значениям и содержанию.

Виды угроз. Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

Таблица 3.1

Системная классификация угроз информации

Параметры классификации	Значения параметров	Содержание значения
1. Виды угроз	1.1. Нарушение физической целостности 1.2. Нарушение логической структуры 1.3. Нарушение содержания 1.4. Нарушение конфиденциальности 1.5. Нарушение права собственности	Уничтожение (искажение) Искажения структуры Несанкционированная модификация Несанкционированное получение Присвоение чужого права
2. Природа происхождения	2.1. Случайные 2.2. Преднамеренная	Отказы Сбои Ошибки Стихийные бедствия Побочные влияния Злоумышленные действия людей

Глава 3

Параметры классификации	Значения параметров	Содержание значения
3. Предпосылки появления угроз	3.1. Объективные 3.2. Субъективные	Количественная недостаточность элементов системы Количественная недостаточность элементов системы Разведорганы иностранных государств Промышленный шпионаж Уголовные элементы Недобросовестные сотрудники
4. Источники угроз	4.1. Люди 4.2. Технические устройства 4.3. Модели, алгоритмы, программы Технологические схемы обработки 4.5. Внешняя среда	Посторонние лица Пользователи Персонал Регистрации Передачи Хранения Переработки Выдачи Общего назначения Прикладные Вспомогательные Ручные Интерактивные Внутримашинные Сетевые Состояние атмосферы Побочные шумы Побочные сигналы

Содержание значений этого параметра определяется уровнем, на котором происходит негативное воздействие на информацию. Оно может иметь место на синтаксическом, семантическом **или** pragmatическом уровне.

2. Происхождение угроз. В табл. 3.1 выделено два значения данного параметра: случайное и преднамеренное. При этом под случайным понимается такое происхождение угроз, которое обу-

словливаются спонтанными и не зависящими от воли людей обстоятельствами. Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния. Сущность перечисленных событий (кроме стихийных бедствий, сущность которых ясна) определяется следующим образом:

а) отказ - нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих основных функций;

б) сбой - временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

в) ошибка - неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

г) побочное влияние - негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обусловливается злумышленными действиями людей.

3. Предпосылки появления угроз. В табл. 3.1 выделены две разновидности предпосылок: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, преднамеренные или непреднамеренные действия недобросовестных сотрудников). Перечисленные разновидности предпосылок интерпретируются следующим образом:

а) количественная недостаточность - физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки информации или/и перегрузку имеющихся элементов;

б) качественная недостаточность - несовершенство организации системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

в) деятельность разведорганов иностранных государств - специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами. К основ-

ным видам разведки относятся агентурная (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых доброжелателей) и техническая, включающая радиоразведку (перехват радиосредствами информации, циркулирующей в радиоканалах систем связи), радиотехническую (регистрацию спецсредствами сигналов, излучаемых техническими системами) и космическую (использование космических кораблей и искусственных спутников для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации другими доступными способами);

г) промышленный шпионаж - негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной утечки или хищения, а также по созданию для себя благоприятных условий в целях получения максимальных выгод (недобросовестная конкуренция);

д) злоумышленные действия уголовных элементов - хищение информации или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

е) действия недобросовестных сотрудников - хищение (копирование) или уничтожение информационных массивов или/и программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленных правил работы.

4. Источники угроз. Под источником угроз понимается непосредственный исполнитель угрозы в плане негативного воздействия на информацию.

Нетрудно видеть, что источники угроз и формы их проявления предопределяют возможности формирования множества причин нарушения защищенности информации по каждому из аспектов защиты, что количественно может быть охарактеризовано показателями уязвимости информации.

3.3. Методы оценки уязвимости информации

При решении практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости. Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры ее уязвимости наиболее целесообразно принять вероятность нарушения защищенности (изменения важнейших характеристик), а также потенциально возможные размеры ущерба, наносимого таким нарушением.

При этом основными параметрами, влияющими на вероятность нарушения защищенности информации, являются: количество и типы структурных компонентов системы или объекта, количество и типы случайных угроз, которые потенциально могут проявиться в рассматриваемый период времени, количество и типы преднамеренных угроз, которые могут иметь место в тот же период, число и категории лиц, которые потенциально могут быть нарушителями установленных правил обработки информации, и, наконец, виды защищаемой информации. Характер такого влияния достаточно сложен, в связи с чем структуризация и оценка вероятности нарушения защищенности превращаются в неформальную задачу, которая может решаться на основе методологического базиса, изложенного в предыдущей главе данного учебного пособия.

Различные подходы к структуризации показателей защищенности информации через формирование полного множества возможных КНПИ подробно изложены в учебнике [31]. Здесь же мы остановимся только на оценке уязвимости информации, связанной с действиями злоумышленников, так как в этой задаче наиболее выпукло проявляется многорубежный характер реализации политики защиты и лишний раз концентрируется внимание на комплексном характере проблемы.

Известно, что несанкционированное получение информации возможно не только путем непосредственного доступа к базам данных, но и многими другими путями, не требующими такого доступа. При этом основную опасность представляют преднамеренные действия злоумышленников. Воздействие случайных факторов само по себе не ведет к несанкционированному получению информации, оно лишь способствует появлению КНПИ, которыми может воспользоваться злоумышленник.

Территориально потенциально возможные несанкционированные действия могут иметь место в различных зонах:

внешней неконтролируемой зоне - территории вокруг объекта, на которой не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации;

зоне контролируемой территории - территории вокруг помещений, где расположены средства обработки информации, которая непрерывно контролируется персоналом или соответствующими техническими средствами;

зоне помещений - внутреннего пространства тех помещений, в которых расположены средства обработки информации;

зоне ресурсов - части помещений, откуда возможен непосредственный доступ к ресурсам системы;

зоне баз данных - части ресурсов системы, из которых возможен непосредственный доступ к защищаемым данным.

При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий:

нарушитель должен получить доступ в соответствующую зону;

во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий КНПИ;

проявившийся КНПИ должен быть доступен нарушителю соответствующей категории;

в КНПИ в момент доступа к нему нарушителя должна находиться защищаемая информация.

Попытаемся теперь с учетом изложенного вывести формулу для оценки уязвимости информации. Для этого введем следующие обозначения:

$P_{ijkl}^{(\delta)}$ - вероятность доступа нарушителя k -й категории в I -ю зону i -го компонента системы;

$P_{ijl}^{(k)}$ - вероятность наличия (проявления) j -го КНПИ в I -й зоне i -го компонента системы;

$P_{ijkl}^{(H)}$ - вероятность доступа нарушителя k -й категории к j -му КНПИ в I -й зоне i -го компонента при условии доступа нарушителя в зону;

$P_{ijl}^{(u)}$ - вероятность наличия защищаемой информации в j -м КНПИ в I -й зоне i -го компонента в момент доступа туда нарушителя.

Тогда вероятность несанкционированного получения информации нарушителем k -й категории по j -му КНПИ в I -й зоне i -го структурного компонента системы определится следующей зависимостью:

$$P_{ijkl} = P_{ijl}^{(\delta)} P_{ijl}^{(k)} P_{ijkl}^{(H)} P_{ijl}^{(u)}. \quad (3.1)$$

Вероятность несанкционированного получения информации в одном компоненте системы одним злоумышленником одной категории по одному КНПИ, назовем базовым показателем уязвимости информации (с точки зрения несанкционированного получения). С учетом (3.1) выражение для базового показателя будет иметь следующий вид:

$$P_{ijk}^{(\delta)} = 1 - \prod_{l=1}^5 (1 - P_{ijkl}) = 1 - \prod_{l=1}^5 \left[1 - P_{ijkl}^{(\delta)} P_{ijl}^{(k)} P_{ijkl}^{(H)} P_{ijl}^{(u)} \right]. \quad (3.2)$$

Рассчитанные таким образом базовые показатели уязвимости сами по себе имеют ограниченное практическое значение. Для решения задач, связанных с разработкой и эксплуатацией систем защиты информации, необходимы значения показателей уязвимости, обобщенные по какому-либо одному индексу (i, j, k) или по их комбинации. Рассмотрим возможные подходы к определению таких частично обобщенных показателей.

Пусть $\{K^*\}$ есть интересующее нас подмножество из полного множества потенциально возможных нарушителей. Тогда вероятность нарушения защищенности информации указанным подмножеством нарушителей по j -му фактору в i -м компоненте системы ($P_{ij\{K^*\}}$) определится выражением:

$$P_{ij\{K^*\}} = 1 - \prod_{k^*} [1 - P_{ijk}^{(6)}] \quad (3.3)$$

где K^* означает перемножение выражений в скобках для всех k , входящих в подмножество $\{K^*\}$.

Аналогично, если $\{J^*\}$ есть подмножество представляющих интерес КНПИ, то уязвимость информации в i -м компоненте по данному подмножеству факторов относительно k -го нарушителя определится выражением:

$$P_{i\{J^*\}k} = 1 - \prod_{j^*} [1 - P_{ijk}^{(6)}] \quad (3.4)$$

Наконец, если $\{I^*\}$ есть подмножество интересующих нас структурных компонентов системы, то уязвимость информации в них по j -му КНПИ относительно k -го нарушителя

$$P_{\{I^*\}jk} = 1 - \prod_{i^*} [1 - P_{ijk}^{(6)}] \quad (3.5)$$

Каждое из приведенных выше выражений позволяет производить обобщение по одному какому-либо параметру. Нетрудно получить и общее выражение, если нас интересуют подмножества $\{I^*\}, \{J^*\}$ и $\{K^*\}$ одновременно. В этом случае

$$P_{\{I^*\}\{J^*\}\{K^*\}} = 1 - \prod_{i^*} [1 - P_{ijk}^{(6)}] \prod_{j^*} [1 - P_{ijk}^{(6)}] \prod_{k^*} [1 - P_{ijk}^{(6)}] \quad (3.6)$$

Очевидно, общий показатель уязвимости P определяется при таком подходе выражением

Глава 3

$$P = 1 - \prod_i [1 - P_{ijk}^{(6)}] \prod_j [1 - P_{ijk}^{(5)}] \prod_k [1 - P_{ijk}^{(6)}] \quad (3.7)$$

На практике наибольший интерес представляют экстремальные показатели уязвимости, характеризующие наиболее неблагополучные условия защищенности информации: самый уязвимый структурный компонент системы (i'), самый опасный КНПИ (j'), самая опасная категория нарушителей (k')

Аналогичным образом может быть проведена оценка уязвимости информации и в других случаях, в частности в случае нарушения целостности.

Рассмотрим далее методы расчета показателей уязвимости информации с учетом интервала времени, на котором оценивается уязвимость. При этом следует учитывать, что чем больше интервал времени, тем больше возможностей у нарушителей для злумышленных действий и тем больше вероятность изменения состояния системы и условий обработки информации.

Можно определить такие временные интервалы (не сводимые к точке), на которых процессы, связанные с нарушением защищенности информации, являлись бы однородными. В учебнике [31] эти интервалы названы малыми. Такой малый интервал, в свою очередь, может быть разделен на очень малые интервалы, уязвимость информации на каждом из которых определяется независимо от других. При этом в силу однородности происходящих процессов уязвимость информации на каждом из выделенных очень малых интервалов будет определяться по одной и той же зависимости.

Тогда, если через P_t^m обозначить интересующий нас показатель уязвимости в точке (на очень малом интервале), а через P^μ - тот же показатель на малом интервале, то

$$P^\mu = 1 - \prod_{t=1}^n (1 - P_t^m) \quad (3.8)$$

где t - переменный индекс очень малых интервалов, на которые поделен малый интервал; n - общее число очень малых интервалов.

Нетрудно видеть, что рассмотренный подход можно распространить и на другие интервалы, а именно: большой интервал представить некоторой последовательностью малых, очень боль-

шой - последовательностью больших, бесконечно большой - последовательностью очень больших.

Однако приведенные выражения будут справедливыми лишь в том случае, если на всем рассматриваемом интервале времени условия для нарушения защищенности информации остаются неизменными. В действительности эти условия могут изменяться, причем наиболее важным фактором здесь является активное действие самой системы защиты информации.

Желающих более подробно ознакомиться с оценкой уязвимости информации на различных временных интервалах мы отсылаем к книге В.А. Герасименко [3], в которой приведен ряд моделей определения значений показателей уязвимости для наиболее распространенных технологических маршрутов обработки информации.

Здесь же мы обратим внимание на то, что во всех рассмотренных нами выражениях, структурирующих оценку уязвимости информации, присутствуют показатели, представляющие собой вероятности реализации тех или иных событий. Значения этих показателей при отсутствии достаточного статистического материала могут быть получены только экспертным путем с использованием, например, описанной выше технологии автоформализации знаний. При этом исключительное значение приобретает оценка достоверности данных, опираясь на которые эксперт-аналитик принимает то или иное решение. В связи с этим представляется целесообразным вопрос оценки достоверности рассмотреть самостоятельно, посвятив ему специальный параграф данной главы.

3.4. Методы оценки достоверности информационной базы моделей прогнозирования значений показателей уязвимости информации

Определяющей компонентой общего алгоритма работы эксперта при решении задачи оценки уязвимости информации (рис. 3.1) является формирование так называемой интегрированной базы данных (ИБД), представляющей собой взаимосвязанную совокупность собственно базы данных (БД), базы знаний (БЗ) и базы моделей (БМ).

Нетрудно видеть, что указанный алгоритм в отличие от известного алгоритма вычислительного эксперимента с имитационной моделью имеет признаки, характерные для самоорганизующихся систем, и позволяет эксперту использовать данные, знания, объективные и субъективные модели для анализа и решения поставлен-

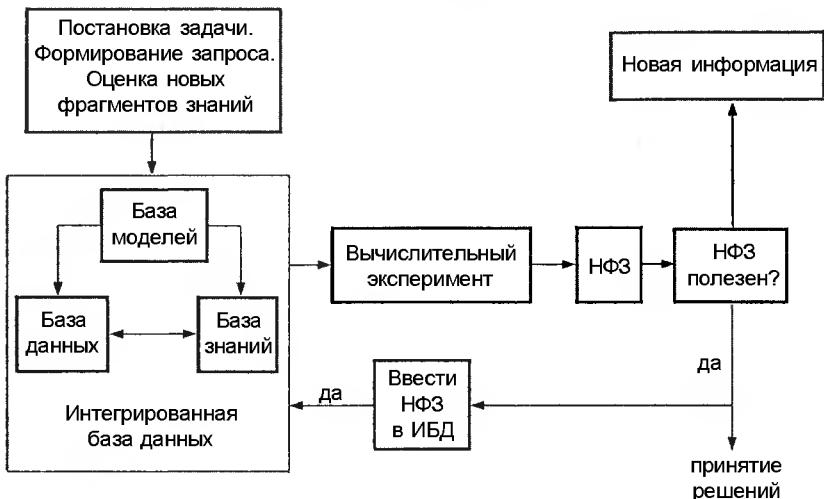


Рис. 3.1. Общий алгоритм работы эксперта

ной проблемы в условиях недоопределенности БД и неполноты БЗ. При этом из всех аспектов, связанных с созданием ИБД, решающее значение приобретает проблема оценки достоверности входящей в нее информации.

Определим достоверность как «уровень разумной уверенности в истинности некоего высказывания, который удовлетворяет некоторым правилам непротиворечивости и в соответствии с этими правилами формально может быть выражен числом» [46].

Известные подходы к решению проблемы оценки достоверности связаны с применением теоремы Байеса (в широком смысле) (см. [46]) и теории нечетких множеств, на основе которых в настоящее время разработаны и применяются в экспертных системах практические способы объединения свидетельств, регистрирующих качественные и логико-семантические связи между фрагментами базы данных.

Используя идею байесовского подхода, можно поставить вопрос о достоверности фрагментов ИБД в более общем плане, рассматривая любой ее фрагмент как гипотезу, а фрагменты с которыми он связан, как свидетельства относительно фрагмента-гипотезы. Под фрагментом ИБД будем понимать часть содержания или структуры, обладающую свойством дискретности и независимости (в идеале содержащую одно независимое понятие), т.е. некоторую

совокупность данных или высказываний, имеющую самостоятельный смысл.

Достоверность (D) фрагмента, поступающего в ИБД, зависит от достоверности источника информации и методики ее получения. Каждый вновь поступающий в ИБД фрагмент (НФЗ - новый фрагмент знаний) есть пара:

$$НФЗ = \langle З, D \rangle, \quad (3.9)$$

где $З$ - значение фрагмента; D - достоверность фрагмента.

Разделим фрагменты-свидетельства на классы: прямые свидетельства (ПС); косвенные свидетельства: условные (УС) и связанные (СС).

Под прямыми свидетельствами будем понимать фрагменты типа измерения значения фрагмента-гипотезы. Они составляют выборку, на основании которой могут быть рассчитаны оценки значения фрагмента-гипотезы, и регистрируют, в основном, статистические связи между фрагментами.

Под условными свидетельствами будем понимать фрагменты типа: «если A и/или B , то C с достоверностью P ». С их помощью можно регистрировать качественные экспертные оценки, логические связи между фрагментами и априорные знания о фрагменте-гипотезе (условия применения того или иного метода, условные функции распределения и т.п.).

Связанные свидетельства регистрируют функциональные или системные связи между фрагментом-гипотезой и другими фрагментами, т.е. структуру некоторой достаточно автономной части ИБД (формулы, модели и т.п.).

НФЗ, будучи включенным в ИБД, взаимодействует с уже содержащимися в ней фрагментами и гипотезами, изменяя как их значения, так и достоверности. Эта реакция достаточно сложна и вызывает модификацию значений и достоверностей всех старых фрагментов ИБД, так или иначе связанных с вновь поступившими НФЗ. Для описания процесса модификации введем понятия системного значения (СЗ) и системной достоверности (СД) фрагмента ИБД, определяемых с учетом всех свидетельств, содержащихся в ИБД.

Таким образом, с учетом введенной классификации проблема оценки достоверности сводится к разработке методов определения в качестве атрибутов фрагмента-гипотезы ИБД системных достоверностей фрагментов, являющихся для данного фрагмента-

гипотезы свидетельствами, а также системной достоверности данного фрагмента-гипотезы.

Рассмотрим возможность разработки формального алгоритма модификации фрагмента ИБД, а также методов обработки свидетельств.

Для модификации значения и достоверности фрагмента ИБД при изменении состава свидетельств можно использовать алгоритм, блок-схема которого изображена на рис. 3.2. Предполагается, что фрагменты представлены в ИБД в виде так называемых фреймов (элементов знаний), которые включают в свой состав:

З - значение фрагмента при поступлении в ИБД;

Д - достоверность фрагмента при поступлении в ИБД;

КПС - кортеж прямых свидетельств для данного фрагмента;

КУС - кортеж условных свидетельств;

КСС - кортеж связанных свидетельств;

ПЗ, ПД - значение и достоверность фрагмента с учетом всех прямых свидетельств;

УЗ, УД - значение и достоверность фрагмента с учетом всех условных свидетельств;

СЗ, СД - системные значение и достоверность фрагмента.

Алгоритм работает следующим образом.

В блоке Π_1 (рис. 3.2) формируются параметры выборки прямых свидетельств и на их основе - точечные или интервальные оценки ($\text{ПЗ}_k, \text{ПД}_k$) параметров распределения значения k -го фрагмента.

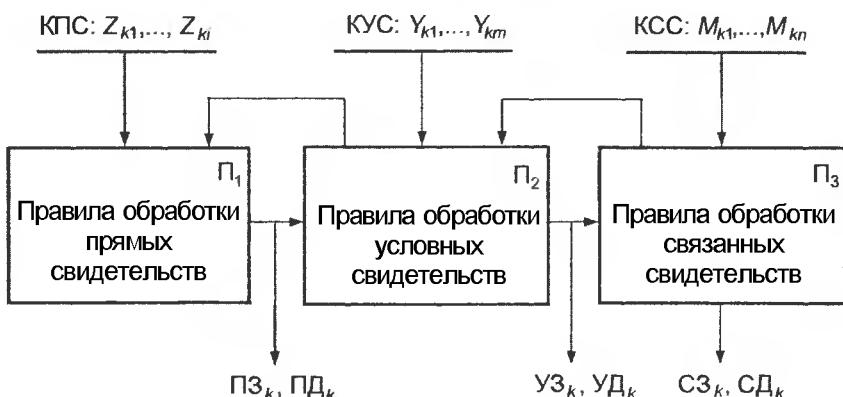


Рис. 3.2. Блок-схема алгоритма вычисления системного значения и системной достоверности фрагмента ИБД

Эти оценки присваиваются соответствующим элементам данного фрагмента, а также подаются на вход блока Π_2 .

В блоке Π_2 вычисляются условное значение и условная достоверность ($УЗ_k$, $УД_k$) k -го фрагмента с учетом состояния условий и ограничений блока Π_2 в данный момент. Полученные $УЗ_k$ и $УД_k$ присваиваются соответствующим элементам фрагмента и одновременно подаются на вход блока Π_3 . До обработки выборки можно пропустить через блок Π_2 каждое ПС.

В блоке Π_3 , $УЗ_k$ и $УД_k$ рассматриваются как значение и достоверность поступившего нового свидетельства и для каждого связанного свидетельства (модели, содержащей этот фрагмент) уточняется вектор состояния, а результат снова подается на вход Π_2 . Процесс заканчивается при достижении заданного числа итераций или заданной точности оценки. Новые системные оценки получат значения всех фрагментов, являющихся составляющими векторов состояний моделей блока Π_3 . Значения C_{3k} и C_{dk} присваиваются соответствующим элементам данного фрагмента.

Очевидная проблема, возникающая при реализации описанного подхода, это разрастание числа фрагментов, вовлекаемых в алгоритм, до числа содержащихся в ИБД, включая все модели. Чтобы ее разрешить, необходимо ограничить число связей между фрагментами, регистрируя только самые существенные. Вопрос этот решает сам эксперт. Как следствие появляются варианты системной достоверности:

СДД - по К наиболее достоверным свидетельствам;

СДЦ - по К наиболее ценным свидетельствам;

СДП - по К последним свидетельствам.

Иными словами, для каждой конкретной задачи необходимо актуализировать свою определенную часть ИБД, т.е. уметь выделить наиболее существенные связи и фрагменты (доминант-фрагменты), образующие поле вычислительного эксперимента. Это позволит не только ограничить множество фрагментов и связей, но и повысит непротиворечивость фрагментов, выделенных из ИБД для решения конкретной задачи.

Рассмотрим более подробно методы обработки свидетельств, которые могут быть применены в описанном алгоритме модификации.

Прямые и условные свидетельства могут быть предварительно структурированы в кубе с осями "фрагмент-источник-время" (рис. 3.3). Этот куб можно рассматривать как многоэтапную экспертизу и применить к нему методы обработки экспертных оценок, рассматривая источники информации как отдельных экспертов.

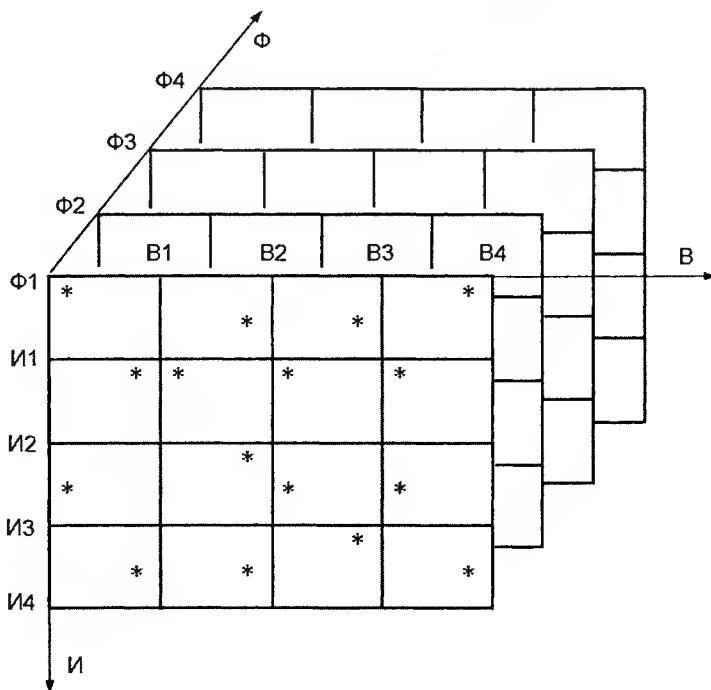


Рис. 3.3. Представление свидетельств в виде куба: (фрагмент, время, источник, * - значение фрагмента)

Различные сечения куба позволяют анализировать разные свойства сгруппированной таким образом информации:

зависимости фрагментов Φ_1, \dots, Φ_k от источников информации I_1, \dots, I_n на некоторый момент времени (статика);

зависимости фрагментов Φ_1, \dots, Φ_k от времени по сведениям из одного источника (динамика);

зависимости одного фрагмента Φ_i от времени по сведениям из разных источников (динамика).

Любые достоверные данные, поступившие в ИБД и относящиеся к определенному моменту времени, рассматриваются на этот момент как эталонные, в соответствии с чем на этот же момент времени пересчитываются и достоверности источников информации. Эти методы традиционны для экспертных систем.

Вычислив параметры выборки, мы можем:

- назначить фрагменту-гипотезе значение и достоверность;

- модифицировать всем фрагментам - ПС достоверности, оставив их значения прежними;
- модифицировать достоверности источников информации.

Кроме метода экспертных оценок для обработки ПС и УС могут быть применены другие достаточно традиционные методы теории вероятностей и математической статистики, а выбор их зависит от наличия априорной информации об исследуемом объекте.

При выборе методов обработки связанных свидетельств, необходимо исходить из того, что такими свидетельствами являются законы конкретной предметной области и построенные на их основе модели исследуемых систем и внешних сред.

Строя модель, фиксируя в ней структуру и параметры исследуемого объекта, анализируя результат вычислительного эксперимента и модифицируя в соответствии с ним, а также в соответствии с поступающими свидетельствами фрагменты ИБД, эксперт формализует свои интуитивные представления и личный профессиональный опыт.

Этот процесс построения моделей самим экспертом и их постоянной модификации при появлении новой информации и является описанным выше процессом автоформализации знаний эксперта. При этом, начальные варианты моделей, как правило, достаточно просты, часто линейны или линеаризованы. Основная задача на первых итерациях - обеспечить принципиальную правильность и устойчивость модели. Однако, для ее дальнейшего улучшения очевидно необходим анализ всей вновь поступающей информации о векторе ее состояния, на основании которого можно было бы модифицировать значения и достоверности фрагментов модели, устранить в ней структурные и параметрические неопределенности.

Понятный и достаточно универсальный алгоритм модификации значения и достоверности вектора состояния моделей такого типа (т.е. целой связи фрагментов) по поступившей информации о некоторых фрагментах вектора состояния дает применение формального аппарата теории динамических систем, устойчивых к отказам [47], в основе которого лежит Байесов подход. Этот аппарат хорошо развит применительно к вероятностным системам, параметры и структура которых могут скачкообразно меняться в случайные моменты времени. Учитывая неполноту БЗ и неопределенность БД, можно сделать вывод, что большинство моделей в задачах оценки и прогнозирования уровня уязвимости информации будет принадлежать именно к этому классу.

Глава 3

Рассмотрим еще один возможный подход к определению достоверности фрагментов интегрированной базы данных, основанный на применении методов фильтрации.

Общая постановка задачи нелинейной оптимальной фильтрации имеет следующий вид:

$$x(k+1) = F[x(k), w(k), d(k)], \quad (3.10)$$

$$y(k) = H[x(k), v(k), d(k)], \quad (3.11)$$

где уравнение состояния (3.10) описывает структуру и динамику исследуемой системы, а уравнение наблюдения (3.11) определяет механизм образования данных, доступных для эксперта-аналитика. Здесь: $x(k)$ - вектор состояния исследуемой системы; $w(k)$ - случайный вектор шумов исследуемой системы, связанных с погрешностями методов моделирования; $y(k)$ - вектор наблюдения; $v(k)$ - случайный вектор шумов наблюдения, связанных с погрешностями канала получения информации (w и v некоррелированы); $d(k)$ - вектор вариативности, характеризующий текущее состояние и структуру системы и канала получения информации (при этом, отказ в системе рассматривается как изменение ее параметров или структуры).

Задача фильтрации заключается в получении по последовательности наблюдений $y(k) = \{y(1), y(2), \dots, y(k)\}$ оценки вектора состояния $x(k)$, оптимальной по критерию минимума среднего квадратического отклонения, и ее корреляционной матрицы.

Допустим, эксперт располагает последовательностью $y(k)$ наблюдений за исследуемым объектом. На основе этих наблюдений и предшествующего опыта (априорная информация) эксперт выдвигает гипотезы F и H о структуре и параметрах наблюдаемого объекта и источника информации. Задавшись начальными условиями, он может теперь проверить справедливость своей гипотезы, последовательно применяя алгоритм фильтрации для уточнения параметров F и H с помощью каждого из имеющихся наблюдений (рис. 3.4).

Этот алгоритм позволяет эксперту каждый раз при поступлении в ИБД новых данных $y(k)$ об исследуемом объекте рекуррентно модифицировать оценку значения его вектора состояния $x(k)$ и корреляционную матрицу ошибок $P(k)$, характеризующую достоверность этой оценки, с учетом всех поступивших на данный момент наблюдений $y(k)$, а также динамики и структуры изучаемого объекта и каналов получения информации.

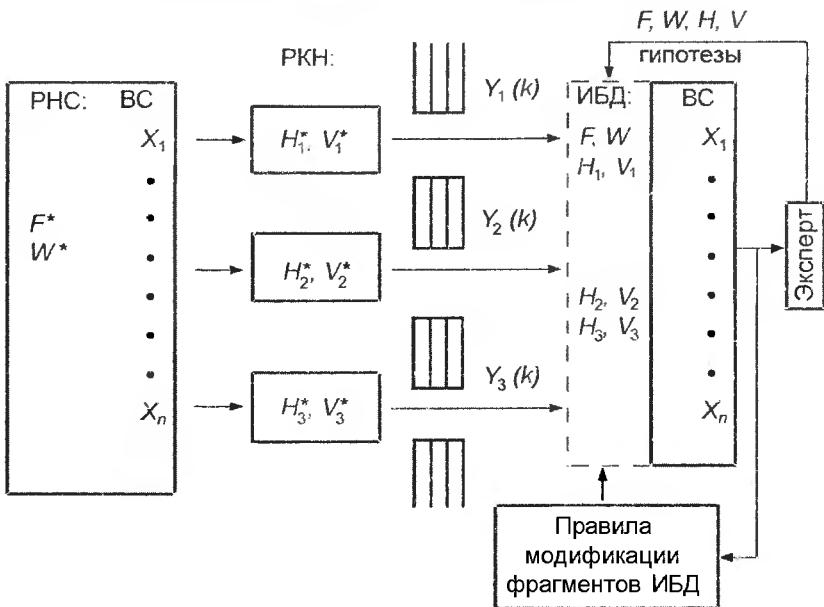


Рис.3.4. Модель информационной среды эксперта
РНС - реальная наблюдаемая система; РКН - реальный канал наблюдения;
ВС - вектор состояния; ИБД - интегрированная база данных

Критерием достоверности гипотезы (F, H) здесь могут быть расхождение z реального наблюдения $y(k)$ и прогноза для наблюдения на k -ом шаге $\bar{y}(k)$:

$$z = y(k) - \bar{y}(k) = y(k) - H [\bar{x}(k), v(k), d(k)], \quad (3.12)$$

а также динамика изменения корреляционной матрицы $P(k)$ для оценки вектора состояния $x(k)$.

Если они достаточно малы, это говорит о том, что эксперт верно идентифицировал по поступившей информации структуру и параметры объекта и источника информации. Если нет - необходимо изменить гипотезу для F или H .

С этой целью рассмотрим множество возможных структур исследуемого объекта $\{F\}$ и источника информации $\{H\}$. Пусть таких структур n . Тогда допустимое значение d_i ($i = 1, \dots, n$) вектора d представляет одну из возможных структур исследуемого объекта и источника информации об объекте.

В общем случае d может изменяться на каждом шаге и на k -том шаге образует произвольную последовательность $D_l(k)$ из k допустимых значений вектора d . Число l таких последовательностей, образующих множество $D = \{D_l(k)\}$, определяется выражением:

$$l = n^k. \quad (3.13)$$

Легко видеть, что $l \rightarrow \infty$ при $n > 1$ и $k \rightarrow \infty$.

Для каждой последовательности $D_l(k)$, в предположении, что она осуществилась на самом деле, на основании имеющихся наблюдений может быть вычислено значение вектора состояния и его достоверность.

Из теории оценивания известно, что критерий минимума среднего квадратического отклонения приводит к оценкам условного среднего:

$$\hat{x}(k) = E[x(k) : Y(k), D_l(k)], \quad (3.14)$$

а их качество определяется условной корреляционной матрицей ошибок оценивания:

$$\hat{P}(k) = E\left\{\left[x(k) - \hat{x}(k)\right]^* \left[x(k) - \hat{x}(k)\right]^T : Y(k), D_l(k)\right\}. \quad (3.15)$$

Опуская вывод, запишем (3.14) и (3.15) в развернутом виде:

$$\hat{x}(k) = \sum_l \hat{x}_l(k)^*; \quad p[D_l(k) : Y(k)], \quad (3.16)$$

где $\hat{x}_l(k) = E[x(k) : Y(k), D_l(k)]$ - частная оценка вектора состояния $x(k)$, т.е. оптимальная оценка, полученная для конкретной реализации $D_l(k)$ последовательности $d(k)$ и удовлетворяющая критерию минимума среднего квадратического отклонения; $p[D_l(k) : Y(k)]$ - апостериорная вероятность этой реализации;

$$\hat{P}(k) = \sum_l \{P_l(k) + DP_l(k)\}^* p[D_l(k) : Y(k)], \quad (3.17)$$

где

$$\hat{P}_l(k) = E[\tilde{x}_l(k)^* \tilde{x}_l^T(k) : Y(k), D_l(k)]; \quad (3.18)$$

$$DP_l(k) = \left[\hat{x}_l(k) - \hat{\bar{x}}(k) \right] * \left[\hat{x}_l(k) - \hat{\bar{x}}(k) \right]^T; \quad (3.19)$$

l – номера всех возможных $D_l(k)$;

$$\tilde{x}_l(k) = \hat{x}_l(k) - \hat{\bar{x}}(k)$$

В этих выражениях $P_l(k)$ и $DP_l(k)$ есть соответствующие корреляционные матрицы ошибок частных оценок вектора состояния.

Таким образом, в общем виде алгоритм оптимальной фильтрации представляет следующую последовательность вычислений:

- для принятой реализации наблюдения $Y(k)$ рассчитываются частные оценки вектора состояния для всех возможных реализаций $D_l(k)$ и соответствующие частные корреляционные матрицы;
- рассчитываются значения $p[D_l(k) : Y(k)]$, играющие роль весовых коэффициентов в уравнениях (3.16) и (3.17);
- рассчитывается по (3.16) оптимальная оценка $\hat{x}(k)$ вектора состояния $x(k)$;
- рассчитывается по (3.17) корреляционная матрица ошибок оценивания;
- рассчитывается прогноз оценки, ее корреляционной матрицы и наблюдения на следующий шаг;
- рассчитываются переходная матрица исследуемой системы, матрица канала наблюдения и корреляционные матрицы шумов на следующий шаг.

Этот процесс сходится при достаточно общих предположениях (если угаданы структура и опорные функции), причем особенно эффективно уточнение параметров идет во время первых нескольких шагов.

При практической реализации алгоритма оптимальной фильтрации возникают следующие проблемы:

- при возрастании числа наблюдений k неограниченно возрастает / и, следовательно, число частных оценок, что требует неограниченных вычислительных ресурсов;
- требуется разработка конкретных подходов к вычислению частных оценок вектора состояния, соответствующих корреляционных матриц и вероятности различных последовательностей $D_l(k)$.

Возможные пути преодоления этих трудностей могут быть сведены к следующему:

- выбор определенных структур для исследуемой системы и ка-

нала наблюдения;

- выбор определенных классов $d(k)$ и $D(k)$;
- ограничение числа учитываемых наблюдений;
- введение некоторых гипотез при аппроксимации прогноза значения вектора состояния исследуемой системы.

В итоге задача может решаться в следующей постановке:

$$x(k+1) = d_1(k) * F(k+1, k) * x(k) + d_2(k) * w(k) \quad , (3.20)$$

$$y(k) = d_3(k) * H(k) * x(k) + d_4(k) * v(k). \quad , (3.21)$$

где сделаны следующие предположения: структура исследуемой системы и канала наблюдения линейна; шумы $w(k)$ и $v(k)$ - белые, не-коррелированы между собой и с вектором $x(k)$.

В уравнениях (3.20) и (3.21) $d(k) = \{d_1(k), d_2(k), d_3(k), d_4(k)\}$ задают конкретные возможные режимы исследуемой системы и канала наблюдения, например:

$d(k) = \{1, 1, 1, 1\}$ - нормальный режим функционирования исследуемой системы и канала наблюдения, когда эксперту известны с точностью до шума их структура и параметры;

$d(k) = \{1, 1, 1, s \gg 1\}$ - в канале наблюдения резко возрос уровень шума, в результате чего возрос разброс поступающих к эксперту данных без изменения среднего значения вектора состояния исследуемой системы;

$d(k) = \{1, 1, 0, 1\}$ - отсутствует информация в канале наблюдения, в результате чего в поступающих к эксперту данных пропала систематика и остался один белый шум;

$d(k) = \{1, 1, 0, s \gg 1\}$ - отсутствует информация в канале наблюдения и в то же время резко возрос шум; такой вариант означает, скорее всего, что изменилось содержание поступающей информации, а эксперт, не умея «расшифровать» эту информацию, принимает ее за шум;

$d(k) = \{1, 0, 1, 1\}$ - отсутствуют шумы в модели исследуемой системы, т.е. эксперт сумел подобрать точную детерминированную модель;

$d(k) = \{1, s \gg 1, 1, 1\}$ - резко возросли шумы в модели исследуемой системы; при этом если шум остался белым, то модель эксперта верна, но сам исследуемый объект стал менее детерминированным, а если шум окрашен (имеет систематику), то модель эксперта требует уточнения (систематика должна быть расшифрована экспертом и включена в модель исследуемой системы).

Таким образом, видно, что даже с приведенным сравнительно простым набором возможных значений вектора вариативности $d(k)$

можно описать широкий круг проблем, связанных с достоверностью фрагмента ИБД, а в более широком плане - получить универсальный и гибкий формальный аппарат модификации фрагментов ИБД при поступлении в нее нового фрагмента.

Исследование конкретной проблемы, стоящей перед экспертом, следует начинать с тех случаев, когда изменения и модификации затрагивают прежде всего канал наблюдения. Если эксперт изучает некоторую сложную систему (объект) достаточно долго, то имеет определенное представление о ее структуре и параметрах, пусть и не очень точное. В этой ситуации главной становится задача оценки достоверности источников информации, а задача уточнения параметров исследуемой системы решается по мере решения первой задачи. Для такой постановки $d(k) = \{1, 1, d_3(k), d_4(k)\}$ и, соответственно, система уравнений принимает вид:

$$x(k+1) = F(k+1, k) * x(k) + w(k), \quad (3.22)$$

$$y(k) = d_3(k) * H(k) * x(k) + d_4(k) * v(k). \quad (3.23)$$

Для нормального режима функционирования исследуемой системы и канала наблюдения уравнение имеет вид:

$$x(k+1) = F(k+1, k) * x(k) + w(k), \quad (3.24)$$

$$y(k) = H(k) * x(k) + v(k), \quad (3.25)$$

а алгоритм модификации вектора состояния исследуемой системы для k -го шага есть классический алгоритм оптимального фильтра Калмана (рис. 3.5).

Располагая этим алгоритмом можно досконально изучить на этапе предварительного моделирования исследуемую систему, основной режим работы которой описывается линейной системой уравнений, а также получить все частные оптимальные оценки вектора состояния системы и их корреляционные матрицы, что снижает часть перечисленных выше проблем реализации общего алгоритма оптимальной фильтрации.

Наибольшие трудности вызывает корректное вычисление условной вероятности $p[D_k(k) : Y(k)]$ даже для несложных систем. Анализ точных выражений для $p[D_k(k) : Y(k)]$, однако, показывает, что для многих случаев, связанных с исследованием уровня уязвимости информации, данную вероятность можно аппроксимировать двумя-тремя значениями типа 0-1/2-1 (нет - может быть - да).

Дело в том, что особенностью экспертных задач оценки уровня обеспечения безопасности информации является, как отмечалось

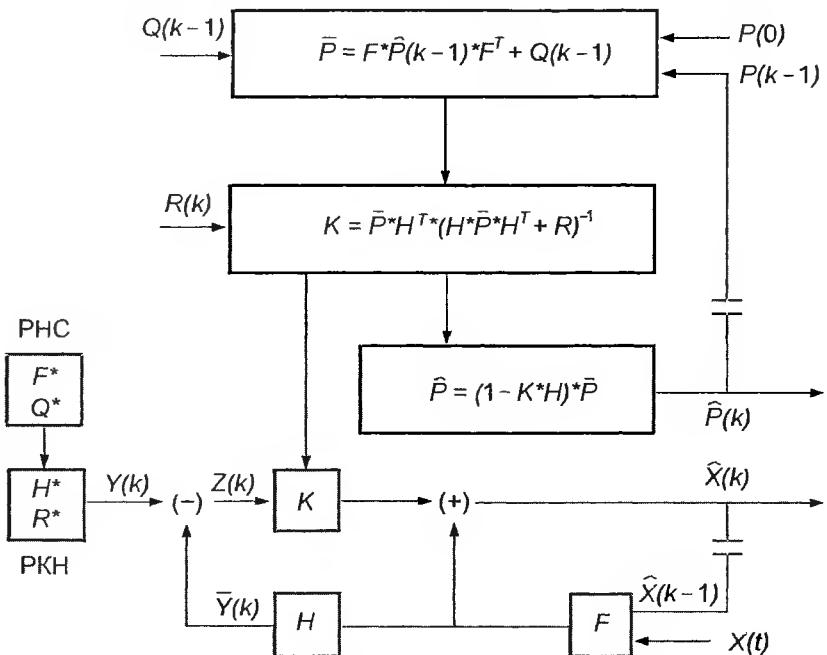


Рис. 3.5. Блок-схема алгоритма ОФК (оптимальный фильтр Калмана): РНС - реальная наблюдаемая система; РКН - реальный канал наблюдения; \dashv - звено задержки; Q и R - корреляционные матрицы шумов системы и канала наблюдения

выше, неполнота данных, которыми располагает эксперт практически на всех этапах исследования сложного объекта информатизации. Принцип баланса точностей рекомендует в таких случаях не пользоваться тонкими сложными методами моделирования, поскольку их точность будет загублена неполнотой и неточностью исходной информации, а их сложность практически неизбежно приведет к невероятному результату в силу неадекватности отдельных частей модели и объекта. В соответствии с этим принципом должен соблюдаться некоторый разумный баланс между требующейся точностью ответа, точностью исходных данных, точностью модели и точностью метода исследования. В этом смысле сделанное допущение вполне разумно, особенно на первых этапах исследования сложного объекта, когда проверяются, в основном, правильность структуры исследуемой системы и канала наблюде-

ния, а также области возможных значений их параметров. Критерием здесь может быть отклонение очередного наблюдения от его прогноза, например:

$$p[D_l(k) : Y(k)] = \begin{cases} 0, & \text{если } |z| > r_0 * \sqrt{\det P_z}, \\ 1, & \text{если } |z| < r_l * \sqrt{\det P_z}, 0 < r_l < r_0, \\ 1/2 & \text{в иных случаях,} \end{cases} \quad (3.26)$$

т.е. вычисление условной вероятности предельно упрощается: необходимо только сравнить поступившее наблюдение y с некоторыми пороговыми значениями и выбрать соответствующее значение $p[D_l(k) : Y(k)]$ (рис. 3.6).

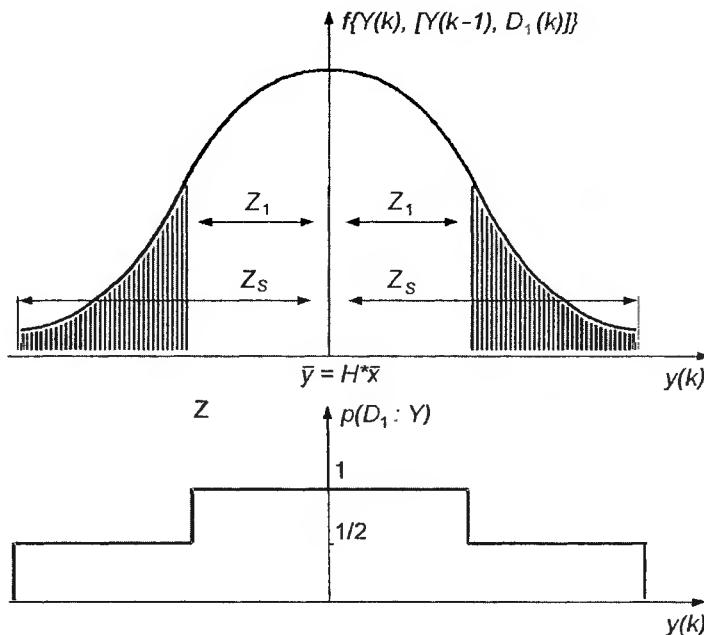


Рис. 3.6. Определение $p[D_l(k) : Y(k)]$ по отклонению наблюдения $y(k)$ от прогноза $\bar{y}(k)$

3.5. Модели оценки ущерба от реализации угроз безопасности информации

Уязвимость информации не определяется только вероятностями проявления тех или иных угроз. Совершенно очевидно, что с другой стороны она характеризуется возможным ущербом, который будет иметь место в случае их реализации.

Вопрос оценки ущерба представляет на сегодняшний день наиболее сложную задачу, практически не поддающуюся формализации и решаемую только с использованием методов экспертных оценок. При этом в целях формирования прогнозных оценок ущерба можно с успехом применять описанную нами выше технологию формализации профессиональных знаний, опирающуюся на некоторые модели, которые могут составить первоначальную базу моделей, в дальнейшем уточняемую и видоизменяющую экспертом.

Исходной посылкой при разработке этих моделей может явиться очевидное предположение, что полная ожидаемая стоимость защиты информации может быть выражена суммой расходов на защиту и потерь от ее нарушения. В работе [3] В.А. Герасименко показал, что при этом подходе оптимальным решением было бы выделение на защиту информации средств в размере C_{opt} (см. рис. 3.7), поскольку именно при этом обеспечивается минимизация общей стоимости защиты информации.

Поскольку, как видно из рис 3.7, при оптимальном решении целесообразный уровень затрат на защиту равен уровню ожидаемых потерь при нарушении защищенности, то для оценки суммарных затрат, достаточно определить только уровень потерь.

Для решения этой задачи профессором В.А. Герасименко в [3] был использован подход, основанный на динамической модели оценки потенциальных угроз. Рассмотрим его более подробно.

Допустим, что проявление угрозы рассматриваемого типа характеризуется случайной переменной λ с распределением вероятностей $f(\lambda)$. Заметим, что функция распределения $F(\lambda)$ должна определяться на основе обработки данных о фактах реального проявления угроз этого типа, которая проводится экспертом с обязательной оценкой достоверности используемой информации (см. предыдущий параграф).

Если рассматривать проявление данной угрозы в течение определенного периода времени, то числу этих проявлений r будет соответствовать распределение вероятностей $f(r|\lambda)$, которое может быть выражено функцией распределения Пуассона:

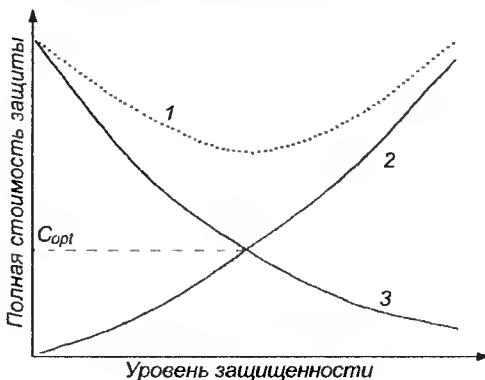


Рис. 3.7. Стоимостные зависимости защиты информации:
1 - ожидаемая полная стоимость; 2 - стоимость защиты; 3 - уровень ущерба

$$P(\bar{r} = r / \lambda) = \frac{(\lambda t)^r e^{-\lambda t}}{r!} \quad (3.27)$$

где t – период времени, за который определены значения r .

По ряду значений r_1, r_2, \dots, r_n функция $f(\lambda)$, может быть выражена функцией гамма-распределения

$$f(\lambda / a, b) = \frac{b^a \lambda^{a-1} e^{-b\lambda}}{(a-1)!} \quad (3.28)$$

где a и b параметры распределения, определяемые по рекурентным зависимостям:

$$\begin{aligned} a'' &= a' + r_1 + r_2 + \dots + r_n \\ b'' &= b' + t_1 + t_2 + \dots + t_n \end{aligned} \quad (3.29)$$

где r_1, r_2, \dots, r_n – число проявлений рассматриваемой угрозы в периоды наблюдения t_1, t_2, \dots, t_n .

Далее отметим, что безусловное распределение вероятностей проявления угроз за период времени t может быть представлено в виде:

$$f(r / a, b, t) = \int_0^{\infty} f(r / \lambda t) f(\lambda / a, b) d\lambda. \quad (3.30)$$

Глава 3

Тогда результирующее распределение

$$f_{nb}(r/P, a) = \frac{(r+a-1)}{r!(a-1)!} P^r (1-P)^{a-1}. \quad (3.31)$$

Количество проявлений угроз при этом характеризуется математическим ожиданием

$$E(\bar{r}/t) = \frac{at}{b} \quad (3.32)$$

и дисперсией

$$V = (\bar{r}/t) = \frac{at}{b(t+b)}. \quad (3.33)$$

Таким образом, мы описали вероятности проявления угроз. Для того, чтобы оценить ущерб от проявления угроз, рассмотрим для начала средние оценки ущерба, для которых может быть принята нормальная функция распределения с параметрами m и V :

$$f(\bar{m}, V/m'V', n', K') = f_n(m/m', V)f_g(V/V', \chi'), \quad (3.34)$$

где $f_n(\dots)$ и $f_g(\dots)$ - функции нормального и гамма-распределений вероятностей; n' и χ' - параметры нормального и гамма распределений.

Если в заданный период времени имеет место r проявлений рассматриваемой угрозы, которые приводят к ущербу x_1, x_2, \dots, x_r соответственно, то параметры распределения вероятностей ожидаемых потерь корректируются следующим образом:

$$\left. \begin{aligned} m'' &= \frac{n'm' + r\bar{x}}{n''}; \\ V'' &= \frac{\chi'V'n'(m')^2 + (r-1)S^2 + r\bar{x}^2 - n''(m'')^2}{\chi'+2}, \end{aligned} \right\} \quad (3.35)$$

где $n'' = n' + r$; $\chi' + r$; $\bar{x} = \sum x_i / r$; $\sum (x_i - \bar{x})^2 / (r-1)$.

Выделим далее неопределенные параметры m и V из функции распределения вероятностей для стоимости проявления угрозы данного типа. Тем самым будет получено прогнозируемое распределение для ущерба от возможного проявления рассматриваемой угрозы

$$f_s(x/m'', V'' \chi'') = \int_{-\infty}^{+\infty} \int_0^{\infty} f(x/m, V) f(m/m'', V'', V) f_s(V/V'', \chi'') dm dV, \quad (3.36)$$

где $f_s(\dots)$ - член семейства распределения Стьюдента.

Ожидаемое изменение значения \bar{x} определяется параметрами:

$$\left. \begin{aligned} E(\bar{x}) &= m''; \\ V(\bar{x}) &= \frac{\chi''}{\chi'' - 2} V''. \end{aligned} \right\} \quad (3.37)$$

Ожидаемые полные затраты в условиях проявления рассматриваемой угрозы \bar{C}_i определяются по формуле:

$$\bar{C}_i = \sum_{j=1}^{\bar{r}_i} \bar{x}_{ij}. \quad (3.38)$$

Поскольку полные затраты в условиях проявления угроз являются случайными величинами (из-за случайного характера нанесенного ущерба), то для их оценки необходимо знание соответствующей функции распределения вероятностей.

Таким образом, если бы существовали систематизированные статистические данные о проявлениях угроз и их последствиях, то рассмотренную модель, почерпнутую нами из работы [3], можно было бы использовать для решения достаточно широкого круга задач защиты информации. Более того, эта модель позволяет не только находить нужные решения, но и оценивать их точность, что, как подчеркивалось выше, имеет принципиальное значение. К сожалению, в силу ряда объективных и субъективных причин такая статистика в настоящее время практически отсутствует, что делает особо актуальной организацию непрерывного и регулярного сбора и обработки данных о проявлениях угроз, охватывающих возможно большее число реальных ситуаций.

Рассмотренная выше модель может быть сформулирована и в терминах теории игр. Предположим, что злоумышленник затрачивает X средств с целью преодоления защиты, на создание которой израсходовано Y средств. В результате он может получить защищаемую информацию, количество которой оценивается функцией $I(x, y)$. Положим далее, что $f(n)$ - есть ценность для злоумышленника n единиц информации, а $g(n)$ - суммарные затраты на создание

Глава 3

этого же числа единиц информации. Тогда чистая прибыль зломуышленника

$$V(x, y) = f[I(x, y)] - x, \quad (3.39)$$

а потери собственника информации

$$u(x, y) = g[I(x, y)] + y. \quad (3.40)$$

В соответствии с известными правилами теории игр оптимальные стратегии обеих сторон могут быть определены из условий:

$$\left. \begin{array}{l} f[I(x, y)] \frac{dI(x, y)}{dx} = 1; \\ g[I(x, y)] \frac{dI(x, y)}{dy} = -1. \end{array} \right\} \quad (3.41)$$

Для практического использования этой модели необходимо определить стоимость информации, а также задать функции I , f и g , что в условиях отсутствия необходимого объема статистических данных является практически неразрешимой проблемой, если опираться на формальные методы.

Таким образом, мы снова вынуждены возвращаться к описанным выше приемам автоформализации знаний, которые составляют основу методологического базиса теории защиты информации.

Рассмотренные нами подходы и модели позволяют в общем случае определять текущие и прогнозировать будущие значения показателей уязвимости информации. Необходимо только сделать некоторые существенные замечания относительно их адекватности. Во-первых, практически все приведенные нами модели построены в предположении независимости случайных событий, совокупности которых образуют сложные процессы защиты информации, а во-вторых - для обеспечения работы моделей необходимы исходные данные, формирование которых при отсутствии достоверной статистики сопряжено с большими трудностями.

Таким образом, при использовании этих моделей фактически делаются следующие допущения:

- возможности проявления каждой из потенциальных угроз не зависят от проявления других;
- каждый из злоумышленников действует независимо от других, т.е. не учитываются возможности формирования коалиции злоумышленников;
- негативное воздействие на информацию каждой из проявив-

шихся угроз не зависит от такого же воздействия других проявившихся угроз;

- негативное воздействие проявившихся угроз на информацию в одном каком-либо элементе системы может привести лишь к поступлению на входы связанных с ним элементов искаженной информации с нарушенной защищенностью и не оказывает влияния на такое же воздействие на информацию в самих этих элементах;

- каждое из используемых средств защиты оказывает нейтрализующее воздействие на проявившиеся угрозы и восстанавливющее воздействие на информацию независимо от такого же воздействия других средств защиты;

- благоприятное воздействие средств защиты в одном элементе системы лишь снижает вероятность поступления на входы связанных с ним элементов искаженной информации и не влияет на уровень защищенности информации в самих этих элементах.

В действительности же события, перечисленные выше, являются зависимыми, хотя степень зависимости различна - от незначительной, которой вполне можно пренебречь, до существенной, которую необходимо учитывать. Однако строго формальное решение данной задачи в силу приводившихся нами выше причин в настоящем времени невозможно, поэтому остаются лишь методы экспертных оценок и в частности, технология автоформализации знаний эксперта.

Что касается обеспечения моделей необходимыми исходными данными, то как неоднократно отмечалось, практическое использование любых предлагаемых моделей оценки уязвимости упирается в ограничения, связанные с неполнотой и недостоверностью исходных данных. В связи с этим отметим, что материалы данной главы, посвященные оценке и корректировке достоверности интегрированной базы данных моделирования, дают необходимый инструментарий для работы экспертов-аналитиков.

Вообще, правильно поставленная работа с исходными данными в условиях высокой степени их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением информационной безопасности. Поэтому проблема заключается не просто в формировании необходимых данных, а в перманентном их оценивании и уточнении. Поскольку экспертные оценки и технология автоформализации знаний в этих условиях становятся одними из основных методов решения основных задач защиты информации, а адекватность экспертных оценок существенно зависит от объема их выборки, то необходима организация и перманентное

Глава 3

осуществление массовой экспертизы в системе органов, ответственных за защиту информации. Существо концепции такой экспертизы будет рассмотрено в гл. 6.

Краткие выводы

1. Обоснование структуры и содержания системы показателей уязвимости информации, исследование влияния на них различных параметров угроз, разработка комплекса моделей и методологии адекватной оценки реальной уязвимости могут быть выполнены на основе системной классификации угроз, проведенной по следующим параметрам: виды угроз, происхождение угроз, предпосылки появления угроз, источники угроз. Перечисленные параметры находятся в сложных взаимосвязях, учет которых необходим для построения адекватных моделей, описывающих процессы нарушения целостности и защиты информации.

2. Основными параметрами, определяющими вероятность нарушения защищенности информации, являются: количество и типы структурных компонентов системы, количество и типы случайных дестабилизирующих факторов, количество и типы злоумышленных дестабилизирующих факторов, число и категории нарушителей, виды защищаемой информации.

Из множества разновидностей различных показателей уязвимости информации целесообразно выделить два показателя: первый (базовый) характеризует уязвимость в одном структурном компоненте системы при однократном проявлении одного дестабилизирующего фактора и относительно одного потенциального нарушителя, второй (общий) - уязвимость информации в целом по всем потенциально возможным дестабилизирующими факторам относительно всех потенциально возможных нарушителей. Все другие показатели являются частично обобщенными.

Для практического решения задач защиты информации могут быть также использованы показатели, характеризующие наиболее неблагоприятные ситуации (экстремальные показатели): самый уязвимый структурный компонент системы, самый опасный дестабилизирующий фактор, самый опасный нарушитель.

3. Одной из наиболее принципиальных особенностей проблемы защиты информации является абсолютный характер требования полноты выявленных угроз. При этом формирование полного множества угроз является ярко выраженной неструктуризованной проблемой.

Для первоначального формирования возможно более полного множества угроз целесообразно использовать различные модификации экспертных оценок. Наиболее эффективными здесь оказываются методы, основанные на технологии автоформализации знаний эксперта.

4. Рассмотренные в гл. 3 модели, а также модели, предлагаемые в других источниках (см., например, [3]), в общем случае позволяют определять текущие и прогнозировать будущие значения тех или иных показателей уязвимости информации в различных ситуациях функционирования систем и объектов. Однако все эти модели, построены в предположении независимости случайных событий, совокупности которых образуют сложные процессы защиты информации, а для обеспечения их работы необходимы исходные данные, систематизация и обобщение подавляющего большинства которых должны базироваться на сети центров защиты информации, организующих проведение массовой экспертизы.

Глава четвертая

ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

4.1. Постановка задачи и анализ существующих методик определения требований к защите информации

В самом общем виде и на чисто прагматическом уровне требования к защите могут быть определены как предотвращение угроз информации, по крайней мере тех из них, проявление которых может привести к существенно значимым последствиям. Но поскольку, как уже неоднократно нами отмечалось, защита информации есть случайный процесс (показатели уязвимости носят вероятностный характер), то и требования к защите должны выражаться терминами и понятиями теории вероятностей.

По аналогии с требованиями к надежности технических систем, обоснованными в классической теории систем, требования к защите могут быть сформулированы в виде условия:

$$P_3 \geq \bar{P}_3, \quad (4.1)$$

где P_3 - оценка реальной вероятности защищенности информации, а \bar{P}_3 - требуемый уровень защищенности.

С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем. Однако на практике решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории систем могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим переход от концепции создания инструментальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими процессами (иными словами снова встает проблема перехода от экстенсивных к интенсивным способам решения проблем защиты информации).

Требования к защите информации

Проблема определения требований к защите информации имеет комплексный характер и может рассматриваться как в организационном, так и в техническом аспектах. Причем в условиях автоматизированной обработки информации существует большое количество каналов несанкционированного ее получения, которые не могут быть перекрыты без применения специфических технических и программно-аппаратных средств. Это серьезно повышает удельный вес технических аспектов и приводит к необходимости определения требований к системам защиты, содержащим указанные средства.

Наиболее подходящим здесь оказывается подход, основанный на выделении некоторого количества типовых систем защиты, рекомендуемых для использования в тех или иных конкретных условиях и содержащих определенные механизмы защиты, т.е. подход, базирующийся на создании системы стандартов в области защиты информации.

Основу такой системы, действующей в настоящее время в Российской Федерации составляют руководящие документы, разработанные Гостехкомиссией России в начале 90-х годов и дополненные впоследствии рядом нормативных актов. Эти документы были созданы в результате исследований и практической деятельности в данной области министерств оборонных отраслей промышленности и министерства обороны СССР, и с учетом «Критериев оценки доверенных компьютерных систем» министерства обороны США, которые достаточно широко известны под названием «Оранжевая книга», и которые вместе с Европейскими и Канадскими критериями легли в последнее время в основу «Общих критериев» (стандарта ISO 15408-99 «Критерии оценки безопасности информационных технологий»).

К указанным документам Гостехкомиссии России относятся:

- руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», 1992 г.;
- руководящий документ «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», 1992 г.;
- руководящий документ «Защита от несанкционированного доступа к информации. Термины и определения», 1992 г.;
- руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показа-

тели защищенности от несанкционированного доступа к информации», 1992 г.;

- руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992 г.;

- руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1997 г.;

- руководящий документ «Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», 1998 г.;

- руководящий документ «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации», 1998 г.

Одновременно Россия использует ряд международных стандартов, принятых в качестве прямого заимствования и ориентированных на обеспечение информационной безопасности при взаимодействии открытых систем.

Кроме того, имеются стандарты, касающиеся защиты информации от ее утечки через побочные электромагнитные излучения и наводки (ПЭМИН).

Если не касаться вопросов криптографии и защиты информации от ее утечки через ПЭМИН, которые решаются во всех странах на национальном уровне, общие вопросы обеспечения безопасности информационных технологий развиваются во всех странах параллельно, а в последние годы совместно. Основу обеспечения безопасности информационных технологий составляет решение трех задач: обеспечение секретности (конфиденциальности), обеспечение целостности и обеспечение доступности. Эта основа заложена в стандартах, касающихся обеспечения безопасности информационных технологий, практически всех стран.

Во всех перечисленных выше документах Гостехкомиссии России используется методологический подход, принятый в свое время при разработке «Оранжевой книги». В последней, в частности, предусмотрено шесть фундаментальных требований, которым должны удовлетворять вычислительные системы, использующиеся

для обработки конфиденциальной информации. Эти требования касаются стратегии защиты, подотчетности, а также гарантий защиты.

Из других разработок, основанных на этом же подходе, могут быть также названы предложения министерства торговли и национального бюро стандартов США, министерства промышленности Великобритании и некоторые другие.

Аналогичный подход реализован и в упоминавшихся выше «Общих критериях». Анализ этого международного стандарта, проведенный российскими специалистами, свидетельствует о том, что он полностью соответствует по сути сложившейся в России методологии защиты информации от НСД. Однако по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости «Общие критерии» несколько превосходят Российские стандарты.

4.2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты

Наличие рассмотренных выше методик определения требований по защите информации и закрепление их в официальных документах создают достаточно надежную базу для решения практических проблем защиты. Однако нетрудно видеть, что с точки зрения современной постановки задачи защиты информации все они являются недостаточными по ряду причин, а именно:

1) методики ориентированы на защиту информации только в средствах вычислительной техники и практически не затрагивают объектовый, а тем более региональный уровень обеспечения информационной безопасности;

2) в используемых подходах учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации;

3) в научном плане методики обоснованы недостаточно (за исключением требований к защите информации от утечки по техническим каналам).

Возможные подходы к преодолению указанных недостатков были предложены в монографии В.А. Герасименко [3] и развиты в дальнейшем авторским коллективом учебника «Основы защиты информации» [31]. Учитывая их принципиальное значение для совершенствования стандартов и методических документов в условиях современной постановки задачи защиты информации, представляется целесообразным рассмотреть эти подходы более под-

робно и на страницах данного учебного пособия, тем более что за прошедшее время они были уточнены и приближены к потребностям практики.

Рассмотрим предварительно подходы к оценке параметров защищаемой информации, что, позволит нам в дальнейшем обоснованно подойти к классификации возможных ситуаций защиты.

Информацию в общем случае можно рассматривать в двух аспектах - как ресурс, обеспечивающий ту или иную деятельность общества и как объект труда, над которым производятся определенные действия в целях информационного обеспечения решаемых задач.

Показатели, оценивающие информацию как ресурс, определяются ее значимостью для решения конкретной задачи, а также полнотой и адекватностью имеющихся сведений. Кроме того, важное значение имеет релевантность информации, иными словами ее засоренность ненужными данными, и толерантность, т.е. форма представления информации с точки зрения удобства восприятия и использования ее в процессе решения задач.

Таким образом, для оценки информации как обеспечивающего ресурса можно использовать следующие показатели: важность; полнота, адекватность, релевантность, толерантность.

Как объект труда информация выступает, во-первых, как сырье, добываемое и поступающее на обработку, во-вторых, как полуфабрикат, образуемый в процессе обработки, и, в-третьих, как продукт обработки, выдаваемый для использования. Для обработки информации используются различные средства, основными из которых являются средства фиксации, передачи и переработки. С точки зрения использования этих средств основными характеристиками должны быть форма (способ) представления и объемы информации безотносительно к ее смысловому содержанию.

Заметим еще, что в условиях потенциальной возможности проявления большого количества информационных угроз, которые могут оказать негативное воздействие на информацию, естественно приходится принимать меры противодействия дестабилизирующем факторам. При этом важность информации должна рассматриваться уже не только в смысле значимости ее для решаемых задач, но и в смысле организации процесса ее обработки. Таким образом, важность информации имеет значение как при оценке ее в качестве обеспечивающего ресурса, так и в качестве объекта труда.

Рассмотрим возможные подходы к определению значений перечисленных показателей.

Важность информации. В соответствии с изложенным выше, важность информации должна оцениваться по двум группам критериев - по назначению информации и по условиям ее обработки.

В первой группе, очевидно, следует выделить две составляющие - важность задач для обеспечиваемой деятельности и степень важности информации для эффективного решения соответствующих задач.

Во второй группе также выделим две составляющих - уровень потерь в случае реализации угроз безопасности информации и уровень затрат на восстановление измененной информации.

Обозначим:

K_{VI} - коэффициент важности информации; .

K_{B3} - коэффициент важности задач, для обеспечения решения которых используется информация;

K_{IZ} - коэффициент важности информации для эффективного решения задач;

K_{PI} - коэффициент важности информации с точки зрения потерь при снижении ее качества;

K_{CB} - коэффициент важности информации с точки зрения стоимости восстановления ее качества.

Тогда, очевидно:

$$K_{VI} = f(K_{B3}, K_{IZ}, K_{PI}, K_{CB}). \quad (4.2)$$

Иными словами, для оценки важности информации необходимо уметь определять значения перечисленных выше коэффициентов и знать вид функциональной зависимости (4.2). Однако, как и для большинства задач, связанных с проблемой защиты информации, здесь также не удается предложить каких-либо формальных приемов решения. Поэтому мы вынуждены снова основываться на рассматривавшихся выше неформально-эвристических методах.

В данном случае значения входящих в формулу (4.2) критериев будем выражать лингвистическими переменными так, как это показано на рис. 4.1.

Затем сформируем возможные комбинации критериев в пределах каждой группы (табл. 4.1). Если теперь свести воедино полученные результаты, то можно сформировать итоговую классификацию информации по важности (табл. 4.2). При этом нами сделано предположение, что диагональные элементы классификационной структуры являются одинаково важными.

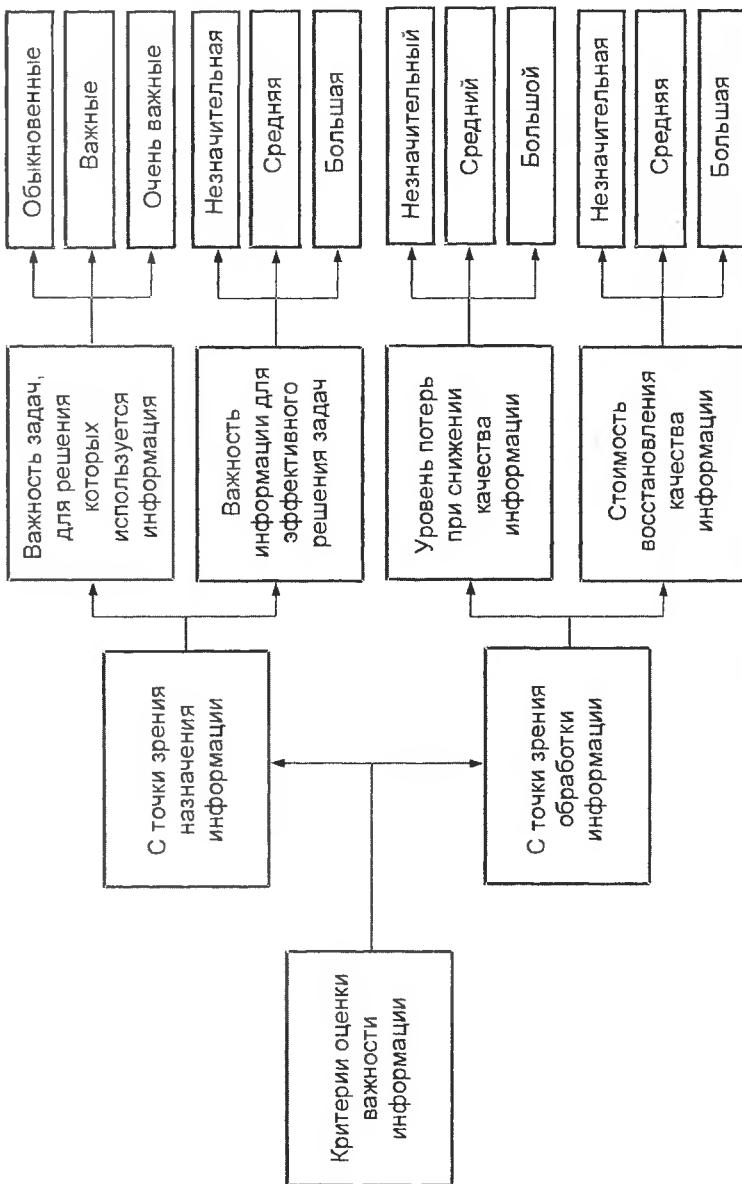


Рис. 4.1. Структура и значения критериев оценки важности информации

Требования к защите информации

Таблица 4.1а

Первичная классификация информации по важности относительно назначения

Важность задачи	Важность информации для задачи		
	Незначительная	Средняя	Большая
Обыкновенная	1н	2н	3н
Важная	4н	5н	6н
Очень важная	7н	8н	9н

Таблица 4.16

Первичная классификация информации по важности относительно обработки

Уровень потерь	Стоимость восстановления		
	Незначительная	Средняя	Большая
Незначительный	1о	2о	3о
Средний	4о	5о	6о
Большой	7о	8о	9о

Таким образом, вся информация может быть разделена на семнадцать классов важности. Однако номер класса сам по себе не характеризует важность информации на содержательном уровне, да и оперировать семнадцатью различными классами затруднительно. Улучшить положение можно объединив все элементы классификационной структуры так, как показано в табл. 4.2 пунктирными линиями. В итоге семнадцать классов будут преобразованы в семь категорий важности: малой (А), обычновенной (Б), полусредней (В), средней (Г), повышенной (Д), большой (Е) и чрезвычайной важности (Ж).

Далее для проведения аналитических расчетов необходимо получить количественные выражения введенных показателей важности. При этом естественно предположить, что важность информации категории А убывает от класса 3 к классу 1, приближаясь к 0, а категории Ж возрастает от класса 15 к классу 17, приближаясь к 1. Естественно также предположить, что возрастание важности информации от класса 1 к классу 17 происходит неравномерно, причем наиболее адекватной, видимо, будет зависимость в виде логистической кривой (рис. 4.2).

Таблица 4.2.

Итоговая классификация информации по важности

		Относительного обработки										
		10	20	30	40	50	60	70	80	90		
Важность информации	1н	1	2	3	4	5	6	7	8	9		
	2н	2	3	4	5	6	7	8	9	10		D
	3н	3									11	E
	4н	4									12	
	5н	5									13	
	6н	6									14	
	7н	7									15	
	8н	8									16	
	9н	9	10	11	12	13	14	15	16	17		J

Теперь мы имеем все необходимое для определения показателя важности информации. Последовательность и содержание такой оценки приведены на рис. 4.3.

Полнота информации. Полнота представляет собой показатель, характеризующий достаточность информации для решения соответствующих задач. Поэтому, чтобы иметь возможность определять данный показатель, необходимо для каждой задачи или группы задач заблаговременно составить перечень сведений, которые требуются для их решения. Для представления таких сведений удобно воспользоваться так называемыми объектно-характеристическими таблицами (ОХТ). ОХТ - это двухмерная матрица, по строкам которой приведен перечень наименований объектов, процессов или явлений, входящих в круг интересов соответствующей задачи, а по столбцам - наименования их характеристик (параметров), необходимых для решения задачи.

Требования к защите информации

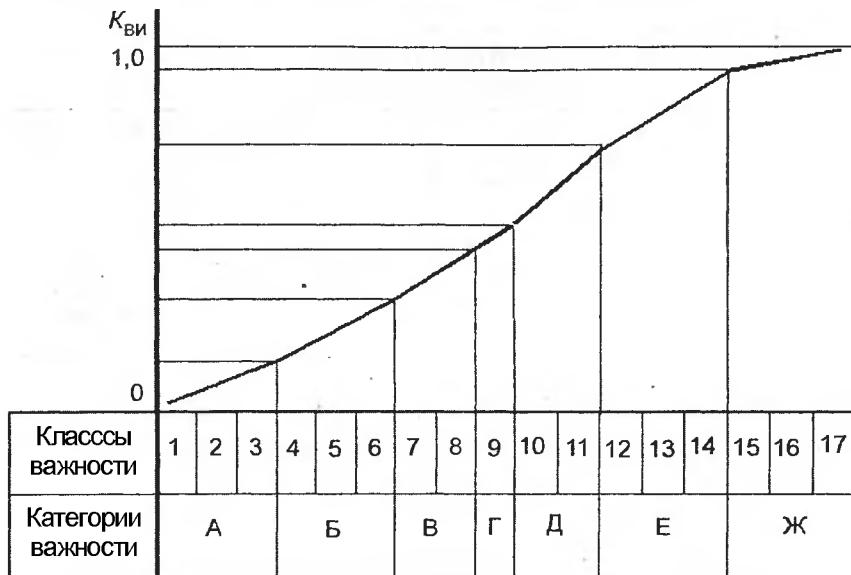


Рис. 4.2. Коэффициент важности информации

Значения характеристики при этом будут располагаться на пересечении соответствующих строк и столбцов. Совокупность всех ОХТ, необходимых для обеспечения решения всех задач объекта, может быть названа его информационным кадастром [5].

Рассмотрим возможную методику оценки полноты информации.

Обозначим через $d_{\mu v}$ элемент, находящийся в μ -й строке и v -м столбце интересующего нас компонента соответствующей ОХТ, причем:

$$d_{\mu v} = \begin{cases} 1, & \text{если по данному элементу информация имеется;} \\ 0, & \text{в противном случае.} \end{cases}$$

Тогда в качестве коэффициента полноты информации в данной ОХТ можно принять величину:

$$K_{\Pi} = \frac{\sum_{\mu} \sum_{v} d_{\mu v}}{mn}, \quad (4.3)$$

где m - число строк, а n - число столбцов ОХТ.



Рис. 4.3. Последовательность и содержание оценки важности информации

Однако при этом не учитывается важность (значимость) различных элементов. В целях устранения этого недостатка положим, что $K_{\mu\nu}^{(e)}$ есть коэффициент важности элемента μ -й строки и v -го столбца. Тогда, очевидно, в качестве меры взвешенной полноты информации в рассматриваемой ОХТ можно принять величину:

$$K_{\Pi}^{(e)} = \frac{\sum_{\mu} \sum_{v} d_{\mu v}}{mn \sum_{\mu} \sum_{v} K_{\mu v}^{(e)}}. \quad (4.4)$$

Адекватность информации. Под адекватностью традиционно понимается степень соответствия оцениваемой информации действительному состоянию тех реалий, которые она отображает. В общем случае адекватность определяется двумя параметрами - объективностью генерирования информации и продолжительно-

Требования к защите информации

стью интервала времени между моментом генерирования и текущим моментом, т.е. моментом оценивания ее адекватности.

Объективность генерирования информации, очевидно, зависит от способа получения значений интересующих нас характеристик и качества его реализации.

Классификация характеристик по возможным способам получения их значений приведена на рис. 4.4. Используя эту классификацию все возможные значения адекватности информации по объективности ее генерирования можно структурировать так, как приведено в табл. 4.3.

Как и в случае оценки важности информации предположим, что при высоком качестве определения значения непосредственно и при том количественно измеряемой характеристики адекватность соответствующей информации будет близка к 1, а при низком качестве определения значения неизмеряемой характеристики, не имеющей даже отдаленного аналога, адекватность информации близка к нулю.

Естественно также предположить, что внутри данного интервала изменения адекватности происходит в соответствии с логистической кривой, как это показано на рис. 4.5.



Рис. 4.4. Классификация характеристик по способам получения их значений

Таблица 4.3

Структуризация значений адекватности информации по объективности генерирования

Тип характеристики			Качество определения значения характеристики		
			Хорошее	Среднее	Плохое
Измеряемая	Непосредственно	Количественно	1	2	3
		Качественно	2	3	4
	Косвенно	Аналитически	3	4	5
		Логически	4	5	6
Не измеряемая	Имеющая аналоги	В данной среде	5	6	7
		В сходной среде	6	7	8
	Не имеющая аналогов	Конкретного	7	8	9
		Даже отдаленного	8	9	10

Рассмотрим теперь, как изменяется адекватность информации в зависимости от продолжительности интервала времени между моментом генерирования и текущим моментом. Для оценки адекватности по данному параметру используем известный из теории информации закон старения информации. Его вид показан на рис. 4.6. При этом под t_0 понимается момент времени генерирования оцениваемой информации.

Как следует из рисунка, закон старения информации характеризуется четырьмя основными интервалами:

Δt_1 - продолжительностью интервала времени, в течение которого оцениваемая информация практически полностью сохраняет свою адекватность;

Δt_2 - продолжительностью интервала времени, в течение которого адекватность информации уменьшается не более чем на одну четверть;

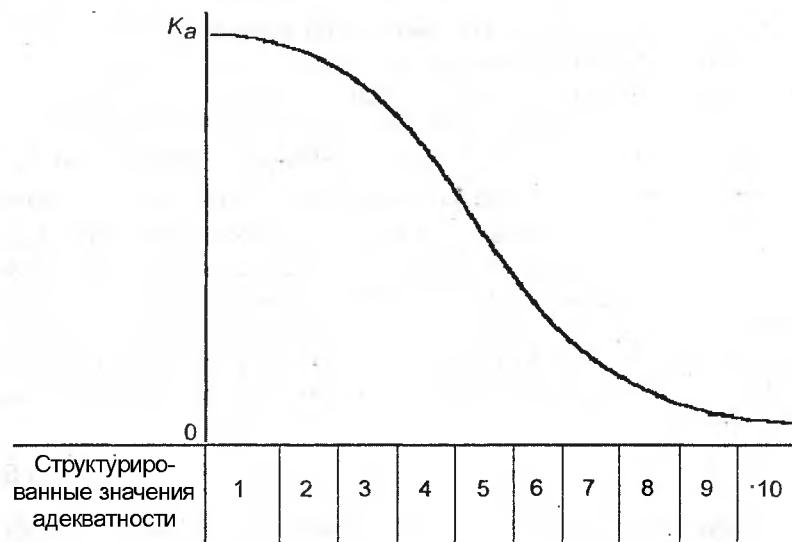


Рис. 4.5. Показатель адекватности информации по способу генерирования

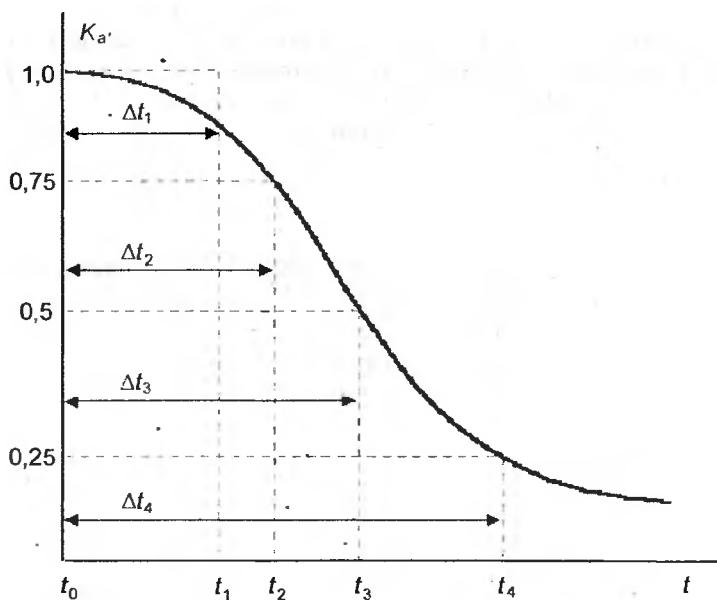


Рис. 4.6. Общий вид закона старения информации

Δt_3 - продолжительностью интервала времени, в течение которого адекватность информации уменьшается наполовину;

Δt_4 - продолжительностью интервала времени, в течение которого адекватность информации уменьшается на три четверти.

Учитывая, что обе составляющие адекватности информации K_a (в зависимости от способа генерирования) и $K_{a'}$ (в зависимости от момента оценивания) определяются большим числом факторов, многие из которых носят случайный характер, есть все основания утверждать, что они являются величинами случайными и поэтому могут интерпретироваться как вероятности того, что информация по соответствующему параметру является адекватной. В соответствии с этим общий показатель адекватности информации K_a может быть определен как:

$$K_a = K_a K_{a'} \quad .(4.5)$$

Независимость величин K_a и $K_{a'}$ при этом представляется вполне естественной.

Релевантность информации. Релевантность характеризует соответствие информации потребностям решаемой задачи. Для количественного выражения данного показателя обычно используют так называемый коэффициент релевантности K_p , определяющий отношение объема релевантной информации N_p к общему объему анализируемой информации N_0 :

$$K_p = \frac{N_p}{N_0} \quad .(4.6)$$

К оценке релевантности информации в таком представлении можно подойти следующим образом. Пусть имеется информационный кадастр, состоящий из некоторого количества ОХТ. Тогда релевантность η -й ОХТ можно выразить формулой:

$$K_p^\eta = \frac{\sum_{\mu} \sum_{v} d_{\mu v \eta}^{(\rho)}}{m_\eta n_\eta} \quad , (4.7)$$

где

$$d_{\mu v \eta}^{(\rho)} = \begin{cases} 1, & \text{если элемент } d_{\mu v \eta} \text{-й ОХТ соответствует решаемой задаче;} \\ 0, & \text{в противном случае;} \end{cases}$$

или с учетом коэффициентов важности элементов ОХТ:

$$K_p^\eta = \frac{\sum_{\mu} \sum_{\nu} d_{\mu\nu\eta}^{(p)} K_{\mu\nu\eta}^{(e)}}{m_\eta n_\eta \sum_{\mu} \sum_{\nu} K_{\mu\nu\eta}^{(e)}}. \quad (4.8)$$

Коэффициент релевантности всего информационного кадастра, очевидно, может быть выражен формулой:

$$K_p = \frac{\sum_{\mu} \sum_{\nu} d_{\mu\nu\eta}^{(p)}}{\sum_{\mu} \sum_{\nu} m_\eta n_\eta}, \quad (4.9)$$

или с учетом коэффициентов важности элементов ОХТ:

$$K_p^\eta = \frac{\sum_{\eta} \sum_{\mu} \sum_{\nu} d_{\mu\nu\eta}^{(p)} K_{\mu\nu\eta}^{(e)}}{\sum_{\eta} m_\eta n_\eta \sum_{\mu} \sum_{\nu} K_{\mu\nu\eta}^{(e)}}. \quad (4.10)$$

Толерантность информации. Толерантность, как отмечалось выше, есть показатель, характеризующий удобство восприятия и использования информации в процессе решения задачи. Уже из самого определения видно, что понятие толерантности является очень широким, в значительной мере неопределенным и субъективным. Даже для цифровой информации значение толерантности может быть самым различным. Поэтому вряд ли можно надеяться на разработку строго формальной методики определения показателя толерантности. Из эвристических методов наиболее подходящими здесь представляются методы экспертно-лингвистических оценок. При этом в качестве значений лингвистической переменной могут быть использованы такие понятия, как: «весома удобно, комфортно» (информация представлена в таком виде, что ее использование в процессе решения задачи происходит естественным образом, не требуя дополнительных усилий), «удобно» (использование информации если и требует дополнительных усилий, то лишь незначительных), «средне» (использование информации требует дополнительных усилий, вообще говоря, допустимых), «плохо» (использование информации сопряжено с

большими трудностями), «очень плохо» (использование информации или вообще невозможно, или требует неоправданно больших усилий).

Показатели, оценивающие информацию как объект труда.

Как было определено выше, основными показателями этого вида могут быть эффективность кодирования и объем информации. Поскольку методы определения данных показателей достаточно полно разработаны в теории информации, то специально на них останавливаться нет необходимости.

Требуемый уровень защиты информации должен определяться с учетом значений всех рассмотренных выше показателей. Методика такого определения может базироваться на следующей полуэвристической процедуре:

1) все показатели информации делятся на три категории: определяющие, существенные и второстепенные, причем основным критерием такого деления должна служить цель, для достижения которой осуществляется защита информации;

2) требуемый уровень защиты определяется по значениям определяющих показателей информации;

3) выбранный уровень при необходимости может быть скорректирован с учетом значения существенных показателей. Значения второстепенных показателей при этом могут игнорироваться.

Возможный вариант классификации показателей информации в зависимости от целей защиты, полученный с помощью экспертных оценок, приведен в табл. 4.4.

Естественно, что требуемый уровень защиты информации в конкретных условиях существенно зависит от учета факторов, которые влияют на защиту. Таким образом, формирование возможно более полного множества этих факторов и возможно более адекватное определение степени их влияния на требуемый уровень защиты представляется на сегодня одной из наиболее актуальных задач.

Сформулированная задача, однако, так же, как и практически все описанные нами ранее задачи, не может быть решена с помощью традиционных формальных методов. Если бы мы располагали достаточным объемом статистических данных о функционировании различных систем и механизмов защиты информации, то, вообще говоря, данную задачу можно было бы решить статистической обработкой этих данных, по крайней мере, по некоторому полуэвристическому алгоритму. Но таких данных либо вообще нет, либо они оказываются далеко не полными, а достоверность их вызывает серьезные сомнения. В силу сказанного в настоящее время для указанных целей можно воспользоваться лишь

Требования к защите информации

рассмотренными в гл. 2 неформально-эвристическими методами, т.е. методами, основанными на широком привлечении знаний, опыта и интуиции компетентных и заинтересованных специалистов.

Ниже излагаются возможные подходы к решению рассматриваемой задачи названными методами.

Нетрудно видеть, что поставленная задача довольно четко может быть разделена на две подзадачи - формирование возможно более полного и хорошо структурированного множества факторов, существенно значимых с точки зрения защиты информации, и определение показателей значимости (весов) факторов. Анализируя содержание этих подзадач и существование рассмотренных в гл. 2 неформально-эвристических методов, нетрудно заключить, что для решения первой из них наиболее эффективным представляется сочетание алгоритма автоформализации знаний и метода психоинтеллектуальной генерации, а второй - комбинация известных методов экспертных оценок.

Таблица 4.4.

Классификация значений показателей информации в зависимости от целей защиты

Показатель информации	Вид сохраняемой тайны			Защита информации как товара
	государственная	промышленная, коммерческая	конфиденциальная	
Важность	Определяющее	Определяющее	Определяющее	Определяющее
Адекватность	Существенное	Существенное	Существенное	Определяющее
Релевантность	Второстепенное	Существенное	Существенное	Определяющее
Тolerантность	Второстепенное	Существенное	Второстепенное	Существенное
Способ кодирования	Второстепенное	Второстепенное	Второстепенное	Существенное
Объем	Второстепенное	Существенное	Существенное	Определяющее

Основным в решении первой подзадачи в этом случае является разработка так называемой психо-эвристической программы (ПЭП), представляющей собой перечень и последовательность (общий алгоритм) обсуждения вопросов, составляющих существо рассматриваемой проблемы, развернутую схему и методические указания, обеспечивающие целенаправленное обсуждение каждого вопроса.

При разработке ПЭП для обоснования множества факторов, влияющих на требуемый уровень защиты информации, следует учитывать их исключительно большое количество и разноплановый характер. Поэтому представляется целесообразным разделить все факторы на некоторое число групп. Тогда задачу формирования возможно более полного множества факторов можно решать по трехшаговой процедуре: первый шаг - формирование перечня групп факторов, второй - формирование перечня факторов в каждой из выделенных групп, третий - структуризация возможных значений факторов. Общая схема ПЭП для решения рассматриваемой задачи по этой процедуре представлена на рис. 4.7.

Первоначальное формирование перечня групп факторов может осуществляться двояко в зависимости от того, сформирован он предварительно (на основе процедуры автоформализации знаний) или нет. В первом случае обсуждение должно вестись в целях обоснования содержания и возможной корректировки перечня, во втором - формирования перечня и затем уже его обоснования и уточнения. На рис. 4.8 приведена развернутая схема обсуждения применительно к первому случаю.

Сформированное по указанной методологии множество факторов включает следующие пять групп.

Группа 1 - факторы, обусловливаемые характером обрабатываемой информации:

- 1.1. степень конфиденциальности;
- 1.2. объемы;
- 1.3. интенсивность обработки.

Группа 2 - факторы, обусловливаемые архитектурой системы:

- 2.1. геометрические размеры системы;
- 2.2. территориальная распределенность системы;
- 2.3. структурированность компонентов системы.

Группа 3 - факторы, обусловливаемые условиями функционирования системы:

- 3.1. расположение в населенном пункте;
- 3.2. расположение на территории объекта;
- 3.3. обустроенностъ.

Требования к защите информации

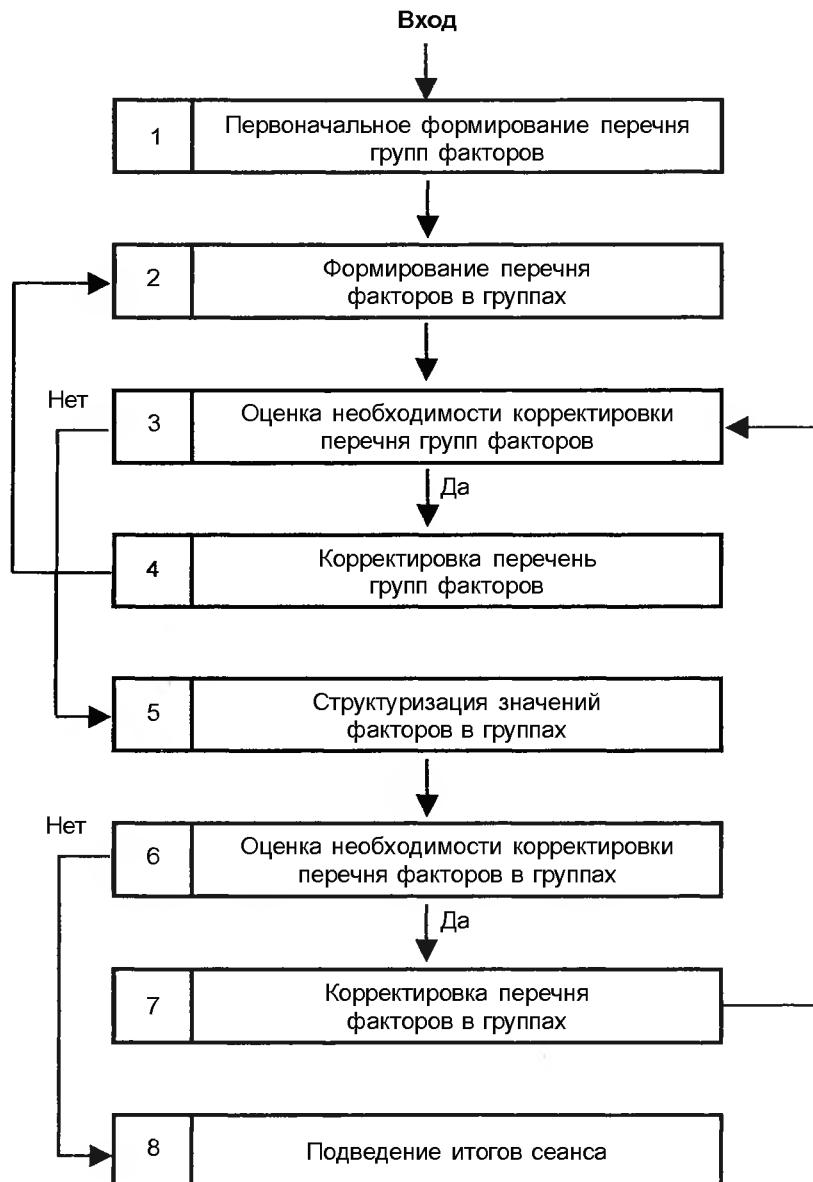
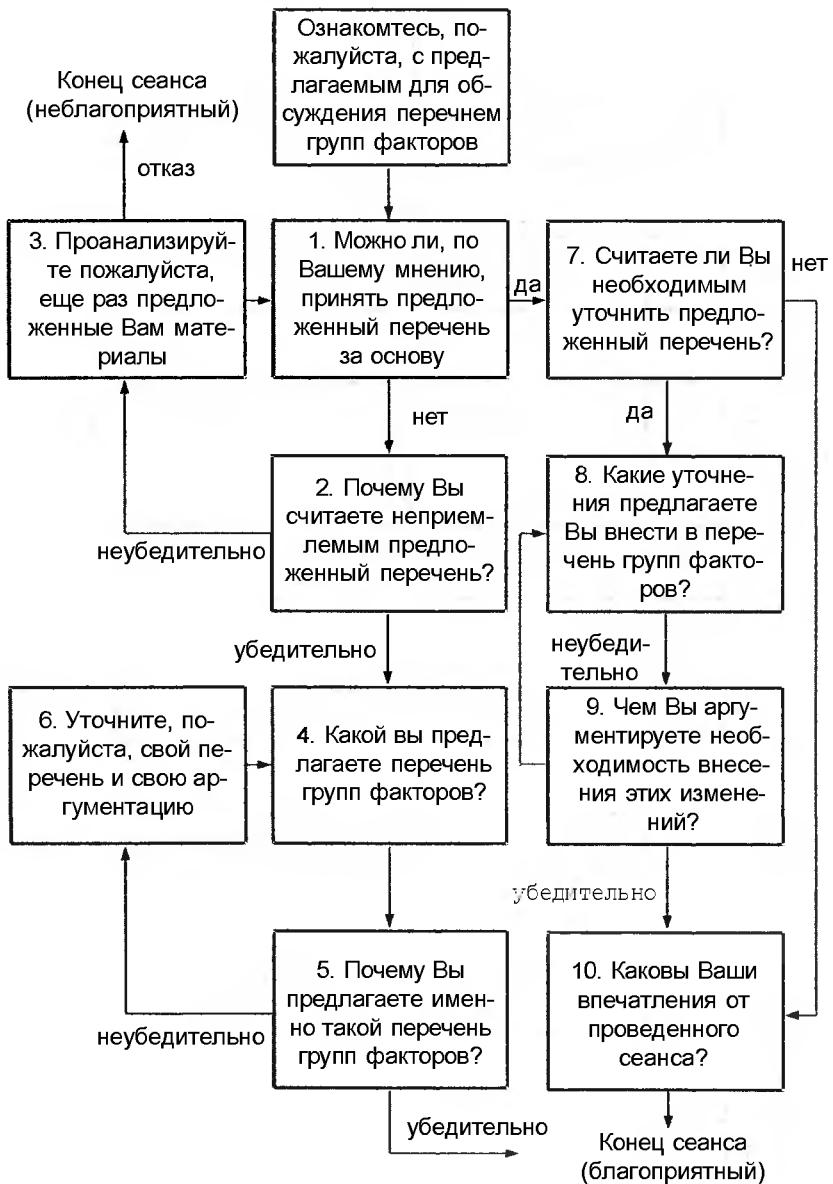


Рис. 4.7. Общая структура программы формирования перечня факторов, влияющих на требуемый уровень защиты информации



Требования к защите информации

Группа 4 - факторы, обусловливаемые технологией обработки информации:

- 4.1. масштаб обработки;
- 4.2. стабильность информации;
- 4.3. доступность информации;
- 4.4. структурированность информации.

Группа 5 - факторы, обусловливаемые организацией работы с информацией:

- 5.1. общая постановка дела;
- 5.2. укомплектованность кадрами;
- 5.3. уровень подготовки и воспитания кадров;
- 5.4. уровень дисциплины.

Значения всех указанных факторов, выраженные в лингвистических переменных, приведены в табл. 4.5.

Таблица 4.5.

Значения факторов, влияющих на требуемый уровень защиты информации

Наименование группы факторов	Наименование факторов	Значение факторов
1. Обусловливаемые характером обрабатываемой информации	1.1. Степень конфиденциальности	1. Очень высокая 2. Высокая 3. Средняя 4. Невысокая
	1.2. Объемы	1. Очень большие 2. Большие 3. Средние 4. Малые
	1.3. Интенсивность обработки	1. Очень высокая 2. Высокая 3. Средняя 4. Низкая
2. Обусловливаемые архитектурой системы	2.1. Геометрические размеры системы	1. Очень большие 2. Большие 3. Средние 4. Незначительные
	2.2. Территориальная распределенность системы	1. Очень большая 2. Большая 3. Средняя 4. Незначительная

Глава 4

Наименование группы факторов	Наименование факторов	Значение факторов
2. Обусловливаемые архитектурой системы	2.3. Структурированность компонентов системы	1. Полностью отсутствует 2. Частичная 3. Достаточно высокая 4. Полная
3. Обусловливаемые условиями функционирования системы	3. 1. Расположение в населенном пункте	1. Очень неудобное 2. Создает значительные трудности для защиты 3. Создает определенные трудности для защиты 4. Очень хорошее
	3.2. Расположение на территории объекта	1. Хаотично разбросанное 2. Разбросанное 3. Распределенное 4. Компактное
	3.3. Обустроенностъ	1. Очень плохая 2. Плохая 3. Средняя 4. Хорошая
4. Обусловливаемые технологией обработки информации	4.1. Масштаб обработки	1. Очень большой 2. Большой 3. Средний 4. Незначительный
	4.2. Стабильность информации	1. Отсутствует 2. Частично стабильная 3. Достаточно упорядоченная 4. Регулярная
	4.3. Доступность информации	1. Общедоступная 2. С незначительными ограничениями на доступ 3. С существенными ограничениями на доступ 4. С полным регулируемым доступом
	4.4. Структурированность информации	1. Полностью отсутствует 2. Частичная 3. Достаточно высокая 4. Полная

Требования к защите информации

Наименование группы факторов	Наименование факторов	Значение факторов
5. Обусловливаемые организацией работы с информацией	5.1. Общая постановка дела	1. Очень плохая 2. Плохая 3. Средняя 4. Хорошая
	5.2. Укомплектованность кадрами	1. Очень слабая 2. Слабая 3. Средняя 4. Полная
	5.3. Уровень подготовки и воспитания кадров	1. Очень низкий 2. Низкий 3. Средний 4. Высокий
	5.4. Уровень дисциплины	1. Очень низкий 2. Низкий 3. Средний 4. Высокий

Нетрудно видеть, что они сведены в некоторую унифицированную схему и расположены так, что на первом месте находятся значения, предопределяющие наиболее высокие требования к защите информации, а на четвертом - наиболее низкие требования.

Таким образом, всего выделено 17 факторов, каждый из которых может принимать одно из четырех значений. В этом случае общее число различных вариантов потенциально возможных условий защиты, как показывают расчеты, превысит $1,7 \times 10^{10}$, т. е. составит число астрономического порядка.

В общем случае для каждого из потенциально возможных вариантов условий должны быть определены свои требования к защите информации, что при таком количестве вариантов практически невозможно. Следовательно, необходимо разделить все множество возможных вариантов на некоторое (сравнительно небольшое) число классов, в рамках каждого из которых все входящие в него варианты с точки зрения требований к защите должны считаться идентичными. Указанная классификация сопряжена с решением комбинаторной задачи весьма большой размерности и с высоким уровнем неопределенности. Возможные подходы к ее решению рассматриваются в следующих параграфах данной главы.

4.3. Определение весов вариантов потенциально возможных условий защиты информации

Выше мы установили, что конечная цель анализа факторов, влияющих на требуемый уровень защиты информации, заключается в делении всего множества вариантов потенциально возможных условий защиты на некоторое (желательно как можно меньшее) число классов, каждый из которых будет объединять варианты, близкие по требованиям к защите. Для практической реализации такой классификации необходим показатель, количественно характеризующий относительные важности вариантов условий с точки зрения требований к защите.

В сформированной в предыдущем параграфе классификационной структуре факторов выделено три уровня: группа факторов, факторы в пределах группы, значения факторов. Если теперь обозначить:

R_i - вес i -й группы факторов в общем перечне групп;

Q_{ij} - вес j -го фактора в i -й группе;

S_{ijk} - вес k -го значения j -го фактора в i -й группе,

то вес m -го варианта условий защиты $W_m(i,j,k)$, очевидно, выражится функцией:

$$W_m(i,j,k) = f(R_i, Q_{ij}, S_{ijk}). \quad (4.11)$$

Отсюда следует, что решение сформулированной задачи сводится к определению величин R_i , Q_{ij} , S_{ijk} и вида функциональной зависимости (4.11).

Мы уже отмечали, что для определения значений перечисленных выше величин целесообразнее всего использовать методы экспертных оценок. Анализ сущности рассматриваемых величин позволяет утверждать, что для их определения могут быть использованы практически все известные разновидности экспертных оценок. Рассмотрим, например, использование здесь метода парных сравнений.

Данная разновидность экспертных оценок заключается в том, что каждый из экспертов оценивает объекты, события, параметры путем присвоения каждой паре из них коэффициента превосходства одного элемента пары над другим. При этом, естественно, предполагается, что если K_{ab} есть коэффициент превосходства объекта A над объектом B , то K_{ba} (коэффициент превосходства объекта B над объектом A) выражается величиной $1/K_{ab}$.

На рис. 4.9 приведен пример заполненной экспертом соответствующей анкеты, причем справа от таблицы приведены возможные значения коэффициентов предпочтения и их смысловое содержание, а в табл. 4.6 - сводные данные об оценках групп факторов коллективом из 21 эксперта. Обработка приведенных результатов дает значения, показанные в крайней правой колонке табл. 4.6.

Рассмотрим далее вопрос о виде функциональной зависимости (4.11). Наиболее простой и в то же время часто используемой функцией в подобных ситуациях является произведение составляющих коэффициентов при условии, что они нормированы по одной шкале. Поскольку величины R_i , Q_{ij} , S_{ijk} нормированы по шкале 0-1, то тогда

$$W_m(i,j,k) = R_i(m) \cdot Q_{ij}(m) \cdot S_{ijk}(m), \quad (4.12)$$

а чтобы и величины $W_m(i,j,k)$ были нормированы в той же шкале, можно воспользоваться зависимостью:

$$W_m(i, j, k) = \frac{R_i(m) \cdot Q_{ij}(m) \cdot S_{ijk}(m)}{\sum_m R_i(m) \cdot Q_{ij}(m) \cdot S_{ijk}(m)}. \quad (4.13)$$

Однако в предыдущем параграфе было показано, что общее количество потенциально возможных вариантов условий защиты выражается числом астрономического порядка, и осуществить вычисления по этой зависимости практически невозможно.

Возможные выходы из этого положения рассмотрены в следующем параграфе.

4.4. Методы деления поля значений факторов на типовые классы

В предыдущих параграфах ситуация защиты структурирована нами до формирования множества потенциально возможных вариантов сочетаний значений факторов и разработки методики оценки значимости вариантов. Следующая задача заключается в рациональном делении множества возможных вариантов на классы таким образом, чтобы в пределах каждого класса находились однородные в определенном смысле варианты. При этом однородность вариантов класса определяется главным образом возможностью предъявления единых требований по защите информации ко всем вариантам соответствующего класса. Нетрудно видеть, что сформулированная выше задача иначе может быть названа задачей

Глава 4

Группа факторов		Номера групп факторов					Шкала относительной важности	
№	Наименование	1	2	3	4	5	Σ	
1	Характер обрабатываемой информации	5	7	6	7	25	1 3 5 7 9	равнная важность умеренное превосходство одной группы над другой существенное превосходство значительное превосходство очень сильное превосходство
2	Архитектура системы	1/5		3	2	4	9 _{1/5}	2, 4, 6, 8 промежуточные значения
3	Условия функционирования системы	1/7	1/3		2	1	3 _{10/21}	
4	Технология обработки информации	1/6	1/2	1/2		3	4 _{1/6}	
5	Организация работы с информацией	1/7	1/4	1	1/3		11 _{14/84}	Эксперт: Белов

Рис. 4.9. Анкета экспертизы по методу парных сравнений

Таблица 4.6.

Сводные данные экспертной оценки важности групп факторов группой из 21 эксперта

№ групп факторов	Эксперты										
	1	2	3	4	5	6	7	8	9	10	11
1	25	10,3	21	15	22	22	22	9	4	21	26
2	9,2	7,5	8,1	5,6	15,5	15,5	15,5	1,4	1,2	7,4	3,6
3	3,5	1,9	3,5	3,6	3,3	3,3	3,3	2,9	8,5	0,8	9,7
4	4,2	18	2,2	5,3	5,8	5,8	5,8	8	13	3,7	0,8
5	1,2	2,7	2,5	3,5	3,8	3,8	3,8	11	7,3	17,3	12,2
→	12	13	14	15	16	17	18	19	20	21	R_i
1	24	7	12	13	17	20	1,1	0,6	16	14	15,33
2	2,3	0,8	2,5	13	15	1,3	13	22	7,7	0,9	8,05
3	2,3	5,4	6,	0,8	3,9	1,5	3,2	3,8	3,9	1,2	3,59
4	2,3	17	8,7	3,8	8	11,3	8,5	7,7	1	8,7	7,11
5	15,3	23	8,3	13	6,5	11,3	7,5	17,3	14	14	8,73

формирования необходимого и достаточного набора типовых систем защиты информации (СЗИ), который удовлетворял бы требованиям к защите информации при любом потенциально возможном варианте значений факторов. Естественно, что число типовых СЗИ должно быть возможно меньшим.

Можно выделить три возможных подхода к решению этой задачи: *теоретический, эмпирический и комбинированный*, т.е. *теоретико-эмпирический*. Рассмотрим основные положения этих подходов.

Теоретический подход. Наиболее общим методом деления элементов множества на классы является так называемый кластерный анализ, который определяется как классификация объектов по осмысленным, т.е. соответствующим четко сформулированным целям группам. Основная суть кластерного анализа заключается в том, что элементы множества делятся на классы в соответствии с некоторой мерой сходства между различными элементами.

Процедура кластеризации в общем виде может быть представлена последовательностью следующих шагов:

Глава 4

- 1) формирование множества элементов, подлежащих делению на классы;
- 2) определение множества признаков, по которым должны оцениваться элементы множества;
- 3) определение меры сходства между элементами множества;
- 4) деление элементов множества на классы;
- 5) проверка соответствия полученного решения поставленным целям.

Нетрудно видеть, что применительно к рассматриваемой здесь задаче первые два шага нами уже сделаны выше. Рассмотрим возможные подходы к осуществлению следующих шагов приведенной процедуры.

Третий шаг заключается в определении меры сходства между элементами классифицируемого множества. Нет необходимости доказывать, что выбором меры сходства элементов в решающей степени определяется результат классификации, его соответствие поставленным целям, поэтому данный шаг считается центральным.

В теоретическом плане решение этой задачи заключается в формировании соответствующей метрики, т.е. представление элементов множества точками некоторого координатного пространства, в котором различие и сходство элементов определяются метрическим расстоянием между соответствующими элементами. Любая метрика должна удовлетворять совокупности следующих условий:

- 1) симметричности:

$$d(x, y) = d(y, x) \geq 0,$$

где x и y - различные элементы множества, $d(x, y)$ - расстояние между элементами x и y ;

- 2) неравенства треугольника:

$$d(x, y) \geq d(x, z) + d(y, z),$$

где x, y, z - различные элементы множества;

- 3) различимости неидентичных элементов:

$$d(x, y) \neq 0,$$

где x, y - неидентичные элементы;

- 4) неразличимости идентичных элементов:

$$d(x, x) = 0,$$

где x и x' - идентичные элементы.

Нетрудно показать, что введенный в предыдущем параграфе показатель важности варианта условий W_m отвечает всем приведенным выше условиям метрики.

Что касается самого значения меры сходства, то наибольшее распространение получили коэффициент корреляции, расстояние и коэффициент ассоциативности.

Коэффициент корреляции между элементами с номерами j и k (r_{jk}) вычисляется по следующей зависимости:

$$r_{jk} = \frac{\sum_{i=1}^n (x_{ij} - \bar{x}_j)(x_{ik} - \bar{x}_k)}{\sqrt{\sum_{i=1}^n (x_{ij} - \bar{x}_j)^2 \sum_{i=1}^n (x_{ik} - \bar{x}_k)^2}}, \quad (4.14)$$

где x_{ij} и x_{ik} - значения i -й переменной для элементов j и k соответственно, \bar{x}_j и \bar{x}_k - среднее всех значений соответствующих элементов, n - число элементов.

Под расстоянием d_{ij} как мерой сходства понимаются величины

$$d_{ij} = \sqrt{\sum_{i=1}^n (x_{ik} - x_{jk})^2}, \quad (4.15)$$

или

$$d_{ij} = \sum_{k=1}^p |x_{ik} - x_{jk}|, \quad (4.16)$$

где x_{ik} и x_{jk} - значения k -й переменной для i -го и j -го элементов соответственно; p - число переменных в оценке элементов.

Коэффициент ассоциативности (S) используется для оценки меры сходства элементов, описываемых бинарными переменными. Вычисляется он по зависимости:

$$S_{ij} = \frac{(a + d)}{(a + b + c + d)} \quad (4.17)$$

причем значения входящих в нее величин берутся из матрицы:

$$, \overbrace{\begin{matrix} j \\ 1 & 0 \end{matrix}}_i \begin{cases} 1 & a & b \\ 0 & c & d \end{cases}$$

где 1 означает наличие соответствующей переменной, а 0 - ее отсутствие.

Нетрудно видеть, что при $d = 0$ выражение для коэффициента ассоциативности имеет вид:

$$S_{ij} = \frac{a}{a + b + c} \quad (4.18)$$

Основная задача кластерного анализа заключается в рациональном делении анализируемого множества элементов на кластеры (классы) в соответствии с выбранной мерой сходства. Основными характеристиками, по которым оцениваются выделенные кластеры, считаются плотность, дисперсия, размеры, форма и отделимость.

Плотность характеризует уровень скопления (количество, близость) элементов, классифицируемых в кластере, дисперсия - степень рассеивания элементов в координатном пространстве относительно центра кластера, размеры - «радиус» кластера, форма - геометрию расположения элементов в кластере, отделимость - степень перекрытия кластеров и расстояние между ними в координатном пространстве.

К настоящему времени разработано большое количество различных методов деления множества элементов на кластеры. Однако наибольшее распространение в практических приложениях получили иерархические агломеративные методы. Их суть в общем виде заключается в представлении классифицируемых элементов в виде древовидной структуры (дендограммы) в зависимости от степени взаимосвязей между ними.

Деление дендограммы на кластеры осуществляется различными методами, причем наибольшее распространение получили методы одиночной связи, полной связи, средней связи и метод Уорда.

По методу одиночной связи кластер образуется по правилу: элемент включается в уже сформированный кластер, если хотя бы один из элементов кластера находится на том же уровне, что и анализируемый.

Метод полной связи предполагает, что анализируемый элемент включается в существующий кластер, если его сходство с каждым элементом кластера не ниже задаваемого порога.

Метод средней связи заключается в вычислении среднего сходства анализируемого элемента со всеми элементами в уже существующем кластере.

Элемент включается в кластер, если значение среднего сходства не ниже устанавливаемого порога.

Метод Уорда построен таким образом, чтобы оптимизировать минимальную дисперсию в пределах создаваемых кластеров. Целевая функция при этом определяется как сумма квадратов отклонений.

Нетрудно показать, что полученные нами выше оценки факторов, влияющих на требуемый уровень защиты информации, позволяют сформировать меру близости между различными вариантами условий, удовлетворяющую рассмотренным выше требованиям. Наиболее простым выражением данной меры близости вариантов m' и m'' будет:

$$\Delta W_{m',m''} = |W_{m'} - W_{m''}|. \quad (4.19)$$

Практическая реализация строго теоретического подхода к решению рассматриваемой задачи наталкивается на так называемое «проклятие размерности», заключающееся в непреодолимых вычислительных трудностях ввиду того, что множество потенциально возможных вариантов условий защиты, характеризуется, как это показано в предыдущем параграфе, числом астрономического порядка. Возможные пути преодоления указанных трудностей будут рассмотрены ниже при изложении сущности теоретико-эмпирического подхода.

Эмпирический подход. Сущность данного подхода заключается в решении рассматриваемой задачи на основе опыта и здравого смысла компетентных специалистов. К настоящему времени известно несколько примеров выделения типовых систем защиты информации.

Так, нетрудно видеть, что рассмотренные в начале данной главы наиболее известные методы выделения типовых СЗИ основаны преимущественно на эмпирическом подходе, причем без какого-либо объективного обоснования.

Однако при наличии рассмотренных выше весов возможных вариантов защиты можно предложить более наглядный, и потому психологически более приемлемый метод, основанный на эвристическом подходе.

Смысл веса варианта заключается в том, что чем больше этот вес, тем выше требования к защите информации в соответствующих условиях. Тогда требования к защите в зависимости от весов вариантов можно представить так, как показано на рис. 4.10 (выделенные интервалы получены методом половинного деления). Требования к защите при таком подходе будут определяться тем из интервалов, в который попадает соответствующее значение W_m . Возможные характеристики выделенных СЗИ приведены в табл. 4.7.

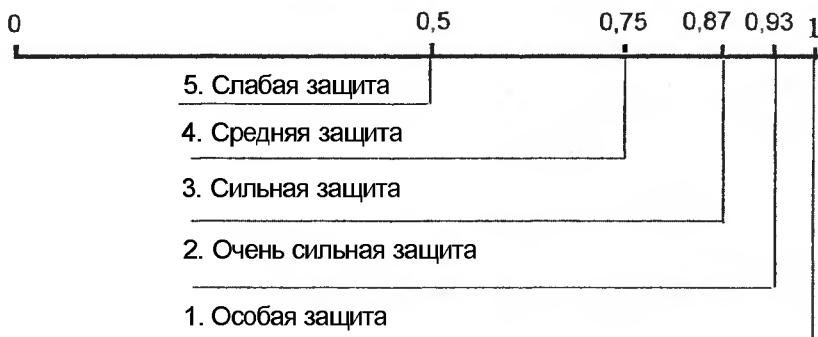


Рис. 4.10. Определение требований к защите информации методом половинного деления шкалы 0 - 1

В гл. 2, посвященной общей теории защиты, было введено понятие стратегии защиты как общей направленности усилий по защите информации, причем выделено три базовых стратегии: оборонительная, наступательная и упреждающая. Естественно предположить, что каждый из выделенных выше уровней защиты может достигаться в рамках каждой из предусмотренных стратегий.

Исключениями из этого правила могут быть только следующие ситуации: в рамках оборонительной стратегии вряд ли целесообразно предусматривать очень сильную (а тем более - особую) защиту, особая же защита даже в рамках наступательной стратегии может рассматриваться скорее в виде исключения; аналогично можно предположить, что слабая защита (не предусматривающая использования дополнительных средств защиты) не может носить наступательный (а тем более - упреждающий) характер; сомнительно также, чтобы средняя защита носила упреждающий характер.

Требования к защите информации

Таблица 4.7

Характеристики типовых СЗИ по уровню защиты информации

№ п/п	Класс СЗИ по уровню защиты	Ориентировочное количественное значение уровня защиты	Общая характеристика СЗИ
1	Слабой защиты	$\leq 0,5$	Обеспечивается защита в пределах возможностей серийных средств обработки информации и общедоступных организационно-правовых мер
2	Средней защиты	0,5-0,75	Может быть достигнута путем дополнения серийных средств и общедоступных организационных мер некоторыми средствами регулирования и разграничения доступа и поддержанием достаточно четкого уровня организации обработки информации
3	Сильной защиты	0,75-0,87	Может быть обеспечена комплексным применением широкого спектра различных средств защиты и строгой организацией процессов функционирования системы
4	Очень сильной защиты	0,87-0,93	Может быть обеспечена при соблюдении трех условий: 1) наличие развитой и высоко организованной СЗИ; 2) строжайшая организация процессов жизнедеятельности системы; 3) непрерывное управление процессами защиты
5	Особой защиты	$> 0,93$	Дополнительно к предыдущему требуется: 1) создание СЗИ по индивидуальному проекту; 2) реализация мандатной системы доступа

Тогда общая классификационная структура СЗИ может быть представлена так, как показано на рис. 4.11, причем здесь обведены прямоугольниками и обозначены цифрами без индексов основные классы систем, а обведены пунктиром и обозначены цифрами с индексами - дополнительные.

Конкретное содержание механизмов защиты типовых СЗИ может быть определено на основе анализа характеристик факторов,

Уровень защиты	Стратегия защиты		
	Оборонительная	Наступательная	Упреждающая
Слабый	1		
Средний	2	2н	
Сильный	3о	3	3у
Очень сильный		4	4у
Особый		5н	5

Рис. 4.11. Классификационная структура типовых СЗИ

влияющих на требуемый уровень защиты. Фрагменты таких характеристик в содержательном выражении приведены в табл. 4.8.

Рассмотрим еще один метод, основанный на эмпирическом подходе. Вычислим значения:

$$W_m(i,j,k)^{(\max)} = R_i^{(\max)} \cdot Q_{ij}^{(\max)} \cdot S_{ijk}^{(\max)}, \quad (4.20)$$

$$W_m(i,j,k)^{(\min)} = R_i^{(\min)} \cdot Q_{ij}^{(\min)} \cdot S_{ijk}^{(\min)}. \quad (4.21)$$

В целях нормирования значению $W_m(i,j,k)^{(\max)}$ припишем вес, равный 1, а $W_m(i,j,k)^{(\min)}$ - 0. Соответственно для варианта с $W_m^{(\max)}$ вероятность надежной защиты должна быть близка к 1, а для варианта с $W_m^{(\min)}$ - близка к 0. Для определения промежуточных значений должна быть выбрана функция:

$$\bar{P}_{\text{tp}} = f(\bar{W}_m) \quad (4.22)$$

наиболее адекватно отражающая существование процессов защиты информации. Здесь \bar{P}_{tp} - требуемая вероятность надежной защиты, а \bar{W}_m - приведенное по норме 0-1 значение W_m . Очевидно:

$$W_m = \frac{\bar{W}_m}{\bar{W}_m^{(\max)}} \quad (4.23)$$

В качестве функции $f(\bar{W}_m)$ целесообразнее всего принять логистическую кривую.

Теоретико-эмпирический подход. Данный подход основывается на комплексном использовании рассмотренных выше теоретического и эмпирического подходов. При этом естественным представляется стремление в максимальной степени использовать результаты строгого анализа задачи и определить те трудности, которые при этом возникают.

Дезагрегируем общую классификационную структуру факторов, влияющих на требуемый уровень защиты (табл. 4.5), на части: первую, включающую факторы первой и второй групп, вторую, включающую факторы третьей, четвертой и пятой групп, но только с учетом первых двух значений каждого фактора, и третью, тоже включающую факторы третьей, четвертой и пятой групп, но с учетом последних двух значений каждого фактора. Проведем затем классификацию вариантов условий в пределах каждой выделенной части (например, по рассмотренному выше иерархическому агglomerативному методу), а затем из трех полученных дендрограмм

Глава 4

Таблица 4.8

Фрагменты характеристики факторов, влияющих на требуемый уровень защиты информации

Наменование группы факторов	Факторы	Значение	Условия присвоения значений	Требования к защите информации
Обусловливающие обработываемой информацией	Степень конфиденциальности информации	Очень высокое	Нарушение защищенности информации ведет к крупномасштабным не восполнимым потерям	1. Доступ к информации по мандатам ограниченного действия 2. Исключение с вероятностью, близкой к 1, косвенной утечки информации по техническим каналам 3. То же по организационным каналам
	Высокое		Нарушение защищенности ведет к достаточно крупным и трудновосполнимым потерям	1. Высокоэффективное разграничение доступа к информации при опознавании пользователя с вероятностью, близкой к 1 2. Надежная (с вероятностью не ниже 0,93) защита от утечки информации по техническим каналам 3. То же по организационным каналам
	Среднее		Нарушение защищенности может привести к весьма ощутимым потерям, восполнение которых может потребовать значительных усилий и расходов	1. Разграничение доступа к информации с использованием сертифицированных серийных средств 2. Предупреждение косвенной утечки информации с использованием недорогих серийных средств 3. Организация обработки информации с соблюдением общепринятых правил обработки защищаемой информации
	Низкое		Нарушение защищенности не ведет к ощутимым потерям	Дополнительные средства защиты не требуются

составим общую, на основе которой и выделим типовые классы вариантов условий. Общее число вариантов условий в этом случае будет следующим: $N_1 = 4096$, $N_2 = N_3 = 2048$.

Такое число при надлежащем построении вычислительного алгоритма вполне подъемно для современных ЭВМ.

Для решения рассматриваемой здесь задачи рационального деления множества вариантов условий защиты на типовые классы плодотворным оказывается итеративный метод, сущность которого может быть представлена следующим алгоритмом.

1. Произвести исходное деление элементов на предполагаемое (желательное, заданное) число кластеров. Вычислить центры тяжести полученных кластеров.

2. Произвести перераспределение элементов по кластерам по принципу ближайшего расстояния до центра тяжести.

3. Вычислить новые центры тяжести кластеров.

Шаги 2 и 3 циклически повторяются до тех пор, пока не перестанут меняться кластеры.

Краткие выводы

1. На этапе перехода от экстенсивных к интенсивным способам защиты информации конкретные требования к защите определяются характером, видом и объемом обрабатываемой информации, продолжительностью ее пребывания в системе обработки, технологией обработки и организацией информационного процесса, структурой и этапом жизненного цикла системы.

Выработка данных требований в каждом конкретном случае может быть осуществлена на основе структурно-логического анализа систем и ситуаций защиты и структурированного их описания с широким применением методологии и методов неформальной теории систем.

2. В современных условиях наиболее подходящим оказывается подход, основанный на выделении некоторого количества типовых систем защиты и разработке рекомендаций по их использованию.

На сегодняшний день в целях типизации СЗИ у нас в стране и за рубежом разработано несколько регламентирующих документов, определяющих критерии оценки защищенности систем и механизмы защиты, которые должны использоваться при обработке информации различной степени конфиденциальности. Однако с точки зрения современной постановки задачи защиты они имеют ряд принципиальных недостатков, так как ориентированы на защи-

ту информации только в средствах ЭВТ и учитывают далеко не все факторы, оказывающие существенное влияние на уязвимость информации. Кроме того, их научное обоснование оставляет желать многое лучшего.

3. В целях усовершенствования методик определения требований к защите информации и типизации на этой основе систем защиты необходимо решение следующей последовательности задач:

- разработка методов оценки параметров защищаемой информации;
- формирование перечня и классификация факторов, влияющих на требуемый уровень защиты;
- структуризация возможных значений факторов;
- структуризация поля потенциально возможных вариантов условий защиты;
- оптимальное деление поля возможных вариантов на типовые классы;
- структурированное описание требований к защите в пределах выделенных классов.

4. Для оценки параметров защищаемой информации могут быть использованы показатели, характеризующие ее как обеспечивающий ресурс в процессе решения различных задач и как объект труда в процессе информационного обеспечения решаемых задач.

К показателям первого вида относятся важность, полнота, адекватность, релевантность и толерантность информации, а второго вида - способ кодирования и объем информации.

5. Для оценки важности, полноты и адекватности информации может быть применен подход, базирующийся на неформально-эвристических методах и использовании лингвистических переменных. В результате получается ряд классификаций указанных параметров, позволяющих практически решать задачи оценки защищаемой информации. При этом все рассмотренные показатели в зависимости от вида защищаемой информации могут быть разделены на три категории: определяющие, существенные и второстепенные.

6. В целях формирования возможно более полного множества факторов, влияющих на защиту информации, и возможно более адекватного определения степени их влияния на требуемый уровень защиты может быть использован подход, базирующийся на неформально-эвристических методах с широким привлечением знаний, опыта и интуиции компетентных и заинтересованных специалистов.

Практическое использование этого подхода позволило выделить в общей сложности 17 факторов, каждый из которых может принимать одно из четырех значений. Таким образом, общее число возможных вариантов условий защиты превышает $1,7 \times 10^{10}$, что, естественно, делает задачу определения конкретных требований к защите информации практически нразрешимой.

Данная ситуация приводит к необходимости деления всего множества возможных вариантов на некоторое число классов, которые можно было бы использовать в дальнейшем для практического решения поставленной выше задачи.

7. Осуществление классификации множества вариантов потенциально возможных условий защиты информации фактически является задачей формирования необходимого и достаточного набора типовых систем защиты информации.

На основании теоретического, эмпирического и теоретико-эмпирического подходов к решению этой проблемы может быть получена классификационная структура типовых СЗИ, содержащая пять основных и пять дополнительных классов.

Общее число вариантов условий при такой классификации в случае надлежащего построения вычислительного алгоритма оказывается вполне подъемным для современных ЭВМ.

Глава пятая

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Определение, типизация и стандартизация систем защиты информации

Определим систему защиты информации как совокупность средств, методов и мероприятий, предусматриваемых в составе того или иного объекта для решения выбранных задач защиты. Введением понятия СЗИ постулируется, что все ресурсы, выделяемые для защиты информации, должны объединяться в единую, целостную, функционально самостоятельную систему.

Концептуально важнейшим требованием, предъявляемым к СЗИ, является требование адаптируемости, которое обуславливается, с одной стороны, тем, что многочисленные факторы, влияющие на требуемый уровень защиты, могут существенно изменяться, а с другой - тем, что сами процессы защиты информации относятся к слабоструктуризованным. Управление такого рода процессами эффективно только при условии адаптируемости системы.

Помимо этого к СЗИ предъявляются также различные требования функционального, эргономического, экономического, технического и организационного характера.

В процессе формирования основ теории защиты информации были сформулированы общеметодологические принципы построения и функционирования СЗИ, впервые изложенные в работе [3]. В условиях системно-концептуального подхода к защите, развиваемого в данном учебном пособии, эти принципы включают концептуальное единство системы, адекватность предъявляемым требованиям, адаптируемость, функциональную самостоятельность, удобство использования, минимизацию предоставляемых прав, полноту контроля, активность реагирования, экономичность.

Архитектура СЗИ должна быть аналогичной архитектуре защищаемой системы и может рассматриваться в функциональном, организационном и структурном аспектах.

Функционально СЗИ представляет собой совокупность реализуемых ею функций защиты. Организационно она состоит из меха-

низмов обеспечения защиты информации, механизмов управления ими и механизмов общей организации работы системы.

В понятие организационного построения СЗИ входит также распределение ее элементов по организационно-структурным компонентам защищаемой системы. Исходя из этого в организационном построении СЗИ должны быть предусмотрены подсистемы защиты в каждом из структурных компонентов и некоторое управляющее звено, которое в специальных публикациях получило название ядра СЗИ.

Определим ядро системы защиты как специальный компонент, предназначенный для объединения всех подсистем СЗИ в единую целостную систему для организации, обеспечения и контроля ее функционирования [3]. С учетом этого функциями ядра СЗИ должны быть: организация и обеспечение блокирования бесконтрольного доступа к базам защищаемых данных; включение компонентов СЗИ в работу при поступлении запросов на обработку защищаемых данных; управление работой СЗИ в процессе обработки защищаемых данных; организация и обеспечение проверок правильности функционирования СЗИ; организация и ведение массивов эталонных данных СЗИ; обеспечение реагирования на сигналы о несанкционированных действиях; ведение протоколов СЗИ.

Структурно СЗИ строится по аналогии со структурным построением защищаемой системы. Таким образом, ее структурная схема может быть представлена так, как показано на рис. 5.1 [3]

Важное значение для обеспечения надежности и экономичности защиты имеют типизация и стандартизация систем защиты информации. Типизация в этом случае понимается как разработка типовых аппаратных, программных или организационных решений, а также технологических процессов защиты, а стандартизация - как процесс установления и применения стандартов (исходных для сопоставления с ними образцов, эталонов, моделей). Стандарт как нормативно-технический документ определяет комплекс норм, правил, требований к объекту.

Анализ рассматривавшихся нами выше концептуальных подходов к защите информации и к архитектурному построению СЗИ показывает, что с целью создания наилучших предпосылок для оптимизации защиты целесообразно выделить три уровня типизации и стандартизации: высший - уровень системы защиты в целом; средний - уровень составляющих компонентов; низший - уровень проектных решений по средствам и механизмам защиты.

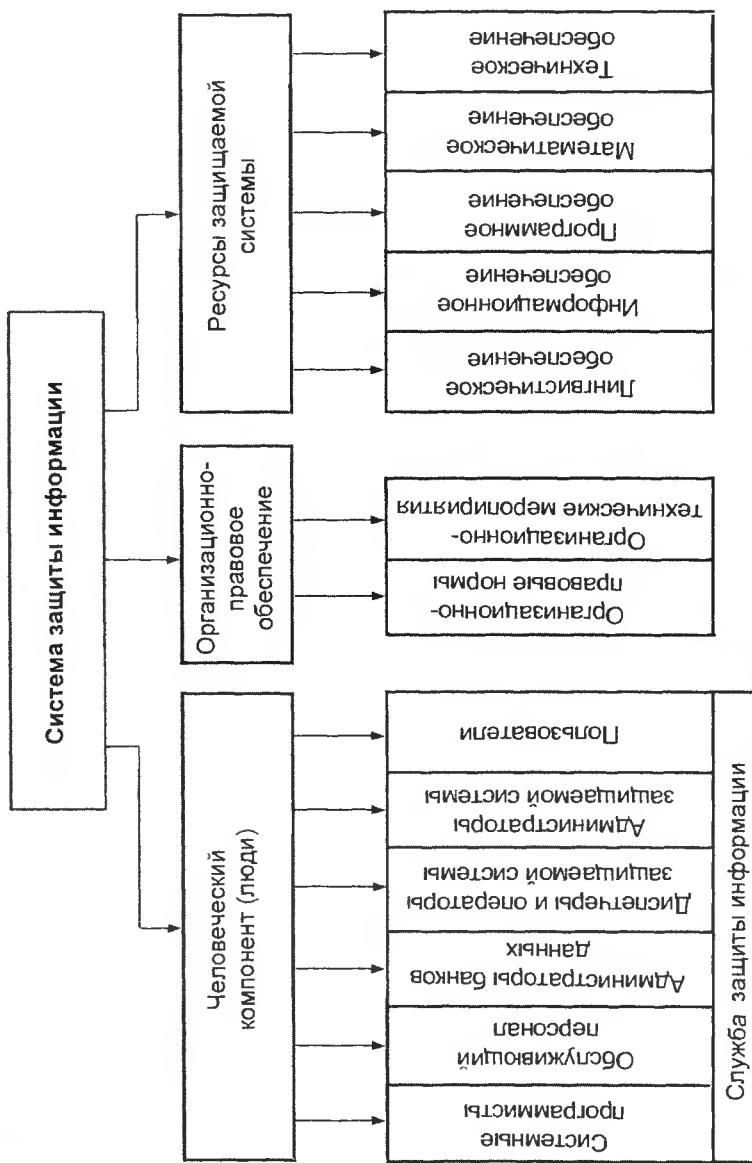


Рис. 5.1. Общая структурная схема системы защиты информации

Типизация и стандартизация на высшем и среднем уровнях предполагает некоторую системную классификацию СЗИ, при которой все потенциально необходимые системы делились бы на группы, каждая из которых была бы адекватна некоторым вполне определенным потребностям в защите информации, а вся совокупность таких групп охватывала бы все потенциально возможные варианты потребностей в защите.

В предыдущей главе нами был рассмотрен теоретико-эмпирический подход к решению такого рода задачи, основу которого составляют формирование полного множества всех потенциально возможных вариантов условий защиты, определение количественных характеристик каждого из вариантов и кластеризация всего поля вариантов по критерию не превышения заданного числа классов или меры различия количественных характеристик вариантов в пределах каждого из классов. Применив эмпирическую часть этого подхода к типизации СЗИ, мы можем получить их классификацию по уровню защиты, обеспечиваемому соответствующей системой, и активности реагирования на несанкционированные действия.

Как было показано выше (см. рис. 4.10), по уровню обеспечиваемой защиты все СЗИ целесообразно разделить на следующие четыре категории:

1) системы слабой защиты - рассчитанные на такие системы или объекты, в которых обрабатывается информация, имеющая низкий уровень конфиденциальности;

2) системы сильной защиты - рассчитанные на системы или объекты, в которых обрабатывается информация, подлежащая защите от несанкционированного доступа, но объемы этой информации не очень велики, и обрабатывается она эпизодически;

3) системы очень сильной защиты - рассчитанные на системы или объекты, в которых регулярно обрабатываются большие объемы конфиденциальной информации;

4) системы особой защиты - рассчитанные на системы или объекты, в которых регулярно обрабатывается информация повышенной секретности.

По активности реагирования на несанкционированные действия все системы защиты можно разделить на следующие три типа:

1) пассивные СЗИ, в которых не предусматриваются ни сигнализация о несанкционированных действиях, ни воздействие системы защиты на нарушителя;

2) полуактивные СЗИ, в которых предусматривается сигнализация о несанкционированных действиях, но не предусматривается воздействие системы на нарушителя;

3) активные СЗИ, в которых предусматриваются как сигнализация о несанкционированных действиях, так и воздействие системы на нарушителя.

В общем случае можно предположить, как это делалось в [3, 31], что СЗИ каждой категории по уровню защиты могут относиться к разным типам активности реагирования. Однако исходя из здравого смысла вряд ли целесообразно строить активные системы слабой защиты. В то же время системы особой защиты обязательно должны быть активными. Таким образом, при классификации можно говорить об обязательных (О), целесообразных (Ц), нецелесообразных (НЦ), допустимых (Д) и недопустимых (НД) СЗИ. В итоге получается вариант, приведенный на рис. 5.2.

		Тип СЗИ		
		Пассивные	Полуактивные	Активные
Категории СЗИ	Слабой защиты	$\frac{D}{C}$ 1	D C^*	D NC
	Сильной защиты	ND	$\frac{D}{C}$ 2	$\frac{D}{C^*}$ 2a
	Очень сильной защиты	ND	$\frac{D^*}{C^*}$ 3a	$\frac{D}{C}$ O^* 3
	Особой защиты	ND	ND	O 4

Рис. 5.2. Допустимые и целесообразные типы СЗИ для различных категорий (* - в отдельных случаях)

Следует отметить, что полученная классификация не учитывает тип информационно-вычислительной системы, для которой предназначается СЗИ. В целях получения полного множества потенциально необходимых СЗИ воспользуемся классификацией типов систем, предложенной ВА Герасименко в [3], а именно будем различать персональную ЭВМ, используемую локально (ПЭВМ), групповую ЭВМ, используемую локально (ГЭВМ), вычислительный центр предприятия или организации (ВЦП), вычислительный центр коллективного пользования (ВЦКП), локальную вычислительную сеть (ЛВС), слабораспределенную (в пределах населенного пункта, небольшой территории) вычислительную сеть (СВС), сильнораспределенную, региональную вычислительную сеть (РВС), глобальную вычислительную сеть (ГВС).

Для всех перечисленных вариантов может быть предложен типовой проект СЗИ каждого из шести классов, показанных на рис. 5.2. Однако, как и в предыдущем случае, нецелесообразно использовать активные СЗИ для защиты информации в ПЭВМ. С другой стороны, явно недостаточно использовать пассивные СЗИ слабой защиты для защиты информации в РВС и ГВС. Поэтому, как и в предыдущей классификации, в полном множестве СЗИ необходимо предусмотреть выделение целесообразных, допустимых и обязательных систем, что в итоге приведет нас к классификации, показанной на рис. 5.3.

Что касается типизации и стандартизации на среднем уровне, то она предусматривает разработку типовых проектов структурно или функционально ориентированных компонентов СЗИ. В качестве первых логично выбрать компоненты СЗИ, ориентированные на защиту информации в конкретных типовых структурных компонентах защищаемой системы. В качестве же функционально ориентированных можно выбрать такие компоненты, как регулирование доступа на территорию, в помещения, к техническим средствам, программам и массивам данных, подавление излучений и наводок, предупреждение наблюдения и подслушивания, маскировка информации и, наконец, управление системой защиты.

Последней из рассматриваемых нами является типизация и стандартизация на низшем уровне, которая предполагает разработку типовых проектных решений по реализации различных средств защиты информации. Основными здесь являются технические, программные, организационные и криптографические средства. Причем типовое проектное решение для каждого из этих средств должно быть оформлено по соответствующим правилам.

Один из весьма перспективных вариантов покомпонентной типизации и стандартизации СЗИ был предложен в работе [3] как вариант, основанный на так называемой шестирубежной модели.

Вариант СЗИ						
	1 Слабой защиты. Пассивные	2 Сильной защиты. Полу- активные	2а Сильной защиты. Активные	3 Очень сильной защиты. Активные	3а Очень сильной защиты. Популятивные	4 Особой защиты. Активные
ПЭВМ	Ц 1	Д/Ц* 1а				
ГЭВМ	Ц* 2а	Ц 2	Д/Ц* 2б			
ВЦП	Д* 3а	Ц 3	Д/Ц* 3б	Д* 3в		
ВЦКП			Ц 4	Ц* 4а	Ц* 4б	Д* 4в
ЛВС		Ц* 5а	Ц 5	Д* 5б		
СВС		Ц* 6а	Ц* 6б	Ц 6	Ц* 6в	Д* 6г
РВС		Ц* 7а	Ц 7	Д* 7б	Д* 7в	Ц* 7г
ГВС			Ц 8		Ц* 8а	

Tin nifopmahnnoho-
Bpincnterphoh cnctempi

Рис. 5.3. Итоговая классификация СЗИ:
 Ц – целесообразно; Д – допустимо; * – в отдельных случаях

В последствии с учетом развития сетевых информационных технологий указанная модель была трансформирована в семирубежную и была достаточно подробно изложена в учебнике [31]. Существо подхода состоит в том, что защита информации, вообще говоря, будет обеспечена лишь в том случае, если защищены такие элементы, имеющие отношение к системе или объекту, как территория, в пределах которой расположены здания и помещения с размещенными в них средствами и ресурсами, используемыми для обработки и хранения защищаемой информации, а также линии (каналы) связи, используемые для сопряжения элементов системы с другими (внешними) объектами.

В этом случае организационно СЗИ может быть представлена совокупностью следующих рубежей защиты: 1) территория, занимаемая защищаемой системой или объектом; 2) здания, расположенные на территории; 3) помещения внутри зданий, в которых расположены ресурсы системы и защищаемая информация; 4) ресурсы, используемые для обработки и хранения информации, и сама защищаемая информация; 5) линии связи, проходящие в пределах одного и того же здания; 6) линии (каналы) связи, проходящие между различными зданиями, расположенными на одной и той же охраняемой территории; 7) линии (каналы) связи, проходящие по неконтролируемой территории.

Под рубежом защиты в модели понимается соответствующим образом организованная совокупность всех средств, методов и мероприятий, используемых на рассматриваемом элементе системы или объекта для защиты информации. Нетрудно видеть, что тем или иным сочетанием перечисленных рубежей может быть представлена СЗИ практически любой системы или объекта. Каждый из рубежей защиты при этом может быть реализован с помощью типовых проектных решений.

Таким образом, можно констатировать, что у нас имеются весьма широкие возможности для типизации и стандартизации средств, механизмов и компонентов СЗИ и даже целых СЗИ. Дальнейшее развитие данного вопроса идет в направлении синтеза подходов, изложенных в данном параграфе и предыдущей главе книги.

5.2. Система защиты информации как многокритериальный развивающийся объект

Рассмотренные выше в гл. 2 методы моделирования процессов защиты информации, в том числе с использованием энтропийного подхода, могут достаточно эффективно применяться при решении

задач анализа и синтеза СЗИ. При этом необходимость учета множества факторов, влияющих на защиту и находящихся в сложном динамичном взаимодействии, приводит нас к представлению системы защиты как многокритериального развивающегося объекта. В связи с этим в данном параграфе рассматривается подход к анализу и оценке СЗИ для целей управления их развитием.

Многокритериальный развивающийся объект определен в [48] как множество реализаций сложной системы, описываемой заданным набором критериев и развивающейся под действием внешних объективных и внутренних субъективных факторов.

С этой точки зрения можно выделить несколько особенностей СЗИ, которые и позволяют рассматривать их в качестве многокритериальных развивающихся объектов. Перечислим эти особенности.

Для СЗИ существует рассмотренное в предыдущем параграфе некоторое естественное разбиение их реализаций на классы. При этом могут быть выделены один или несколько критериев (так называемых классифицирующих критериев), по которым может быть проведено группирование в классы. Следует отметить, что если классифицирующий критерий используется в дальнейшем в анализе, то необходима его числовая оценка (числовые критерии - заместители).

Для каждой СЗИ существует устойчивая, монотонная функция спроса (стратегии принятия решений), описывающая рынок потребления такого рода систем. Эта функция в [48] названа ранговой функцией полезности многокритериального развивающегося объекта и обусловлена объективным характером его взаимодействия с внешней средой.

Для СЗИ существует также устойчивая, монотонная функция, которая в [48] названа функцией полезности при анализе рисков. Эта функция определяется разнообразием типов принимаемых решений, что, вообще говоря, обусловлено субъективным характером распределения ресурсов, выделяемых на защиту информации.

Разнообразие типов реализаций СЗИ, обусловлено разнообразием стратегий защиты (политик безопасности), а также типов технических решений. Об этом шла обстоятельная речь в предыдущем параграфе, посвященном типизации и стандартизации систем защиты.

СЗИ характеризуется в динамике своего развития как появлением новых классов объектов, так и появлением новых типов объектов в том или ином классе, т.е. фактически возникновением новых технических решений и связанных с ними политик безопасности.

Характер этого процесса явно не последовательный и определяется как развитием техники, так и возникновением новых потребностей рынка средств защиты информации.

Все эти особенности СЗИ могут быть описаны в рамках концепции так называемого монотонного критерия [49]. Рассмотрим подробнее механизм такого описания.

Представим каждую реализацию СЗИ точкой в пространстве единичных критериев $X \equiv \{x_1, \dots, x_m\}$. Единичные критерии - это нормированные в шкале $[0;1]$ показатели с неубывающими предпочтениями. Эти критерии задаются как значения функций перевода для физически измеряемых критериев [49]. Множество реализаций СЗИ в пространстве единичных критериев, как это видно из материалов предыдущего параграфа, разбивается на классы эквивалентности, которые в пространстве неубывающих предпочтений можно представить как поверхности одного уровня некоторого монотонного критерия $\mathcal{E}(X)$.

Если сгруппировать реализации СЗИ по близости применяемых решений, получается направления в пространстве критериев, определяющие политики безопасности. Математически линию в многомерном пространстве можно задать системой одномерных функций одного параметра (обозначим его через t)

$$x_i(t) = T_i(t), \quad (i = 1, \dots, m). \quad (5.1)$$

Система функций $T_1(t), \dots, T_m(t)$ характеризует политику безопасности.

Для описания критерия $\mathcal{E}(X)$ используем упоминавшуюся выше ранговую функцию полезности (РФП) и функцию полезности при анализе рисков (ФПР). Значение $\mathcal{E}(X)$ в k -м классе эквивалентности определим через значение РФП $R(k)$. Вид поверхности одного уровня $\mathcal{E}(X) = \text{const}$ определяет отношение к риску лица, принимающего решение (ЛПР), т.е. ФПР. Таким образом, анализ и оценка СЗИ непосредственно связаны с анализом структуры монотонного критерия $\mathcal{E}(X)$ в пространстве критериев, упорядоченных по возрастанию.

Анализ структуры монотонного критерия $\mathcal{E}(X)$ базируется на его специальном представлении, что отражено в следующей теореме.

Теорема. Любой положительный, непрерывный, ограниченный монотонно возрастающий критерий $\mathcal{E}(x_1, \dots, x_m)$ (кроме критерия минимального типа), заданный на множестве значений x_i ($i = 1, \dots, m$) $0 \leq x_i \leq 1$, может быть представлен (с любой заданной точностью) в виде

$$\mathcal{E}(x_1, \dots, x_m) = \sum_{i=1}^m \alpha_i(x_1, \dots, x_m) R(x_i), \quad (5.2)$$

где $\alpha(x_1, \dots, x_m)$ - непрерывные положительные функции, называемые коэффициентами весомости показателей;

$$\sum_{i=1}^m \alpha_i(x_1, \dots, x_m) = 1;$$

$R(x_i)$ - РФП, определяемая как значение критерия на диагонали, т. е. $R(t) = \mathcal{E}(x_1 = t, \dots, x_m = t)$. Доказательство данной теоремы можно найти в [50].

Формализуем понятие политики безопасности, реализуемой СЗИ. Пусть задана некоторая точка $\hat{X} \equiv \{x_1, \dots, x_m\}$; эта точка определяет направление политики как множество значений x_i , удовлетворяющих системе параметрических уравнений

$$x_i(t) = R^{-1} \left[\frac{\hat{R}(x_i)}{\hat{R}(x_{\max})} R(t) \right] \quad (5.3)$$

Основное свойство политики безопасности заключается в том, что значения критерия на ней факторизуются.

Подставив $x_i(t)$ в (5.2), получим

$$\begin{aligned} \mathcal{E}_T(t) &= \sum_{i=1}^m \alpha_i[x(t)] R[x_i(t)] = \sum_{i=1}^m \alpha_i(t) R \left\{ R^{-1} \left[\frac{\hat{R}(x_i)}{\hat{R}(x_{\max})} R(t) \right] \right\} = \\ &= \sum_{i=1}^m \alpha_i(t) R(\hat{x}_i) \frac{1}{R(x_{\max})} R(t) = \frac{\gamma_T(t)}{R(\hat{x}_{\max})} R(t), \end{aligned} \quad (5.4)$$

где индекс T отмечает заданную политику безопасности, а $\gamma_T(t)$ коэффициент, определяемый политикой безопасности и ФПР.

Таким образом, значения критерия на направлении политики безопасности пропорциональны значениям РФП (стратегии выбора) и коэффициентам политики.

Формализуем понятие функции полезности при анализе риска, используя монотонный критерий $\mathcal{E}(X)$. Так как отношение к риску определяется видом поверхности уровня, то обозначим через

$L(x_1, \dots, x_m)$ каноническое описание поверхности уровня, определяемое условием $\mathcal{E}(X) = \text{const}$. Тогда можно записать

$$\mathcal{E}(x_1, \dots, x_m) = F[L(x_1, \dots, x_m)], \quad (5.5)$$

где $F(L)$ - монотонная функция.

Определим ФПР как $U(t) = L(x_1 = t, \dots, x_m = t)$. Для получения $L(x_1, \dots, x_m)$ можно воспользоваться свойством поверхности уровня как множества, на котором полный дифференциал $\mathcal{E}(X)$ равен нулю или, с учетом канонического представления,

$$d\mathcal{E}(X) = \frac{dF}{dL} dL(X) = A(x_1, \dots, x_m) dL(x_1, \dots, x_m) \quad (5.6)$$

Таким образом, $L(x_1, \dots, x_m)$ определяется выделением общего множителя из выражения для полного дифференциала критерия $\mathcal{E}(X)$.

Используя РФП и ФПР, которые получаются на основании фактических данных о группировании реализации СЗИ по классам в соответствии с тем, как было изложено в предыдущем параграфе, и направлениям политики безопасности, можно ставить задачу синтеза критерия $\mathcal{E}(X)$.

Вместе с тем представляет интерес анализ критериев с точки зрения введенных понятий РФП и ФПР, которые можно было бы рекомендовать для практического использования при решении конкретных задач защиты информации. Остановимся на некоторых из таких критериев.

Один из них аддитивный критерий, который может быть представлен следующим образом:

$$\mathcal{E}(X) = \sum_{i=1}^m \alpha_i x_i, \quad (5.7)$$

$$\text{где } \sum_{i=1}^m \alpha_i = 1$$

$$R(t) = U(t) = \sum_{i=1}^m \alpha_i t = t \quad . \quad (5.8)$$

Таким образом, для аддитивного критерия РФП и ФПР совпадают, т.е. стратегия выбора линейная, а отношение к риску нейтральное.

Другим является обобщенный метрический критерий

$$\mathcal{E}(X) = \left(\sum_{i=1}^m \alpha_i x_i^p \right)^{1/p}, \quad (5.9)$$

где $p > 1$, $\sum_{i=1}^m \alpha_i = 1$;

$$R(t) = \left(\sum_{i=1}^m \alpha_i t^p \right)^{1/p} = t. \quad (5.10)$$

$$d\mathcal{E}(X) = \frac{1}{p} \left(\sum_{i=1}^m \alpha_i x_i^p \right)^{1/p-1} d \left(\sum_{i=1}^m \alpha_i x_i^p \right) \quad (5.11)$$

Таким образом,

$$L(X) = \sum_{i=1}^m \alpha_i x_i^p, \quad (5.12)$$

$$U(t) = \sum_{i=1}^m \alpha_i t^p = t^p. \quad (5.13)$$

Данный критерий имеет линейную стратегию выбора и степень риска p при принятии решений.

5.3. Проектирование систем защиты информации

Вопросам проектирования систем защиты информации посвящено достаточно много различных работ. В частности, методология премирований СЗИ четко сформулирована в монографии В.А.Герасименко [3] и в дальнейшем развита в учебнике [31]. Обобщая эти и другие известные нам работы, мы можем систематизировать предлагаемые подходы к проектированию в виде схемы, показанной на рис. 5.4. При этом классификация возможных подходов представлена на рис. 5.5.

Не вдаваясь в подробное описание методов проектирования, которое читатель может почерпнуть самостоятельно, прочитав, например, соответствующую главу учебника [31], мы сосредоточим здесь внимание на принципиальных вопросах оценки эффективности процессов защиты, реализуемых создаваемой СЗИ.

Системы защиты информации



Рис. 5.4, Последовательность и содержание проектирования систем защиты информации

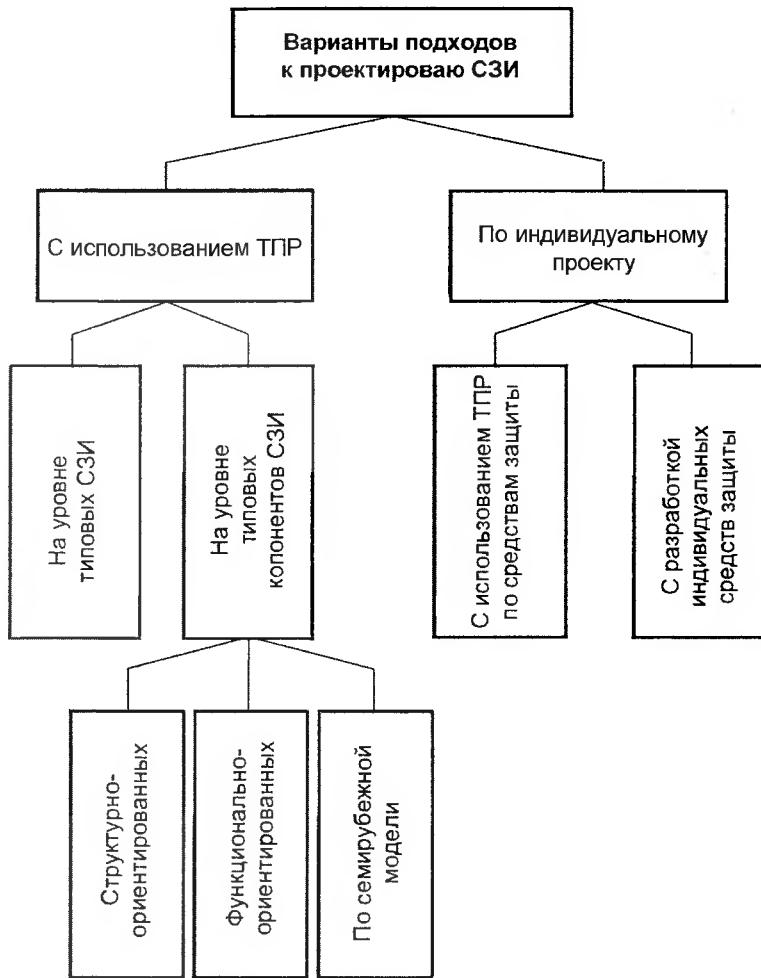


Рис. 5.5. Классификационная структура подходов к проектированию СЗИ

На основе изложенного в гл. 2 энтропийного подхода может быть построена модель решения данной задачи, сходная по своей постановке с задачей анализа гравитационного взаимодействия системы материальных точек.

Пусть T_{il} - количественная оценка эффективности средств защиты, находящихся в l -й зоне защищаемого объекта и используемых в СЗИ для противодействия i -й потенциальной угрозе; Q_i -

полная эффективность всех средств защиты, находящихся в I -й зоне объекта; D_r - необходимая эффективность защиты для гарантированного противодействия r -й угрозе (фактически это количественная оценка угрозы). В качестве ресурсной переменной рассматриваемой системы можно задать C_r - усредненные затраты на реализацию средств защиты, находящихся в I -й зоне объекта и направленных на противодействие r -й угрозе, плюс затраты на ликвидацию последствий в случае реализации угрозы.

Естественно, что количественные оценки всех введенных нами переменных могут быть получены исключительно с использованием тех или иных методов экспертных оценок в соответствии с тем, как это было изложено нами выше в главе 2 данного учебного пособия. Более того, используемые нами в дальнейших выкладках методы, основанные на энтропийном подходе, требуют, чтобы величины T_{lr} , Q_l и D_r были выражены целыми натуральными числами. Этого легко добиться присвоив их значениям определенный ранг, который будет характеризовать эффективность некоторым количеством условных единиц.

По аналогии с гравитационной моделью Ньютона интересующая нас модель оценки эффективности защиты может быть представлена в виде

$$T_{lr} = k \frac{Q_l D_r}{C_{lr}^2} \quad (5.14)$$

где k - некоторая константа, а затраты на реализацию выступают в качестве «расстояния».

Однако у этого уравнения имеется очевидный недостаток: если удвоить заданные значения Q_l и D_r , то эффективность противодействия угрозам учетверится, а естественно ожидать, что она лишь удвоится. Чтобы избежать этого недостатка, величины T_{lr} всегда должны удовлетворять следующим ограничениям:

$$\sum_r T_{lr} = Q_l \quad (5.15)$$

$$\sum_I T_{lr} = D_r \quad (5.16)$$

Этим ограничениям можно удовлетворить, если ввести наборы констант A_r и B_r , связанные соответственно со средствами защиты I -й зоны объекта и r -й угрозой. Назовем их балансирующими

множителями. Кроме того, нет оснований считать, что «расстояние» играет в уравнении (5.14) такую же роль, что и в ньютоновской физике, поэтому введем более общую функцию «расстояния» в виде некоторой «ресурсной» функции $f(C_{lr})$. Модифицированная гравитационная модель имеет, таким образом, следующий вид:

$$T_{lr} = A_l B_r Q_r D_r f(C_{lr}), \quad (5.17)$$

где

$$A_l = \left[\sum_r B_r D_r f(C_{lr}) \right]^{-1} \quad (5.18)$$

$$B_r = \left[\sum_l A_l Q_l f(C_{lr}) \right]^{-1} \quad (5.19)$$

Уравнения для A_l и B_r решаются традиционными методами, и можно легко проверить, что они гарантируют удовлетворение ограничениям (5.15) и (5.16). Величины C_{lr} в этой модели могут служить общей мерой сопротивления реализации r -ой угрозы в l -ой зоне объекта. Поскольку оценка этой меры производится экспертами с учетом не только стоимости защиты, но и таких параметров, как вероятность проявления угрозы, время ее реализации и др., то назовем C_{lr} «обобщенными затратами».

Введем также дополнительное к (5.15) и (5.16) ограничение на T_{lr} , имеющее вид:

$$\sum_l \sum_r T_{lr} C_{lr} = U \quad (5.20)$$

где U - полный ресурс системы.

Перейдем теперь к основной цели нашего исследования и определим необходимое распределение T_{lr} , максимизируя энтропию системы, выраженную в виде [41]:

$$\ln W(\{T_{lr}\}) = \ln T! - \sum_l \sum_r \ln T_{lr}! \quad (5.21)$$

где $W(\{T_{lr}\})$ - полное число состояний системы, соответствующее распределению $\{T_{lr}\}$; T - полная эффективность всех средств защиты объекта, выраженная, как это было принято нами выше, в условных единицах и представляющая сумму рангов эффективности указанных средств.

Для получения набора T_{lr} , максимизирующего $\ln(\{T_{lr}\})$ из уравнения (5.21) при ограничениях (5.15), (5.16) и (5.20), следует максимизировать лагранжиан, равный

$$L = \ln W + \sum_l \lambda_l (Q_l - \sum_r T_{lr}) + \sum_r \lambda_r (D_r - \sum_l T_{lr}) + \\ + \mu (U - \sum_l \sum_r T_{lr} C_{lr}), \quad (5.22)$$

где λ_l , λ_r и μ - множители Лагранжа.

Поскольку предполагается, что T_{lr} достаточно велики, то можно воспользоваться формулой Стирлинга, согласно которой

$$\ln T_{lr} = T_{lr} \ln T_{lr} - T_{lr} \quad . (5.23)$$

Тогда из (5.21) получим

$$\ln W = - \sum_l \sum_r T_{lr} \ln T_{lr} \quad . (5.24)$$

Значения T_{lr} , которые доставляют максимум L и, следовательно, являются искомым распределением средств защиты по зонам объекта и потенциальным угрозам, представляют собой решение системы уравнений

$$\frac{\delta L}{\delta T_{lr}} = 0 \quad (5.25)$$

совместно с ограничениями (5.15), (5.16) и (5.20).

Дифференцируя (5.22), будем иметь

$$\frac{\delta L}{\delta T_{lr}} = -\ln T_{lr} - \lambda_\lambda - \lambda_r - \mu C_{lr} \quad (5.26)$$

Это выражение равно нулю, когда

$$T_{lr} = \exp(-\lambda_\lambda - \lambda_r - \mu C_{lr}) \quad . (5.27)$$

Подставляя (5.27) в (5.15) и (5.16), получим

$$\exp(-\lambda_\lambda) = Q_\lambda \left[\sum_r \exp(-\lambda_r) - \mu C_{l\lambda} \right]^{-1}, \quad (5.28)$$

$$\exp(-\lambda_r) = D_r \left[\sum_l \exp(-\lambda_l) - \mu C_{lr} \right]^{-1}. \quad (5.29)$$

Глава 5

Чтобы представить окончательный результат в более привычном виде, запишем

$$A_l = \frac{1}{Q_l} \exp(-\lambda_l) \quad (5.30)$$

$$B_r = \frac{1}{D_r} \exp(-\lambda_r) \quad (5.31)$$

Отсюда

$$T_{lr} = A_l B_r Q_l D_r \exp(-\mu C_{lr}) \quad (5.32)$$

где в соответствии с уравнениями (5.28) - (5.31) имеем

$$A_l = \left[\sum_r B_r D_r \exp(-\mu C_{lr}) \right]^{-1} \quad (5.33)$$

$$B_r = \left[\sum_l A_l Q_l \exp(-\mu C_{lr}) \right]^{-1} \quad (5.34)$$

Таким образом, искомое распределение описывается модифицированной гравитационной моделью с наперед заданной функцией f . Величина μ , характеризующая среднее значение затрат на одну условную единицу эффективности средств защиты, определяется из системы ограничений задачи. В случае одинаковой эффективности применяемых средств защиты величина μ будет характеризовать среднюю эффективность их применения против конкретных угроз. В итоге нами получен показатель эффективности средств защиты, который учитывает не только суммарную эффективность применяемых средств защиты, но и их оптимальное распределение по зонам защищаемого объекта или системы, исходя из наиболее эффективного противодействия потенциальным угрозам безопасности информации.

5.4. Управление процессами функционирования систем защиты

Функционирование СЗИ как системы организационно-технологического типа должно быть организовано в соответствии с основными принципами управления, разработанными для данного типа систем. Интерпретация этих принципов применительно к

управлению защитой информации приводит нас к общей модели управления, представленной на рис. 5.6 [3, 31].

Исходной основой организации процесса управления в этой модели являются планы обработки информации в защищаемой системе или объекте. Данные планы позволяют сформулировать требования к защите информации на всех этапах ее обработки, которые могут быть выражены вероятностным параметром $P_{з.тр}$.

В соответствии с этим значением показателя защищенности на каждом плановом этапе обработки информации должны быть определены оптимальные наборы средств защиты (технических (Т), программных (П), организационных (О), законодательных (З), морально-этических (М)), обеспечивающих требуемый уровень защиты. Формирование таких наборов и является общей задачей управления средствами защиты.

Далее решение задачи управления предполагает оценку ожидаемого уровня защищенности информации ($P_{з.ож}$), который обеспечивается полученным набором средств и, вообще говоря, может отличаться от требуемого. Если это отличие будет превышать допустимое значение ($\Delta P_{доп}$), то, очевидно, необходимо внести определенную коррекцию в сформированные наборы и повторить оценку.

Однако не исключены и такие случаи, когда имеющимися средствами требуемый уровень защиты принципиально не может быть достигнут. В этом случае должны меняться сами планы обработки информации.

Сформированные в результате реализации процедуры планирования наборы средств защиты в дальнейшем используются в процессе запланированной обработки информации. При этом, как предусмотрено механизмом обратной связи, обязательно должен осуществляться соответствующий контроль действительного уровня защищенности. На основе такого контроля может быть определен показатель действительного уровня защищенности $P_{з.д}$, который сопоставляется с требуемым уровнем $P_{з.тр}$. В случае рассогласования указанных показателей выше допустимой нормы реакция системы управления защитой может заключаться либо в изменении набора используемых средств защиты, либо в изменении уровня требуемой защищенности.

Как видим, описанная нами модель управления защитой информации является частным случаем управления в системах организационно-технологического типа, о чём уже упоминалось выше. Это обстоятельство существенно облегчает формирование технологии управления функционированием СЗИ, поскольку для этого

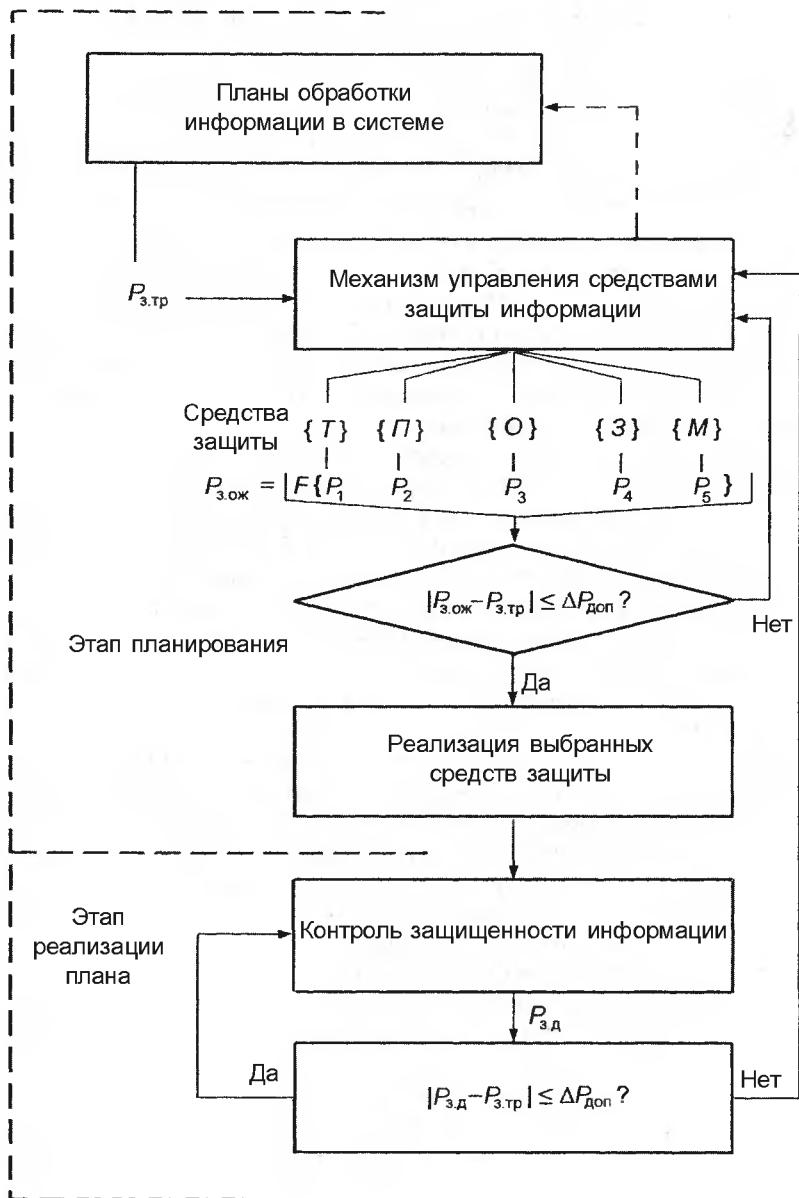


Рис. 5.6. Общая модель управления защитой информации

достаточно трансформировать общие положения концепции управления в системах указанного типа применительно к проблемам защиты информации.

Как известно, основными макропроцессами управления в системах организационно-технологического типа являются планирование, оперативно-диспетчерское управление, календарно-плановое руководство и обеспечение повседневной деятельности. При этом можно говорить о различных периодах управления - краткосрочном, среднесрочном и долгосрочном. Рассмотрим некоторые отличительные особенности данных видов управления применительно к задачам защиты информации.

Краткосрочное управление. Для этого вида управления характерно то, что можно использовать лишь те средства защиты, которые включены в состав защищаемой системы или объекта и находятся в работоспособном состоянии. При этом в общей совокупности процессов управления основную долю занимают процедуры оперативно-диспетчерского управления, т. е. динамического управления непосредственно в ходе обработки информации. Архитектура защищаемой системы и технологические схемы обработки информации какому-либо изменению не подлежат, возможны только включение и выключение тех элементов, которые уже находятся в составе системы или объекта.

Среднесрочное управление. При этом виде управления можно использовать весь арсенал имеющихся и вводимых в планируемый период средств защиты, а основными процедурами управления будут планирование и календарно-плановое руководство. Значительное место в процессах управления здесь будут занимать анализ эффективности решаемых СЗИ задач и разработка на этой основе предложений по развитию средств и методов защиты. Архитектура защищаемой системы не может быть подвергнута существенным изменениям, однако это не исключает некоторых изменений структуры в пределах имеющихся структурных элементов. Технологические схемы обработки информации могут изменяться, могут также формулироваться предложения по совершенствованию и развитию архитектуры защищаемой системы.

Долгосрочное управление. Основными процессами в этом виде управления являются перспективное планирование использования средств защиты, совершенствование концепции и систем защиты информации, разработка новых средств и методов защиты. При необходимости могут существенно изменяться как архи-

Глава 5

тектура защищаемой системы, так и технологические схемы обработки информации.

В табл. 5.1, основа которой взята нами из учебника [31], приведены перечень и содержание задач, сформированных в соответствии с изложенной классификацией процессов управления защитой информации. Подробное изложение их имеется в упомянутом учебнике, к которому мы и отсылаем заинтересованного читателя. Здесь же мы остановимся более подробно на методологических основах выработки управлеченческих решений применительно к области обеспечения защиты информации.

Как уже отмечалось, управление в общем случае представляет собой непрерывную процедуру в системе с обратной связью. Управление системами организационно-технологического типа (системами защиты информации в том числе) имеет организационные и технологические аспекты. Наиболее сложным в системе управления является процесс выработки решения. При осуществлении этого процесса должна быть правильно понята (описана) цепь выполняемого процесса, обработка информации о ходе реализации процесса должна быть осуществлена таким образом, чтобы при минимальном ее количестве можно было провести сравнение фактического состояния процесса с тем, которое должно соответствовать качественному выполнению поставленной задачи в настоящий момент времени и в прогнозируемый период.

Первой операцией при выработке управлеченческого решения является уяснение задачи, что в случае защиты информации в первую очередь определяется ее характером (общедоступная, конфиденциальная и т.д.). Необходимым элементом этой операции является уяснение конкретных элементарных задач на каждом уровне управления.

После этого можно переходить к другой операции - изучению и оценке обстановки (ситуации), в которой осуществляется процесс. Она проводится, как правило, последовательно по элементам. После оценки каждого элемента делаются выводы-обобщения. Необходимо иметь в виду, что при оценке обстановки каждый элемент рассматривается во взаимной связи с другими элементами и всей системой в целом. Такими элементами оценки обстановки могут быть:

- персонал системы (прежде всего, кому поручить выполнение тех или иных элементов задачи);
- главные направления выполнения задачи;
- последовательность действий;

- ресурсы, необходимые для выполнения задачи (материальные, финансовые, трудовые);
- техническое и программное обеспечение;
- экономическая эффективность осуществляемых операций, пространственные факторы (площадь, расстояние и т.п.);
- время выполнения осуществляемых операций;
- организационное обеспечение (структура, связь, координация, контроль и т.п.).

Изучение и оценка обстановки требуют сбора и обработки определенной информации (технической, экономической, правовой, социальной и др.). Например, в любом случае, принимая решение по организации защиты информации, необходимо анализировать ресурсы, которыми располагает защищаемая система, степень выполнения планов обработки информации, возможности ускорения создания и введение в действие тех или иных средств защиты, прогнозировать возможность срыва планов обработки информации из-за реализации угроз безопасности с целью его предупреждения.

Полный анализ всей полученной информации позволяет приступить к формулировке и отбору возможных вариантов решения проблемы защиты информации и выбору оптимального из них.

Сравнивая фактическое положение дел и их прогноз, а также учитывая информацию о внешних условиях, и вырабатывается ряд возможных решений (альтернатив), при реализации которых будет обеспечиваться достижение поставленной цели.

В соответствии с теорией управления в системах организационно-технологического типа, исходя из анализа ограничений, с учетом допустимой степени самостоятельности в принятии решения и принципов нормального протекания процесса (недопустимость потери устойчивости), можно получить допустимые альтернативы, из которых потом выбрать оптимальные, т.е. такие, при которых максимизируется показатель качества процесса.

При окончательной выработке решения, помимо максимизации показателя качества процесса, необходимо учитывать еще много различных обстоятельств, которые далеко не всегда удается описать математически и выразить в форме основного показателя процесса или ограничений.

К числу таких факторов могут относиться некоторые аспекты юридической основы, некоторые факторы, связанные с экономикой и социологией, наконец, с традициями и эмоциональными моментами. Каждый из этих факторов может повлиять на принятие того или иного решения. Поэтому заключительная фаза выработки ре-

Глава 5

Таблица 5.1

Задачи управления защитой информации

Функции управления	Вид управления по срочности		
	1. Краткосрочное	2. Среднесрочное	3. Долгосрочное
1. Планирование	1.1.1. Анализ планов обработки информации в планируемый период 1.1.2. Анализ условий защиты информации в планируемый период 1.1.3. Оценка уязвимости информации в планируемый период 1.1.4. Определение потребностей в средствах и ресурсах защиты в планируемый период 1.1.5. Оценка потенциальных возможностей механизмов защиты 1.1.6. Распределение средств защиты информации	1.2.1. Анализ реализации планов обработки информации в планируемый период 1.2.2. Прогнозирование условий защиты информации в планируемый период 1.2.3. Определение требований к защите информации в планируемый период 1.2.4. Анализ средств и ресурсов защиты, которые могут быть использованы в планируемый период	1.3.1. Анализ ожидаемых структур защищаемых систем и объектов, а также технологических схем обработки информации в планируемый период 1.3.2. Анализ ожидаемого функционального использования защищаемых систем и объектов в планируемый период 1.3.3. Ориентировочное определение требований к защите информации в планируемый период 1.3.4. Оценка ожидаемых ресурсов защиты, которые могут быть использованы в планируемый период 1.3.5. Оценка ожидаемого арсенала средств защиты информации, которые могут быть использованы в планируемый период 1.3.6. Обоснование структуры и технологии функционирования системы защиты!

Функции управления	Вид управления по срочности		
	1. Краткосрочное	2. Среднесрочное	3. Долгосрочное
1. Планирование	<p>1.1.7. Формирование графика использования средств защиты</p> <p>1.1.8. Оценка ожидаемой эффективности использования средств защиты</p>	<p>1.2.6. Ориентировочное определение заданий на защиту информации в следующие интервалы планируемого периода</p> <p>1.2.7. Распределение средств и ресурсов защиты</p>	<p>1.3.8. Определение порядка использования ресурсов и средств защиты в планируемый период</p> <p>1.3.9. Оценка ожидаемой эффективности защиты информации в планируемый период</p> <p>1.3.10. Обоснование требований к структуре защищаемых систем и объектов и технологии обработки информации, исходя из условий ее защиты</p>
2. Оперативно-диспетчерское управление		<p>2.1.1. Регулирование использования средств защиты в соответствии с разработанными планами</p> <p>2.1.2. Сбор, обработка и регистрация оперативной информации, относящейся к защите информации</p> <p>2.1.3. Распознавание сложившейся ситуации</p>	

Глава 5

Функции управления	Вид управления по срочности		
	1. Краткосрочное	2. Среднесрочное	3. Долгосрочное
2. Оперативно-диспетчерское управление	<p>2.1.4. Принятие решений на оперативное вмешательство в функционирование системы защиты</p> <p>2.1.5. Реализация принятых решений</p> <p>2.1.6. Анализ и прогнозирование развития ситуации</p> <p>2.1.7. Разработка предложений по корректировке планов защиты информации</p>		
3. Календарно-плановое руководство	<p>3.1.1. Текущая оценка состояния защиты информации</p> <p>3.1.2. Оценка требований к защите информации, определяемых непрограммными заданиями</p>	<p>3.2.1. Анализ соответствия фактического и требуемого уровня защиты</p> <p>3.2.2. Анализ изменений требований к защите информации</p> <p>3.2.3. Анализ изменения условий функционирования защищаемой системы или объекта</p>	<p>3.3.1. Анализ уровня обеспечения защиты информации</p> <p>3.3.2. Анализ качества функционирования механизмов защиты</p> <p>3.3.3. Анализ ожидаемых изменений в функциональном использоватении защищаемой системы или объекта</p> <p>3.3.4. Анализ ожидаемых изменений условий функционирования защищаемой системы или объекта</p>

Системы защиты информации

Функции управления	Вид управления по срочности		
	1. Краткосрочное	2. Среднесрочное	3. Долгосрочное
3. Календарно-планово-руководство	3.1.3. Оценка влияния на защиту изменения условий функционирования защищаемой системы или объекта 3.1.4. Корректировка текущих планов защиты 3.1.5. Разработка предложений по совершенствованию планирования защиты	3.2.4. Корректировка среднесрочных планов защиты 3.2.5. Разработка предложений по совершенствованию механизмов и развития средств защиты	3.3.5. Разработка предложений по совершенствованию структуры и технологии обработки информации или объекта и технологии обработки информации 3.3.6. Организация разработки, производства и внедрения средств защиты информации 3.3.7. Совершенствование структуры и технологии функционирования механизмов защиты
4. Обеспечение повседневной деятельности		4.1.1. Сбор дополнительной информации, относящейся к защите информации 4.1.2. Базовая обработка информации и формирование исходных данных 4.1.3. Выдача информации	4.2.1. Аналитико-синтетическая обработка данных, относящихся к защите информации 4.2.2. Формирование массивов регламентных данных 4.2.3. Выдача информации

шения в общем случае не может быть формализована и должна выполняться ЛПР. Что же касается предыдущих этапов выработки решений, то они могут быть достаточно хорошо формализованы и решены математически.

Следует отметить, что математические методы оптимизации управлеченческих решений полностью повторяют известные методы оптимального планирования. Необходимо только остановиться на случаях многокритериальных задач, когда не удается свести решение проблемы к единственному критерию оптимальности. Такого рода ситуации особенно характерны для проблемы защиты информации.

В этом случае можно использовать несколько подходов. Первый из них состоит в сведении нескольких критериев K_1, K_2, \dots, K_n к одному:

$$K = \alpha_1 K_1 + \alpha_2 K_2 + \dots + \alpha_n K_n \quad (5.35)$$

где весовые коэффициенты частных критериев α_i определяются с помощью методов экспертных оценок либо логическим анализом.

Второй подход состоит в превращении части критериев в ограничения. В тех случаях, когда удается обосновать ограничения по дополнительным критериям, такой подход вполне оправдан.

Третий подход состоит в ранжировке критериев. Оптимизацию в этом случае первоначально производят по самому важному критерию, а затем определяют область решений, где этот критерий отличается от оптимального его значения не более, чем на 10 %. В найденной таким путем области производится оптимизация по второму критерию и т.д.

Критерий должен правильно учитывать неполноту информации, которая может состоять в случайном характере используемых параметров, полной неопределенности относительно ряда параметров и даже сознательном противодействии выполнению наших задач.

Пусть, например, мы отыскиваем оптимальное значение величины a , при которой максимизируется критерий K . На величину K оказывает влияние параметр A , точное значение которого неизвестно. В этом случае необходимо задаться возможными значениями $A: A_1, A_2, \dots, A_j$; возможными значениями $a: a_1, a_2, \dots, a_i$, и для всех комбинаций этих значений рассчитать критерий K_{ij} .

Для принятия окончательного решения в качестве итогового могут использоваться критерии Лапласа, Гурвица, Сэвиджа и ряд других.

Критерий Лапласа K_{li} определяется из условия, что все значения A_i считаются равновероятными. Тогда итоговый критерий имеет вид

$$K_{li} = \sum_j K_{ij} \quad (5.36)$$

Критерий Гурвица записывается следующим образом:

$$K_{ri} = \mu K_{jmax} + (1-\mu) K_{jmin}, \quad (5.37)$$

где K_{jmax} и K_{jmin} - максимальное и минимальное значения K_{ij} для $i = l$; μ - коэффициент, выбираемый исходя из специфики задачи. При $\mu = 1$ оценка производится по наиболее выгодным результатам (оптимистическая оценка). При $\mu = 0$ оценка производится по наиболее пессимистическим данным. Этот критерий называется критерием Вальда. Он соответствует самой строгой оценке $K_{Bi} = K_{jmin}$.

Критерий Сэвиджа представляет собой «сожаление» между выбором действительным и наиболее благоприятным:

$$K_{Ci} = |K_{ij} - K_{jmax}| \quad (5.38)$$

Если известны вероятности P_j получения тех или иных величин A_j (стохастический случай), то в этом случае итоговый критерий определяется следующей формулой:

$$\bar{K}_i = \sum_j K_{ij} P_j \quad (5.39)$$

В случае полной неопределенности чаще всего используется критерий Лапласа, в случае наличия сознательного противодействия - критерий Гурвица и в ситуации случайной величины параметров с известными характеристиками - критерий (5.39).

В заключение более подробно рассмотрим возможные подходы к организации контроля защищенности информации как одной из важнейших функций управления защитой.

Под этим контролем будем понимать объективную оценку реального уровня защищенности информации, представляющего собой отношение действительного значения показателя защищенности к требуемому. На основе анализа этого отношения и принимается в дальнейшем управленческое решение по использованию тех или иных средств защиты.

Если через $P(t)$ обозначить действительное значение показателя защищенности информации в момент времени t , а через $\bar{P}(t)$ - требуемое значение этого же показателя в тот же момент времени, то при $P(t)/\bar{P}(t) < \delta P_1$, где δP_1 - допустимое снижение уровня защищенности, необходимо усиление защиты, а при $P(t)/\bar{P}(t) > \delta P_2$, где δP_2 - допустимое превышение требуемого уровня защищенности, из схемы защиты могут быть исключены некоторые функционирующие средства, что в результате приведет к экономии ресурсов, затрачиваемых на защиту.

Из методологии оценки уязвимости информации известно, что $P(t)$ зависит от целой совокупности параметров. Их перечень и содержание были достаточно подробно рассмотрены нами в гл. 3.

С учетом этого задача контроля защищенности может быть сведена к следующей последовательности мероприятий:

- сбор возможно более полных данных о всей совокупности параметров, необходимых для определения выбранных показателей защищенности;
- определение с обязательной оценкой достоверности текущих значений всех необходимых параметров;
- определение текущих значений выбранных показателей защищенности информации;
- сравнение действительных значений текущих показателей защищенности с требуемыми значениями.

Как видим, такая постановка задачи предполагает определение текущих значений показателей защищенности информации для тех моментов времени, которые уже прошли, однако на их основе должны приниматься управленические решения относительно будущих моментов времени. Чтобы устранить это противоречие, в приведенный выше перечень мероприятий необходимо включить задачу прогнозирования ожидаемых значений показателей защищенности, которое может осуществляться лишь на основании накопленных данных предыстории процесса. Таким образом, в перечне мероприятий должна быть также и задача накопления данных предыстории.

При реализации сформулированного таким образом полного перечня мероприятий контроля предполагается, что механизмы защиты функционируют в соответствии с запланированным регламентом. Однако в процессе функционирования они сами подвержены воздействию всей совокупности дестабилизирующих факто-

ров, т. е. отказам, сбоям, ошибкам, стихийным бедствиям, злоумышленным действиям и побочным влияниями. Поэтому в перечень мероприятий контроля защищенности необходимо включить также контроль функционирования самого механизма защиты. Последнее, очевидно, должно предполагать планирование контроля, оперативно-диспетчерский и календарно-плановый виды контроля, как и для всех других функций управления

С учетом всего изложенного, структура и общее содержание задач контроля защищенности представлены на рис. 5.7.

Попытаемся формализовать постановку задачи контроля защищенности, используя введенное ранее понятие оптимизации управлеченческих решений. При этом формулировка задачи приобретает следующий вид: разработать и осуществить такую совокупность мероприятий, при которой надежность контроля $P_b(\Delta P, \Delta t)$, т. е. вероятность того, что существенные отклонения показателей защищенности ΔP не останутся невыявленными в течение заданного промежутка времени Δt , - будет не ниже заданной \bar{P}_b , и при этом расходы на организацию контроля C_k будут минимальными, т. е.:

$$P_b(\Delta P, \Delta t) \geq \bar{P}_b \quad (5.40)$$

$$C_k \rightarrow \min \quad (5.41)$$

Если же по каким-либо причинам средства на организацию контроля ограничены значением \bar{C}_k , то постановка задачи видоизменяется следующим образом: разработать и осуществить совокупность мероприятий, при которых

$$C_k \leq \bar{C}_k \quad (5.42)$$

$$P_b(\Delta P, \Delta t) \rightarrow \max \quad (5.43)$$

Непосредственная организация контроля защищенности может изменяться в зависимости от поставленных прагматических целей, которые сформулируем следующим образом:

- контроль состояния параметров, определяющих значения контролируемых показателей;
- контроль наличия (проявления) типовых нарушений правил защиты информации;
- комбинированный контроль.

Первый вариант характерен тем, что контролируются только те параметры, которые, с одной стороны, определяют значения выбран-



Рис. 5.7. Структура и содержание задач контроля защищенности информации

ных показателей защищенности, а с другой - могут быть измерены непосредственно в процессе обработки защищаемой информации.

Чтобы организовать контроль в этом случае, необходимо предусмотреть решение следующих задач:

- обоснование перечня и содержания показателей защищенности, которые должны контролироваться;
- формирование минимального множества параметров, которые могут быть измерены и по значениям которых можно определить значения контролируемых показателей;
- определение точек в структуре обработки информации, где могут быть зафиксированы значения каждого из сформированного множества параметров;
- определение способов измерения параметров;
- выработка методов определения (проверки, верификации) значений параметров;
- разработка методов определения текущих и прогнозирования ожидаемых значений показателей защищенности.

Принципиально важным для данного варианта контроля является то, что непосредственному наблюдению при его реализации подвергаются элементарные параметры, что затрудняет злоумышленникам выбор пути обхода контроля. В то же время очевидно, что множество контролируемых параметров при этом должно быть достаточно представительным, а сами параметры - достаточно элементарными. Только в этом случае будет трудно определить (вскрыть) характер (содержание) контролируемых показателей защищенности.

Контроль по второму варианту заключается в том, что в процессе его реализации выявляются такие нарушения правил защиты информации, которые имели место ранее (возможно в аналогичных ситуациях), или возможность проявления которых предполагается гипотетически. Организация контроля по этому варианту предполагает решение следующих задач:

- формирование и регулярная корректировка списка потенциально возможных нарушений правил защиты;
- определение вероятностных (частотных) характеристик проявления каждого из потенциально возможных нарушений;
- определение возможных мест, условий и характера проявления каждого из нарушений;
- формирование и перманентное уточнение и пополнение списка потенциально возможных нарушений.

Преимуществами данного варианта являются наглядность контроля и практически полный учет опыта функционирования кон-

Глава 5

крайних систем или объектов. Но очевидными являются и ориентация преимущественно на предшествующий опыт, а также незамаскированность для злоумышленников с точки зрения поиска возможных путей уклонения от контроля.

Третий вариант предполагает комбинирование контроля по параметрам и типовым нарушениям. Этот вариант является общим, а потому и может рассматриваться в качестве базового при организации любых видов контроля.

Следует отметить, что в последнее время активно разворачиваются работы по созданию методов аудита информационных систем с точки зрения обеспечения их информационной безопасности. При этом основным в этих методах является контроль работы так называемых легальных пользователей (в том числе программистов, администраторов) путем ретроспективного сравнительного анализа данных об их деятельности, фиксируемых в регистрационных журналах и профилях полномочий. Целью такого анализа является выявление отклонений фактических действий контролируемых лиц от действий, разрешенных им профилями полномочий. На основе статистического анализа таких отклонений можно определить характер намерений соответствующих лиц, в том числе и злоумышленных.

Краткие выводы

1. Все ресурсы, выделяемые в тех или иных системах или объектах для защиты информации, должны быть объединены в единую, целостную, функционально самостоятельную систему защиты информации. Создание СЗИ предполагает удовлетворение целому комплексу функциональных, эргономических, экономических, технических и организационных требований.

2. С точки зрения организационного построения СЗИ представляет собой совокупность механизмов обеспечения защиты информации, механизмов управления механизмами обеспечения защиты информации и механизмов общей организации работы системы защиты. Для увязки всех подсистем СЗИ в единую целостную систему в нее вводится специальный компонент - ядро системы.

Общая структурная схема СЗИ должна включать такие элементы, как человеческий компонент (системные программисты, обслуживающий персонал, администраторы банков данных, диспетчеры и операторы защищаемой системы, администрация, пользователи, служба защиты информации), организационно-правовое обеспечение (организационно-правовые нормы и организационно-технические ме-

роприятия), привлекаемые ресурсы системы (лингвистическое, информационное, программное, математическое и техническое обеспечение).

3. Важнейшее значение для обеспечения надежности и экономичности защиты информации имеют типизация и стандартизация СЗИ. Исходя из концепции защиты информации и подходов к архитектурному построению СЗИ можно выделить три уровня типизации и стандартизации: высший - уровень СЗИ в целом, средний - уровень компонентов СЗИ и низший - уровень проектных решений по средствам и механизмам защиты.

4. Объективные предпосылки для типизации и стандартизации на высшем и среднем уровнях создает системная классификация СЗИ, включающая 6 классов и использующая такие критерии, как уровень обеспечиваемой защиты (слабая, сильная, очень сильная и особая) и активность реагирования на несанкционированные действия (пассивное, полуактивное, активное). Полная классификация учитывает дополнительно тип защищаемой системы (персональная ЭВМ, групповая ЭВМ, ВЦ предприятия, ВЦ коллективного пользования, локальная, региональная или глобальная вычислительная сеть).

Типизация и стандартизация на среднем уровне предполагает разработку типовых проектов структурно и функционально ориентированных компонентов СЗИ. В качестве наиболее перспективного варианта покомпонентной типизации и стандартизации СЗИ может быть использован подход, основанный на семиуребежной модели.

Типизация и стандартизация на низшем уровне предполагает разработку типовых проектных решений по практической реализации средств защиты информации (технических, программных, организационных и криптографических).

5. Учет множества факторов, влияющих на защиту информации и находящихся в сложном взаимодействии, приводит к представлению СЗИ как многокритериального развивающегося объекта. Для анализа СЗИ в этом случае могут быть использованы две функции полезности - ранговая функция полезности и функция полезности при анализе рисков, которые являются основой критериев для оценки политики безопасности, реализуемой системой защиты.

6. Проектирование систем защиты информации может основываться на различных подходах - от использования типовых СЗИ до разработки индивидуального проекта системы с применением индивидуальных средств защиты.

Глава 5

На основе энтропийного подхода может быть построена модель СЗИ, позволяющая найти оптимальное распределение средств защиты по различным рубежам, эффективно противодействующих прогнозируемым угрозам безопасности информации.

7. Управление функционированием СЗИ предполагает реализацию следующих макропроцессов: планирование, оперативно-диспетчерское управление, календарно-плановое руководство и обеспечение повседневной деятельности. Эти процессы могут осуществляться в условиях краткосрочного, среднесрочного и долгосрочного управления.

8. Особое значение в процедурах управления имеет регулярно осуществляемый контроль защищенности информации в защищаемой системе или объекте, который складывается из собственно контроля защищенности информации и контроля функционирования механизмов защиты. Технология контроля защищенности предусматривает контроль состояния параметров, определяющих значения контролируемых показателей, контроль проявления типовых нарушений правил защиты информации, а также комбинированный контроль по параметрам и типовым нарушениям.

Глава шестая

РАЗВИТИЕ ТЕОРИИ И ПРАКТИКИ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Основные выводы из истории развития теории и практики защиты информации

Из всего предшествующего изложения ясно, что к настоящему времени особую актуальность приобрела задача перевода защиты информации на индустриальную основу в общегосударственном масштабе. Обусловливается это прежде всего тем, что сама проблема постепенно перерастает из задачи простого обеспечения компьютерной безопасности в задачу защиты информационных ресурсов как главных ресурсов современного общества и связанную с этим задачу обеспечения информационной безопасности государства.

Детальный ретроспективный анализ истории развития методологических основ защиты информации был дан в гл. 1 данного учебного пособия, где показано, что весь процесс развития этих основ довольно четко делится на три периода, которые названы соответственно эмпирическим, эмпирико-концептуальным и теоретико-концептуальным. Характерными особенностями этих периодов являются:

- эмпирического - защита информации осуществлялась с позиций сугубо эмпирических подходов и лишь в плане предотвращения несанкционированного получения информации, находящейся в компьютерных системах;
- эмпирико-концептуального - на основе накопленного опыта удалось сформировать некие обобщенные концептуальные подходы к защите информации и сделать попытку распространения этих подходов на обеспечение целостности и качества информации (детально об этом см. [30]);
- теоретико-концептуального - концепция защиты была развита до завершенного состояния, ее положения обоснованы научно, обоснована возможность комплексной защиты информации на объекте в целом, обеспечивающей ее физическую и логическую

целостность, а также предупреждающей такие несанкционированные действия, как получение, модификацию и размножение защищаемой информации.

В последние годы были разработаны основы целостной теории защиты информации (для начала на вербальном уровне), в которой в системном плане с единых методологических позиций сформулирована и обоснована вся совокупность основных вопросов защиты в современном их понимании. Конкретно их перечень выглядит следующим образом:

- обоснована современная постановка задачи, центральным положением которой является понятие комплексной защиты информации в целевом, инструментальном и организационном отношениях;

- разработан научно-методологический базис эффективного решения задач защиты информации в виде совокупности методов классической теории систем, формально-эвристических методов (формализации эвристических приемов решения человеком сложных слабоструктуризованных задач) и неформально-эвристических методов, предусматривающих непосредственное участие человека в процессе решения задач;

- введено понятие стратегии защиты информации как генерального направления всех работ по защите, выраженного в самом общем виде, причем обоснована объективная необходимость разработки трех различных стратегий с различной целевой направленностью: оборонительной (защита от уже проявившихся угроз), наступательной (защита от наиболее опасных потенциально возможных угроз), упреждающей (защита от всех потенциально возможных угроз);

- концепция защиты информации доведена до универсального состояния, причем как с точки зрения возможностей реализации в ее рамках любой из названных выше стратегий, так и конкретных условий защиты;

- разработаны и строго обоснованы методология и модели решения всех задач, предусмотренных унифицированной концепцией защиты информации;

- разработаны способы, пути и средства практической реализации УКЗИ;

сформулированы и обоснованы перспективы развития теории и практики защиты информации, причем в качестве основных выделены следующие направления: совершенствование теоретических основ защиты информации, реализация упреждающей стратегии

защиты, перевод защиты на индустриальную основу и постепенное расширение постановки задачи до обеспечения информационной безопасности.

В настоящее время ведутся работы по совершенствованию и практической реализации теории защиты информации. Основная целевая направленность развивающегося при этом подхода была сформулирована выше как повсеместный перевод защиты информации с экстенсивных на интенсивные методы и наиболее полно обоснована в работе [51].

6.2. Перспективы развития теории и практики защиты информации

Выше в качестве наиболее вероятных перспективных направлений развития теории и практики защиты информации названы:

- 1) совершенствование теоретических основ защиты информации;
- 2) перевод защиты информации на индустриальную основу;
- 3) постепенное расширение постановки задачи до обеспечения информационной безопасности объектов, регионов и государства в целом.

Рассмотрим кратко существо и содержание возможного развития в каждом из перечисленных направлений.

Совершенствование теоретических основ защиты информации. Здесь можно выделить две основные задачи:

- обоснование полноты и, при необходимости, доработка существующей теории;
- разработка аксиоматической версии теории.

Содержание первой задачи заключается в преобразовании вербальной теории в некоторую канонизированную в смысле наличия в ней всего необходимого для решения на научной базе полного комплекса задач защиты информации. Такие работы ведутся и уже есть обнадеживающие результаты.

В качестве решения второй задачи предполагается разработка на основе вербальной теории защиты информации теории аксиоматической в виде совокупности необходимых определений, аксиом и теорем. При этом следует иметь в виду, что доказательство теорем неминуемо натолкнется на большие трудности, поскольку постулируемые в них положения и утверждения в подавляющем большинстве случаев не поддаются формализации.

Перевод защиты информации на индустриальную основу. Индустриализация каких-либо производственных процессов предполагает:

- во-первых, полную и научно обоснованную структуризацию всего производственного процесса;
- во-вторых, унификацию способов и методов выполнения всех (или по крайней мере основных) процедур производственного процесса, позволяющих обеспечить массовое их применение;
- в-третьих, регулярное и полное обеспечение процесса инструментальными средствами и всеми необходимыми ресурсами;
- в-четвертых, четкую организацию процесса и обеспечение его квалифицированными кадрами;
- в-пятых, регулярное и целенаправленное управление производственным процессом.

В процессе развития теории и практики защиты информации эволюционно шло и развитие всех перечисленных аспектов, и к настоящему времени оно достигло такого уровня, что при целенаправленном сведении их в единую целостную систему можно уверенно говорить о наличии объективных предпосылок для индустриализации процессов защиты как на отдельно взятом объекте, так и на региональном уровне, а также в общегосударственном масштабе.

К данным предпосылкам можно отнести следующие факторы:

1. Полная и научно обоснованная структуризация процессов защиты информации, которая сформировалась в результате развития теории защиты. Центральным компонентом теории является унифицированная концепция защиты информации, в рамках которой можно обеспечить надежную защиту по любой стратегии базового множества (оборонительной, наступательной, упреждающей). При этом предлагается строгая и логически стройная последовательность работ по защите информации, а именно:

- структурированное описание среды защиты;
- всесторонняя оценка уязвимости информации;
- обоснование требуемого уровня защиты;
- оптимальная организация защиты в соответствии с требуемым уровнем (обеспечиваемая кортежем концептуальных решений по защите информации, состоящим из функций защиты, задач защиты, средств защиты и системы защиты);
- обоснование условий, необходимых для эффективной защиты информации в рамках выбранной стратегии.

2. Унификация способов и методов выполнения процедур защиты информации, которая осуществлена при разработке всех без исключения компонентов УКЗИ, на основе чего сформированы полные (с точки зрения общей теории больших систем) совокупности задач анализа, синтеза и управления.

3. Обеспечение процессов защиты информации инструментальными средствами, в целях которого в ходе становления и развития теории защиты разработаны:

- общая методология защиты информации в современной постановке этой задачи;
- методы решения задач защиты информации;
- комплексы моделей для решения задач анализа систем и процессов защиты информации, синтеза оптимальных систем защиты и управления ими в процессе функционирования.

В процессе практического решения задач защиты информации разработан весьма представительный арсенал средств защиты, так что есть основания говорить о наличии достаточно развитой промышленности этих средств. При этом утвердилась классификационная структура средств защиты информации, включающая классы технических, программно-аппаратных, криптографических, нормативно-правовых, организационных и морально-этических средств.

4. Четкая организация процессов защиты информации и обеспечение их квалифицированными кадрами. Под организацией процессов защиты информации понимается создание стройной системы органов, ответственных за защиту, и внедрение в практику их работы унифицированных методов. К настоящему времени в Российской Федерации создана и развивается довольно стройная система органов, в различной степени обслуживающих решение рассматриваемой проблемы. Сейчас уже можно выделить в составе указанной системы достаточно четко обозначившиеся четыре уровня:

- высший уровень, определяющий общую политику в сфере информатизации, к которому относятся соответствующие структуры законодательной и исполнительной власти;
- средний уровень, непосредственно отвечающий за рациональную реализацию выработанной государственной политики в области защиты информации;
- уровень органов, непосредственно разрабатывающих и реализующих всю совокупность средств, методов и мероприятий по

зашите информации, к которому относятся НИИ, КБ, фирмы, специализирующиеся на исследованиях проблем защиты, разработке средств и систем защиты и оказании услуг конкретным объектам по организации и обеспечению необходимого уровня защиты. Особое место среди органов данного уровня занимают центры защиты информации, концепция организации которых рассмотрена ниже в отдельном параграфе;

- уровень органов, непосредственно реализующих все мероприятия по защите информации на конкретных объектах, которые обычно называют службами защиты информации, службами безопасности и т.п.

Так в общем виде могут быть представлены проблемы индустриализации процессов защиты информации и объективные предпосылки ее осуществления. Но само собою разумеется, что эффективное решение проблемы индустриализации в решающей степени зависит от укомплектования всех органов защиты информации (особенно специализированных центров защиты) высококвалифицированными кадрами.

К настоящему времени в Российской Федерации уже сложилась достаточно развитая система подготовки, переподготовки и повышения квалификации кадров по защите информации. Учитывая важность этой проблемы (наряду с проблемами формирования научно-методологического базиса защиты и разработки необходимого арсенала средств и методов защиты) ниже она будет рассмотрена несколько более подробно, особенно в плане ближайших и отдаленных перспектив ее решения в увязке с проблемами обеспечения информационной безопасности и создания изначально защищенных информационных технологий.

Постепенное расширение постановки задачи до обеспечения информационной безопасности. Стремительный рост роли и значимости информации в жизнедеятельности общества от простой совокупности сведений (фактов), необходимых для решения тех или иных задач, до основного ресурса на этапе постиндустриального развития с неизбежностью ставит вопрос о соответствующих способах, методах и средствах генерирования информации, ее передачи, накопления, хранения, переработки и использования. Все перечисленные процессы в соответствии с требованиями переживаемого периода должны быть переведены на поточно-индустриальную основу. Общие подходы к такому переводу рассмотрены в [5].

Сказанное целиком и полностью относится и к такому виду работы с информацией, как обеспечение ее безопасности. При этом выделяются следующие направления развития процессов защиты информации:

- расширение содержания решаемых задач;
- расширение сферы объектов и процессов, охватываемых решаемыми задачами;
- развитие научно-методологического базиса решения задач;
- развитие инструментальных средств решения задач.

Наибольший интерес здесь представляет развитие самой постановки задачи, т.е. изменение содержания тех целей, которые достигались в процессе предшествующего развития и должны достигаться в процессе развития в обозримом и более отдаленном будущем.

Ретроспективный анализ развития методологических основ защиты информации (о нем говорилось в главе 1) и логико-эвристическое прогнозирование этого развития в будущем позволяют представить эволюционирование постановки задачи защиты информации так, как показано на рис. 6.1. При этом оказывается, что решение задачи во все более расширяющейся постановке может быть обеспечено на базе разработанной и апробированной унифицированной концепции защиты информации при соответствующей интерпретации основных ее положений.

Рассмотрим более подробно выделенные на рис. 6.1 постановки задач.

Обеспечение компьютерной безопасности. Существо задачи в такой постановке, сформированной на заре возникновения самой проблемы защиты информации, заключалось в том, чтобы предотвратить несанкционированное получение информации, находящейся в компьютерных системах, лицами и программами, не имеющими на это соответствующих полномочий.

Комплексное обеспечение компьютерной безопасности. Когда были сформированы основы единой концепции решения задач защиты информации, встал вопрос о применении их для решения и других задач, входящих в понятие компьютерной безопасности, и прежде всего - обеспечения физической целостности и предупреждения несанкционированной модификации информации, находящейся в компьютерных системах. Попытки оказались успешными, расширенная таким образом задача получила название комплексного обеспечения компьютерной безопасности.

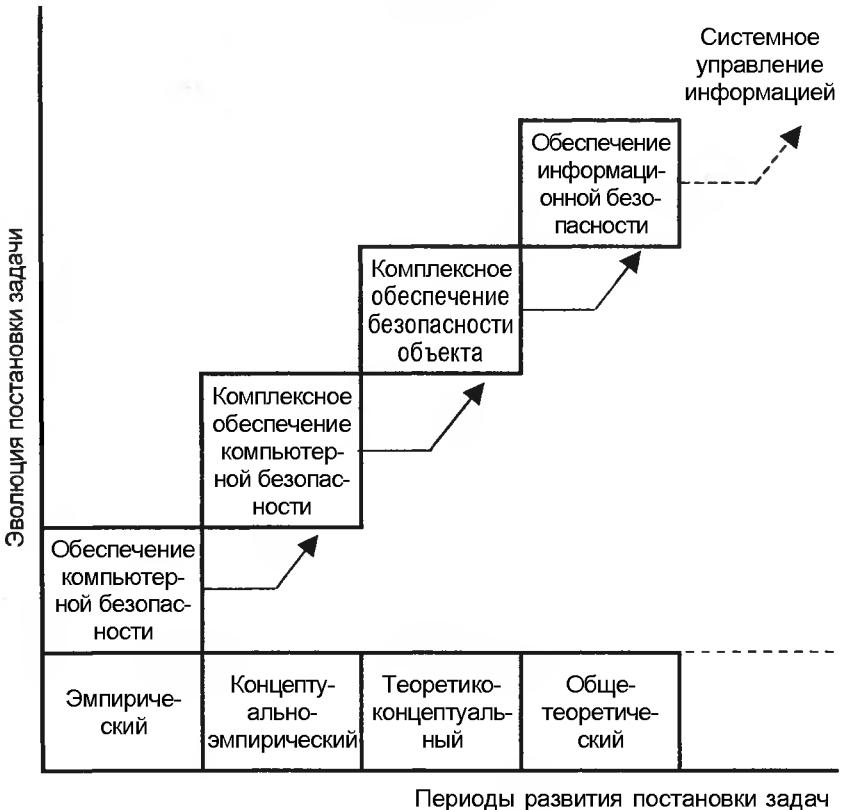


Рис. 6.1. Эволюционный путь развития постановки задачи защиты информации

Комплексное обеспечение безопасности объекта. Процессы эволюционного развития электронной вычислительной техники и ее применения в различных сферах деятельности привели к постепенному срашиванию традиционных и компьютерных информационных технологий и формированию на этой основе единых автоматизированных технологий обработки информации. Указанные технологии носят ярко выраженный человеко-машинный характер, чем предопределилась объективная необходимость перерастания постановки задачи обеспечения комплексной компьютерной безопасности в задачу комплексной защиты информации на объекте, что равносильно задаче комплексного обеспечения безопасности объектов с учетом всех аспектов понятия безопасности.

Изучение этого вопроса показало, что задача в такой расширенной постановке может быть эффективно решена на базе неоднократно упоминавшейся унифицированной концепции защиты информации. Именно в такой постановке в [31] изложены основные положения теории защиты информации, причем наиболее подходящей оказалась рассмотренная там же семиурбежная модель защиты.

Обеспечение информационной безопасности. В последние годы как остроактуальная рассматривается задача обеспечения информационной безопасности в общегосударственном масштабе. Вместе с тем конкретное содержание этой задачи до последнего времени не только не определено, но и, более того, ведутся довольно острые дискуссии, в ходе которых высказываются существенно различающиеся между собою мнения. Все сходятся на том, что проблема носит общегосударственный характер, и, следовательно, нужна государственная концепция обеспечения информационной безопасности.

Сформулированное в Доктрине информационной безопасности Российской Федерации определение понятия информационной безопасности как состояния защищенности жизненно важных интересов личности, общества и государства в информационной сфере подчеркивает сложный и многофакторный характер этой проблемы. Естественно, что решение ее может быть только многоэтапным.

Первым этапом здесь представляется изучение основных задач современного общества и роли информации в их решении. Вторым этапом следует, видимо, назвать формирование совокупности (системы) информационных проблем, обусловленных потребностями решения главных задач развития общества, и определение места в них проблем обеспечения информационной безопасности. Третий этап, очевидно, должен заключаться в поиске путей и способов формирования концептуальных подходов к решению рассматриваемой проблемы. Только после этого можно будет ставить вопрос о методах и средствах решения соответствующих задач, исходя из приведенных выше соображений, можно сформулировать следующую совокупность макрозадач, представляющих решение проблемы информационной безопасности:

- создание современной информационной инфраструктуры;
- создание и поддержка информационных ресурсов;
- защита информационной инфраструктуры и информационных ресурсов;
- защита людей от разрушающего воздействия информации;
- обеспечение готовности к информационному противоборству;

- обеспечение готовности к отражению информационной агрессии;
- обеспечение всеобщей информационной грамотности.

Как показано на рис. 6.1, в перспективе просматривается дальнейшее развитие постановки задачи в глобальную проблему управления информацией, но детальное обсуждение ее выходит за рамки данного учебного пособия.

6.3. Проблемы создания и организации работы центров защиты информации

Выше был сформулирован и обоснован принципиальный тезис о вызревании объективной необходимости и создании соответствующих предпосылок для перевода защиты информации с экстенсивного пути развития на интенсивный. Одна из отличительных особенностей интенсивного подхода заключается в объективной (и преимущественно количественной) оценке меры угроз защищаемой информации, степени требуемой защиты и расходов, необходимых для рационального построения систем защиты. Решение этих задач нуждается в больших объемах исходных данных о вероятностях проявления различных угроз в различных условиях, возможных последствиях их проявления, эффективности и стоимости нейтрализации угроз различными средствами защиты и др. Как известно, получение подавляющего большинства перечисленных данных затруднено тем, что на процессы защиты информации исключительно сильное влияние оказывают случайные неформализуемые или трудноформализуемые факторы. В силу этого оказалось, что для получения исходных данных необходимо широко использовать различного рода неформальные методы.

Кроме того, в последнее время все более обостряется проблема кадрового обеспечения защиты информации. Суть этой проблемы заключается в том, что профессия специалистов по защите информации приобретает массовый характер, а теория и практика защиты развиваются со все возрастающей скоростью. Отсюда, естественно, следует необходимость перманентного развития и совершенствования системы подготовки кадров. Применительно к подготовке молодых специалистов данная задача решается путем совершенствования учебных планов и программ. Гораздо сложнее организовать перманентное повышение квалификации действующих специалистов. Организация централизованных курсов повышения квалификации сопряжена и с большими расходами, и с отрывом все возрастающего числа специалистов от повседневной

работы, что неизбежно окажет негативное влияние на практическое решение задач защиты.

Данные обстоятельства явились побудительным мотивом формирования и дальнейшего развития концепции сети центров защиты информации, основные положения которой излагаются в данном параграфе.

Функции, задачи и структура центров защиты информации

Центр защиты информации определяется как специализированное научное, и/или производственное, и/или учебное, и/или внедренческое предприятие, профессионально ориентированное на решение всей совокупности или части задач, связанных с проведением НИР и ОКР в области защиты информации, производством (приобретением или учетом) средств защиты, оказанием услуг по созданию и поддержанию функционирования систем защиты информации, обучением (подготовкой) специалистов, имеющих отношение к защите информации.

Общей задачей, которую должны решать все ЦЗИ является формирование в пределах их компетенции и квалификации статистических данных об обеспечении информационной безопасности в пределах ареала конкретного центра, а также обмен этими данными с другими центрами.

По своему положению в структуре органов, ответственных за защиту информации в стране, ЦЗИ могут быть:

- федерального подчинения, создаваемые на уровне межведомственных структур исполнительной власти;
- ведомственного подчинения, т.е. создаваемые отдельными министерствами и ведомствами;
- региональные, т.е. создаваемые в регионах, например, в отдельных субъектах федерации или некоторой взаимосвязанной их совокупности.

Кроме того, представляется целесообразным создание некоторого головного ЦЗИ, который осуществлял бы координацию деятельности всей сети центров. В крайнем случае обязанности такого ЦЗИ можно возложить на один из центров федерального подчинения, повысив соответствующим образом его статус.

Само собой разумеется, что каждый из ЦЗИ федерального подчинения, ведомственный или региональный могут создавать свои кустовые ЦЗИ. Тогда общая структура ЦЗИ может быть представлена так, как показано на рис. 6.2.

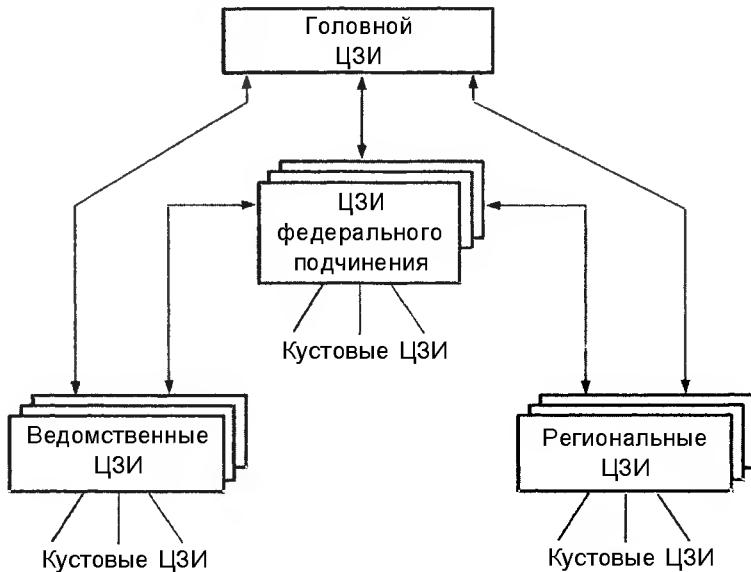


Рис. 6.2. Общая структура сети центров защиты информации

Очевидно, что наиболее эффективным путем создания сети ЦЗИ было бы использование в качестве базы для них существующих вузов и научно-исследовательских организаций, компетентных в вопросах защиты информации и имеющих опыт их решения. Примером такого подхода является сеть региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы, организованная Министерством образования Российской Федерации в 1997 году.

Важное значение имеет определение места ЦЗИ в уже сложившейся структуре органов, ответственных за защиту информации. В принципе оно может быть определено так, как показано на рис. 6.3.

Функции ЦЗИ, определяемые целями их создания и местом в системе органов, ответственных за защиту информации, очевидно, могут быть представлены в следующем виде:

а) исходя из целей создания ЦЗИ:

- формирование научно-методологического базиса защиты информации;
- формирование арсенала средств защиты информации;
- формирование баз исходных данных, необходимых для решения всего множества задач защиты информации;

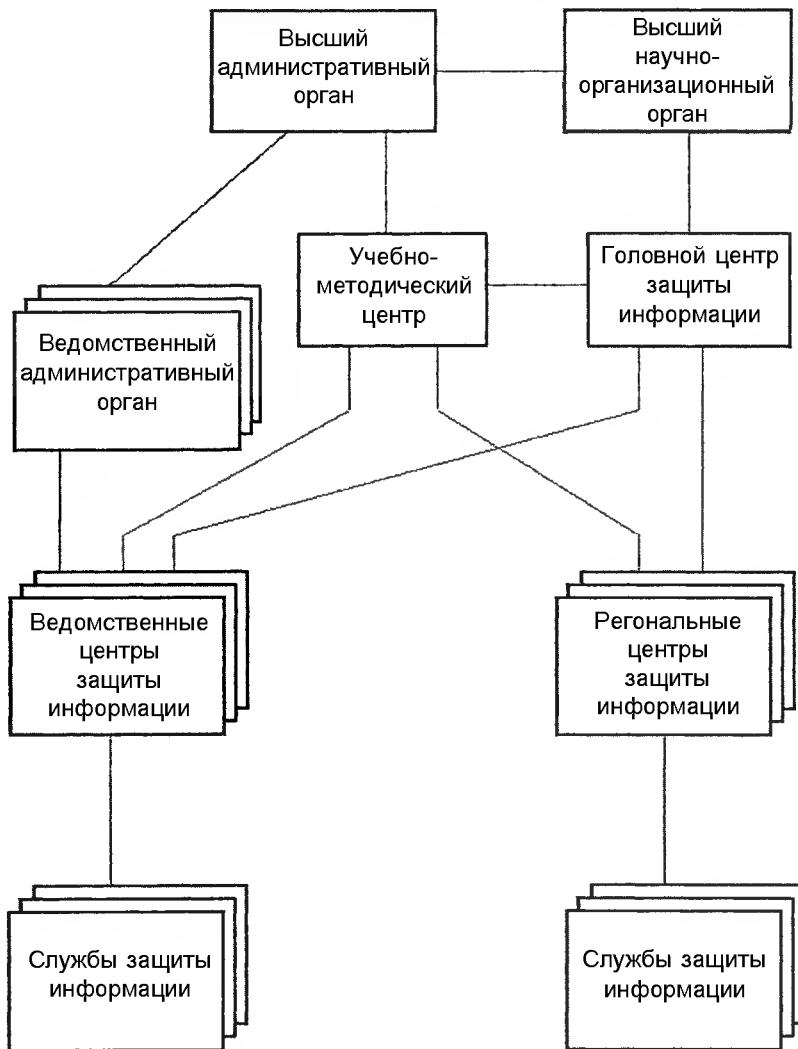


Рис. 6.3. Организационная структура органов, ответственных за защиту информации в общегосударственном масштабе

- обеспечение эффективного внедрения новейших достижений и передового опыта в практику защиты;
- кадровое обеспечение органов защиты информации.

Глава 6

б) исходя из места ЦЗИ в системе органов, ответственных за защиту информации:

- научное обоснование стратегических и организационно-административных решений по защите информации;
- обеспечение проведения единой политики в области защиты информации.

Суммируя и упорядочивая изложенное выше, мы можем представить полное множество функций ЦЗИ следующим перечнем:

- 1) формирование научно-методологического и инструментального базиса защиты информации;
- 2) научное обоснование решений по защите информации;
- 3) обеспечение проведения единой политики в области защиты информации;
- 4) формирование арсенала средств защиты;
- 5) формирование баз исходных данных, необходимых для решения задач защиты;
- 6) обеспечение эффективного и повсеместного внедрения новейших достижений и передового опыта в практику защиты;
- 7) кадровое обеспечение органов защиты информации.

Исходя из указанных функций могут быть сформулированы следующие принципы построения ЦЗИ:

- 1) функциональная и организационная самостоятельность;
- 2) высокий профессионализм;
- 3) гибкость;
- 4) разнообразие форм взаимодействия с абонентами и партнерами;
- 5) непрерывное совершенствование.

Существо перечисленных принципов практически очевидно по их названию, несколько прокомментируем лишь третий из них.

Под гибкостью какой-либо системы понимается способность ее приспосабливаться (адаптироваться) к изменению в некотором диапазоне условий, влияющих на эффективность функционирования системы. Объективная необходимость обеспечения этого свойства в структуре ЦЗИ обусловливается рядом обстоятельств, основными из которых следует назвать следующие:

- 1) широкий диапазон осуществляемых функций;
- 2) значительная размытость (не совсем строгая конкретность) формулировок большого числа функций;
- 3) необходимость участия в осуществлении большинства функций специалистов различной специализации;

- 4) невозможность строгого разделения функций между различными подразделениями центра;
- 5) естественное стремление к экономии сил и средств на создание и обеспечение функционирования сети ЦЗИ и некоторые др.

Наиболее рациональным выходом из такого положения является организация гибкой структуры ЦЗИ в составе постоянных административно-управленческих органов (должностных лиц) и руководящих групп функциональных подразделений. Основной же состав специалистов распределяется по группам центрального подчинения, которые организуются по специальностям (системотехники, технических средств защиты, программно-аппаратных средств защиты, криптографы, организационно-правовых мер защиты и т.д.). Распределение специалистов центрального подчинения между функциональными подразделениями осуществляется в процессе обоснования плана работ на соответствующий период, причем по мере неизбежной динамической корректировки планов может безболезненно осуществляться перераспределение специалистов между функциональными подразделениями.

Перечень основных функциональных подразделений для общего случая может быть следующим:

- 1) научно-методологическое;
- 2) организации и ведения баз данных инструментальных средств защиты информации;
- 3) организации и ведения баз исходных данных для решения задач защиты;
- 4) работы с абонентами ЦЗИ;
- 5) учебно-методическое.

Принцип структурной гибкости можно расширить до создания специализированных летучих подразделений при головном и кустовых ЦЗИ. Реализация такого принципа позволит создать эффективно действующую общегосударственную систему защиты информации, которая в перспективе может перерасти в общегосударственную систему управления информационными ресурсами.

Работа центров защиты информации по формированию баз данных инструментальных средств защиты

Как указывалось выше, основное назначение сети ЦЗИ заключается в организации и обеспечении перевода защиты информации в современных системах ее обработки на принципы и методы поточно-индустриального производства, что означает переход от экстен-

сивных путей защиты к интенсивным. Совершенно очевидно, что для выполнения центрами этой своей макрозадачи абсолютно необходимым является наличие полных и высокоорганизованных научно-методологического, учебно-методического и инструментального базисов, позволяющих осуществить решение всех задач, связанных с защитой информации, на регулярной основе.

Обеспечение этого условия самостоятельно и детально до настоящего времени не рассматривалось, поскольку для экстенсивных подходов к защите информации данная проблема не являлась остроактуальной, а необходимость интенсификации подходов к защите в полном объеме осознана сравнительно недавно (в прямой постановке данная задача была сформулирована в [31]), поэтому детально ее изучить и разработать еще только предстоит, хотя отдельные фрагменты задачи обсуждались в [3], [31] и некоторых других работах.

Основными компонентами рассматриваемого интегрированного базиса очевидно должны быть:

1) научно-методологическое и учебно-методическое обеспечение, представленное комплексом научных материалов, учебно-методических пособий, официальных документов по защите информации и вспомогательных материалов;

2) каталоги, содержащие в упорядоченном виде основную совокупность сведений, необходимых для организации защиты информации: объектов и элементов защиты; показателей и норм защищенности; дестабилизирующих факторов, влияющих на уязвимость информации; методов и моделей оценки уязвимости и определения требуемого уровня защищенности; функций и задач защиты; средств защиты; типовых проектных решений по защите; методов и моделей синтеза оптимальных систем защиты; методов и моделей управления системами защиты в процессе их функционирования; сведений об абонентах ЦЗИ;

3) базы исходных данных, необходимых для обеспечения решения функциональных задач ЦЗИ.

Принципиальные подходы к организации первых двух компонентов базиса рассмотрены в [31], причем рассмотрены достаточно предметно для того, чтобы приступить к практической реализации. Что касается третьего компонента, т.е. баз данных, необходимых для решения функциональных задач ЦЗИ, то в указанной выше работе показана чрезвычайная важность их создания и названы следующие способы получения необходимых данных:

1) выбор из спецификаций (паспортов, описаний и т.п.);

2) аналитические методы, базирующиеся на расчетах по известным или специально разрабатываемым зависимостям между основными параметрами определяемой величины;

3) статистические методы, основанные на сборе данных в процессе функционирования систем защиты информации (включая и постановку натурных экспериментов) или на проведении имитационного моделирования;

4) экспертные оценки в различных их модификациях.

Углубленный анализ существа задач ЦЗИ и возможностей перечисленных методов дает основания утверждать, что при современном состоянии научно-методологических основ защиты информации подавляющая часть необходимых исходных данных может быть получена лишь с использованием методов экспертных оценок. Если при этом учесть, что количество компетентных и достаточно опытных специалистов в этой области неуклонно растет, то вполне обоснованным будет вывод о целесообразности проведения массовой экспертизы в целях эффективного решения задач формирования рассматриваемых здесь баз данных.

Состав и содержание баз исходных данных, необходимых для обеспечения деятельности ЦЗИ, естественно, определяются перечнем и содержанием задач, решаемых центрами в процессе этой деятельности. Основное назначение ЦЗИ в самом общем виде может быть сформулировано как неуклонное проведение в жизнь основных положений унифицированной концепции защиты информации, которая формировалась в процессе разработки теоретических основ защиты и составляет научно-методологический базис перехода от экстенсивных на интенсивные пути решения этой проблемы.

Как следует из общей схемы УКЗИ, приведенной на рис. 1.3, основные задачи, которые будут решать ЦЗИ, могут быть разделены на следующие пять блоков:

1) структуризация среды защиты;

2) оценка уязвимости информации;

3) обоснование требований к защите информации;

4) проектирование оптимальных систем защиты;

5) организация и обеспечение функционирования систем защиты информации.

Для решения перечисленных задач необходимы следующие массивы исходных данных.

Структуризация среды защиты. Исходными данными являются возможные наборы типовых структурных компонентов и типовых их состояний. При этом для формирования графа системы обработки для общего случая, как следует из содержания предыдущих глав учебного пособия достаточно иметь 25 типов различных ТСК и 5 типовых состояний, причем для каждого ТСК должны быть определены вероятности проявления в них угроз различного вида, вероятности нахождения в них защищаемых данных, вероятности доступа к ним потенциальных нарушителей различных категорий и ожидаемого ущерба при использовании потенциально возможных угроз нарушителями различных категорий. Что касается элементов защиты, то их число и основные характеристики определяются условиями функционирования ТСК (автономно, в локальной или глобальной сети, в интересах одного пользователя или их группы и др.). Например, для такого ТСК, как персональные ЭВМ, в зависимости от условий их функционирования выделяются свыше 50 различных элементов защиты.

Оценка уязвимости информации. Выше (см. § 3.3) было показано, что несанкционированное получение информации будет иметь место в том случае, если одновременно произойдет ряд случайных (с точки зрения нарушителя) событий:

Вероятности этих событий и составляют совокупность исходных данных, необходимых для определения вероятности несанкционированного получения защищаемой информации одним злоумышленником одной категории с использованием одной угрозы одному ТСК при нахождении злоумышленника в одной зоне. Выше отмечалось (см., также, [31]), что все остальные возможные показатели уязвимости могут быть определены на основе совокупности соответствующих единичных показателей, в силу чего они и получили название базовых показателей уязвимости информации. Множество же базовых показателей определяется декартовым произведением чисел возможных значений категорий потенциально возможных нарушителей (в настоящее время их насчитывается 10), чисел зон злоумышленных действий (5), возможных чисел ТСК в системе обработки (25) и числа потенциально возможных угроз информации (в настоящее время их насчитывается около 100). Таким образом число базовых показателей уязвимости информации оценивается величиной: $10 \times 5 \times 25 \times 100 = 125000$. Если при этом учесть, что подавляющее число параметров базовых вероятностей зависит от тех условий, в которых функционируют современные системы обработки данных, то при выделении четырех типовых вариан-

тов условий общее число базовых показателей уязвимости будет достигать величины в 500000 значений. Отсюда следует, что задача формирования массива базовых показателей уязвимости должна быть отнесена к числу одной из наиболее важных и постоянно решаемых всей сетью ЦЗИ.

Обоснование требований к защите информации. В процессе создания теории защиты информации был предложен подход к определению требований к защите (см. гл. 4 данного учебного пособия), заключающийся в формировании возможно более полного множества условий, в которых может осуществляться защита информации, и делении этого множества на заданное (или отвечающее заданным условиям) число классов. Множество упомянутых выше условий определяется количеством факторов, влияющих на требуемый уровень защиты, и их значениями. Все факторы разделены на 5 групп:

- 1) факторы, обусловливаемые характером обрабатываемой информации;
- 2) факторы, обусловливаемые архитектурой системы;
- 3) факторы, обусловливаемые условиями функционирования системы;
- 4) факторы, обусловливаемые технологией обработки информации;
- 5) факторы, обусловливаемые организацией работы системы.

В первых трех группах выбрано по три различных фактора, в последних двух - по четыре, следовательно, общее число факторов равно 17. Каждый фактор оценивается четырьмя значениями. Место конкретных условий защиты информации в общем множестве определяется сочетанием трех параметров: веса группы факторов в общем перечне групп, веса фактора в своей группе и веса значения фактора среди других. Названные веса групп факторов внутри групп значений факторов и должны стать одним из элементов баз исходных данных инструментальных средств защиты информации.

Проектирование оптимальных систем защиты. Как следует из общей схемы УКЗИ, основу проектирования систем защиты информации составляет кортеж концептуальных решений по защите. Определяющим компонентом данного кортежа выступает полное множество функций защиты.

Функции защиты осуществляются посредством решения задач защиты, причем понятие задачи защиты информации интерпретируется в общепринятом смысле. Характерное отличие понятия за-

дачи от понятия функции состоит в его неопределенности: если для функций защиты удалось довольно четко и однозначно обосновать полное их множество (см., например, [31]), то множество задач защиты является неопределенным, многовариантным и в значительной мере носит субъективный характер.

В качестве базы, регулирующей процесс формирования множества задач, можно принять упоминавшуюся выше семирубежную модель защиты. Защитные меры, осуществляемые на каждом из семи рубежей, и могут быть представлены как задачи защиты информации. В целях большей определенности в формировании множества задач защиты введено понятие способов защиты, в качестве которых могут быть выделены [31]:

- 1) препятствие,
- 2) управление (регулирование),
- 3) маскировка,
- 4) регламентация,
- 5) принуждение,
- 6) побуждение.

Если для общего случая предположить, что меры защиты по каждому способу будут осуществляться на каждом рубеже защиты, то всего можно предусмотреть $7 \times 6 = 42$ группы задач защиты информации. Очень важными представляются также следующие три обстоятельства:

- 1) решением одной и той же задачи с той или иной вероятностью могут осуществляться несколько функций защиты информации;
- 2) одна и та же функция может осуществляться решением различных задач;
- 3) различные задачи защиты чаще всего будут объединяться в некоторые комплексы совместно решаемых задач.

Тогда работу ЦЗИ по формированию множества задач защиты информации можно представить следующей последовательностью мероприятий:

- 1) составляются возможно более полные перечни задач, которые могут решаться на каждом из рубежей защиты информации по всем возможным способам защиты;
- 2) из полученных перечней задач, предназначаемых для решения на каждом рубеже, формируются подмножества в соответствии с осуществлением каждой из функций защиты информации с заданной вероятностью. Нетрудно видеть, что таких наборов будет, $7 \times 7 \times 6 = 294$ (7 функций защиты, 7 рубежей защиты, 6 вариантов наборов задач);

3) осуществляется максимально возможная унификация сформированных наборов задач.

Для практического решения задач используются соответствующие средства защиты информации, причем к настоящему времени получило практически всеобщее признание деление всех средств защиты на следующие классы:

- 1) технические;
- 2) программно-аппаратные;
- 3) организационные;
- 4) криптографические;
- 5) нормативно-правовые;
- 6) социально-психологические;
- 7) морально-этические.

В каждом из данных классов уже к настоящему времени разработаны и практически используются достаточно представительные наборы различных средств, что создает хорошие предпосылки для эффективного решения сформированных наборов задач защиты информации. Иными словами, для каждого из 294 рассмотренных выше наборов задач можно предусмотреть несколько наборов средств, для каждого из которых можно разработать и сертифицировать инструментарий его реализации.

Последним рассматриваемым нами элементом кортежа концептуальных решений по защите информации является система защиты, под которой понимается высокоорганизованная совокупность всех средств, используемых для защиты в конкретных условиях функционирования конкретного объекта. На основе изложенного выше последовательность и содержание синтеза оптимальных систем защиты информации очевидны, а наличие рассмотренного фактологического базиса создает сравнительно легко реализуемые предпосылки для высокоеффективной организации защиты в очень широком диапазоне потенциально возможных целей. Уместным будет заметить, что при изложенной выше структуре баз исходных данных сравнительно легко может быть построена (например на основе динамического программирования) унифицированная процедура синтеза оптимальных систем защиты информации.

Таким образом, на основе изложенного справедливыми представляются следующие выводы:

1) для обеспечения практической реализации на регулярной основе основных положений УКЗИ необходимы большие объемы разнообразных данных, которые в настоящее время практически отсутствуют;

Глава 6

2) подавляющее большинство исходных данных носит настолько неопределенный характер, что может быть получено (по крайней мере в настоящее время и в обозримом будущем) только неформально-эвристическими методами, для чего необходимо организовать и осуществить массовые экспертные оценки;

3) значительное число исходных данных носит динамический характер, поскольку на их значения существенное влияние оказывают периодически изменяющиеся условия обработки защищаемой информации, и вследствие этого работа по формированию рассматриваемых баз данных должна вестись непрерывно;

4) в целях обеспечения организационного и методологического единства работ по формированию и сопровождению баз исходных данных проведение их наиболее целесообразно возложить на сеть ЦЗИ.

6.4. Подготовка кадров в области обеспечения информационной безопасности

Проблема обеспечения информационной безопасности может рассматриваться в трех аспектах:

- техническом, связанном с созданием защищенных средств хранения и обработки информации и их программного обеспечения;
- нормативно-правовом, устанавливающем систему законов, норм и правил формирования и организации функционирования информационной среды;
- кадровом, предусматривающем подготовку и расстановку кадров специалистов по информационной безопасности.

Учитывая, что от эффективности кадрового обеспечения в решающей степени зависит реализация задач как технического, так и нормативно-правового аспектов информационной безопасности, рассмотрим эти проблемы более подробно, опираясь на опыт их решения в Российской Федерации.

Как уже отмечалось выше, анализ современного состояния проблемы кадрового обеспечения дает нам основания утверждать, что в России в этом направлении достигнуты определенные результаты. С конца 80-х годов в области подготовки кадров по проблемам информационной безопасности активно работают как гражданские, так и военные высшие учебные заведения. В общей сложности подготовку специалистов по тем или иным аспектам безопасности информации ведут сейчас уже несколько десятков вузов. Активно издаются специальные учебники и учебные пособия.

Сложилась и некоторая система повышения квалификации специалистов по безопасности информации.

Таким образом, можно констатировать, что у нас существуют основы дееспособной системы подготовки и повышения квалификации специалистов, готовых и умеющих решать задачи обеспечения безопасности информации. Однако следует признать, что в современных условиях объективные потребности в такого рода специалистах как в количественном, так и в качественном отношении еще далеки от удовлетворения. Необходимо наращивать объем подготовки кадров, расширять номенклатуру специальностей всех уровней и категорий, широко практиковать общеобразовательные курсы информационной безопасности при подготовке кадров различной профессиональной направленности с учетом перспектив информатизации основных сфер деятельности общества, развивать целенаправленную подготовку научно-педагогических кадров высшей квалификации (кандидатов и докторов наук).

Ощущается острая нужда в подготовке кадров для правоохранительных органов, а также работников судов, способных в комплексе решать проблемы борьбы с компьютерной преступностью, включая стадии предупреждения преступлений, их обнаружения, локализации и адекватные ответные меры организационно-правового характера. Эти специалисты должны сочетать соответствующую юридическую и техническую подготовку.

Следует отметить, что практически нетронутым остается такой пласт, как подготовка кадров в области второй составляющей информационной безопасности (защиты технических систем и людей от разрушающего воздействия информации).

Справедливости ради надо сказать, что вторая составляющая информационной безопасности гораздо сложнее, многоаспектней, неопределеннее первой, что порождает особые трудности в решении соответствующих задач. Кроме того, обеспечение сколько-нибудь эффективной защиты от информации возможно лишь при наличии развитой законодательной и нормативно-правовой базы, которая в России только создается. Вместе с тем актуальность этой проблемы чрезвычайно высока, особенно в свете реальных возможностей использования информационного оружия.

Учитывая серьезность рассматриваемых проблем (как защиты информации, так и защиты от нее) Министерство образования Российской Федерации в 1996 году приняло решение о создании специального учебно-методического объединения вузов по образованию в области информационной безопасности, основной зада-

Глава 6

чей которого является разработка государственных образовательных стандартов по соответствующим направлениям подготовки кадров. По предложениям указанного объединения Министерством внесены существенные изменения в классификатор направлений и специальностей высшего профессионального образования в части создания целого блока специальностей в области информационной безопасности.

На сегодняшний день данный блок включает следующие специальности:

- криптография;
- компьютерная безопасность;
- организация и технология защиты информации;
- комплексная защита объектов информатизации;
- комплексное обеспечение информационной безопасности автоматизированных систем;
- информационная безопасность телекоммуникационных систем;
- противодействие техническим разведкам.

Рассмотренные в предыдущих главах учебного пособия научно-методологические подходы к созданию комплексных систем защиты информации явились основой формирования требований к минимуму содержания и уровню подготовки выпускников по указанной группе специальностей.

В качестве конкретного примера реализации этих требований в приложении приведен образовательный стандарт специальности «Комплексная защита объектов информатизации».

Краткие выводы

1. Анализ обобщенных итогов развития теории и практики защиты информации приводит к выводу о том, что к настоящему времени особую актуальность приобрела задача интенсификации процессов защиты и, в конечном счете, перевода защиты на индустриальную основу, причем в общегосударственном масштабе.

Одной из предпосылок успешного решения данной проблемы являются основы целостной теории защиты информации, включающей обоснование современной постановки задачи, научно-методологический базис ее решения, формирование понятия стратегии и унифицированной концепции защиты информации, обоснование методологии и моделей практической реализации УКЗИ.

2. Наиболее вероятными перспективами дальнейшего развития теории и практики защиты информации являются:

- совершенствование теоретических основ защиты;
- практическая реализация идеи интенсификации защиты информации и перевод ее на индустриальную основу;
- постепенная трансформация задачи защиты информации (в основном, обеспечения так называемой компьютерной безопасности) в задачу обеспечения информационной безопасности объектов, регионов и государства в целом.

Центральное место в ближайшей перспективе отводится проблемам перехода от экстенсивных к интенсивным методам реализации процессов защиты информации. Эффективное решение данных проблем предполагает полную и научно обоснованную структуризацию процессов защиты, унификацию способов и методов выполнения процедур защиты, обеспечение процессов защиты необходимым арсеналом инструментальных средств, четкую организацию этих процессов и обеспечение их квалифицированными кадрами.

3. Особая роль в решении вопросов совершенствования организационного обеспечения защиты информации в условиях ее интенсификации принадлежит специализированным центрам защиты. Основными задачами данных центров являются:

- проведение НИОКР в области защиты информации;
- производство (приобретение или учет) средств защиты;
- оказание услуг по созданию и поддержанию функционирования систем защиты информации;
- обучение (подготовка, переподготовка, повышение квалификации) соответствующих кадров специалистов;
- сбор и формирование статистических данных об обеспечении информационной безопасности в пределах ареала конкретного центра, а также обмен этими данными с другими центрами.

4. Для практического применения основ теории защиты информации принципиальное значение имеет формирование репрезентативных баз данных инструментальных средств защиты. Данная деятельность может рассматриваться как одна из важнейших макрозадач центров защиты информации.

В связи с тем, что подавляющее большинство исходных данных носит настолько неопределенный характер, что может быть получено (по крайней мере в настоящее время и в обозримом будущем) только неформально-эвристическими методами, возникает задача организации и осуществления процедуры непрерывной массовой экспертизы.

5. Решение современных проблем защиты информации и более общих проблем обеспечения информационной безопасности наряду с созданием защищенных средств хранения и обработки информации, разработкой и принятием системы законов, норм и правил формирования и организации функционирования информационной среды в определяющей степени зависит также от подготовки и расстановки соответствующих кадров специалистов.

В Российской Федерации к настоящему времени развернута система подготовки и повышения квалификации специалистов в области информационной безопасности. Одно из основных мест в этой системе занимает подготовка кадров по группе специальностей «Информационная безопасность».

ЗАКЛЮЧЕНИЕ

В заключение приведем некоторые общие выводы, позволяющие определенным образом систематизировать содержание современных проблем теории и практики защиты информации.

1. Суть современной постановки задачи защиты информации состоит в переходе от экстенсивных к интенсивным методам решения проблем, базирующимся на целенаправленной реализации всех достижений теории и практики защиты - структурированном описании среды защиты, всестороннем количественном анализе степени уязвимости информации на объекте, научно обоснованном определении требуемого уровня защиты на каждом конкретном объекте и в конкретных условиях его функционирования, построении оптимальных систем защиты на основе единой унифицированной методологии.

2. Основой интенсификации решения проблем защиты является научно-методологический базис нового научного направления - теории защиты информации, использующий достижения методов нечетких множеств, лингвистических переменных, экспертных оценок, неформального оценивания, неформального поиска оптимальных решений, на основе которых, разработана обобщенная модель систем и процессов защиты, структурирован процесс создания оптимальных систем защиты информации в виде кортежа концептуальных решений, составляющих существо унифицированной концепции защиты информации.

3. На основе неформально-эвристических методов разработаны также системные классификации угроз информации, потенциально возможных условий защиты, основных типов архитектурного построения систем защиты, позволяющие осуществить масштабную стандартизацию систем и процессов защиты информации, что является чрезвычайно важным с прагматической точки зрения, так как дает возможность получать решения, близкие к оптимальным, в условиях существенно ограниченных ресурсов.

4. Наиболее вероятными перспективами дальнейшего развития теории и практики защиты информации являются:

- совершенствование теоретических основ защиты информации, переход от вербальной теории защиты к аксиоматической;
- практическая реализация идеи интенсификации защиты ин-

Заключение

формации и перевод ее на индустриальную основу, предполагающие научно обоснованную структуризацию процессов защиты, унификацию способов и методов выполнения процедур защиты, обеспечение процессов защиты необходимым арсеналом инструментальных средств, четкую организацию этих процессов и обеспечение их квалифицированными кадрами;

- постепенная трансформация задачи защиты информации (в основном обеспечения компьютерной безопасности) в задачу обеспечения информационной безопасности объектов, регионов и государства в целом, как это и предусмотрено Доктриной информационной безопасности Российской Федерации.

5. Основой современного организационного обеспечения решения проблемы информационной безопасности является концепция создания специализированных центров защиты информации. На сегодняшний день данная концепция практически реализована в виде сети региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы.

6. Чрезвычайно важным аспектом решения проблемы информационной безопасности является ее кадровое обеспечение. Уровень подготовки кадров напрямую зависит от степени владения ими современными научно обоснованными методами анализа ситуаций защиты и синтеза эффективных систем противодействия угрозам. В связи с этим результаты развития теории защиты информации должны найти полное отражение в учебных планах и программах системы подготовки, переподготовки и повышения квалификации соответствующих специалистов.

ПРИЛОЖЕНИЕ

ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

**Специальность 075400
Комплексная защита объектов информатизации
Квалификация - специалист по защите информации**

1. ОБЩАЯ ХАРАКТЕРИСТИКА СПЕЦИАЛЬНОСТИ 075400- КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

1.1. Специальность утверждена приказом Министерства образования Российской Федерации.

1.2. Квалификация выпускника - специалист по защите информации.

Нормативный срок освоения основной образовательной программы подготовки специалиста по защите информации по специальности 075400 - Комплексная защита объектов информатизации при очной форме обучения составляет 5 лет.

1.3. Квалификационная характеристика выпускника.

Место специальности в области науки и техники.

Область науки и техники, охватывающая совокупность проблем, связанных с проектированием, исследованием и эксплуатацией систем комплексной защиты информации на объектах информатизации.

Объекты профессиональной деятельности.

Объектами профессиональной деятельности специалиста по защите информации по специальности 075400 (Комплексная защита объектов информатизации) являются методы, средства и системы обеспечения защиты информации на объектах информатизации.

Виды профессиональной деятельности.

Специалист по защите информации в соответствии с фундаментальной и специальной подготовкой может выполнять следующие виды профессиональной деятельности:

- экспериментально-исследовательская;
- проектная;
- организационно-управленческая;
- эксплуатационная.

Специалист по защите информации подготовлен к решению следующих задач:

- a) экспериментально-исследовательская деятельность:
 - исследование причин возникновения, форм проявления, возможности параметризации и оценки опасности физических явлений, увеличивающих вероятность нежелательного воздействия на

Приложение

информационные процессы в защищаемом объекте;

- изучение возможных источников и каналов утечки информации, составление методик расчетов и программ экспериментальных исследований по технической защите информации, выполнение расчетов в соответствии с разработанными методиками и программами;

- проведение сопоставительного анализ данных исследований и испытаний;

б) проектная деятельность:

- исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи обеспечения инженерно-технической защиты информации, в том числе с обеспечением требований соблюдения государственной тайны;

- подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по инженерно-технической защите объектов информатизации;

- проектирование и внедрение комплексных систем и отдельных специальных технических и программно-математических средств защиты информации на объектах информатизации, в том числе сравнительного анализа типовых криптосхем;

в) организационно-управленческая деятельность:

обеспечение организационных и инженерно-технических мер защиты информационных систем;

разработка предложений по совершенствованию и повышению эффективности применяемых технических мер на основе анализа результатов контрольных проверок, изучения и обобщения опыта эксплуатации объекта информатизации и опыта работы других учреждений, организаций и предприятий;

- организация работы коллектива исполнителей;

г) эксплуатационная деятельность:

- техническое обслуживание средств защиты информации;

- участие в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;

- проведение контрольных проверок работоспособности и эффективности действующих систем и технических средств защиты информации, составление и оформление актов контрольных проверок.

Приложение

1.4 Возможности продолжения образования специалиста по защите информации, освоившего основную образовательную программу высшего профессионального образования по специальности 075400 - Комплексная защита объектов информатизации.

Специалист подготовлен для продолжения образования в магистратуре и аспирантуре.

2. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ АБИТУРИЕНТА

2.1. Предшествующий уровень образования абитуриента - среднее (полное) общее образование.

2.2. Абитуриент должен иметь документ государственного образца о среднем (полном) общем образовании или среднем профессиональном образовании, или начальном профессиональном образовании, если в нем есть запись о получении предъявителем среднего (полного) общего образования, или высшем профессиональном образовании.

3. ОБЩИЕ ТРЕБОВАНИЯ К ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ ПОДГОТОВКИ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 075400 - КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

3.1. Основная образовательная программа подготовки специалиста по защите информации разрабатывается на основании настоящего государственного образовательного стандарта и включает в себя учебный план, программы учебных дисциплин, программы учебных и производственных практик.

3.2. Требования к обязательному минимуму содержания основной образовательной программы подготовки специалиста по защите информации к условиям ее реализации и срокам ее освоения определяются настоящим государственным образовательным стандартом.

3.3. Основная образовательная программа подготовки специалиста по защите информации состоит из дисциплин федерального компонента, дисциплин национально-регионального (вузовского) компонента, дисциплин по выбору студента, а также факультативных дисциплин. Дисциплины и курсы по выбору студента в каждом цикле должны содержательно дополнять дисциплины, указанные в федеральном компоненте цикла.

3.4. Основная образовательная программа подготовки специалиста по защите информации должна предусматривать изучение

Приложение

студентом следующих циклов дисциплин: цикл ГСЭ - общие гуманитарные и социально-экономические дисциплины; цикл ЕН - общие математические и естественнонаучные дисциплины; цикл ОПД - общие профессиональные дисциплины; цикл ДС - дисциплины специализации, ФТД - факультативные дисциплины, а также итоговую государственную аттестацию.

3.5. Содержание национально-регионального (вузовского) компонента основной образовательной программы подготовки специалиста по защите информации должно обеспечивать подготовку выпускника в соответствии с квалификационной характеристикой, установленной настоящим государственным образовательным стандартом.

4. ТРЕБОВАНИЯ К ОБЯЗАТЕЛЬНОМУ МИНИМУМУ СОДЕРЖАНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПОДГОТОВКИ СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ ПО СПЕЦИАЛЬНОСТИ 075400 - КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ	Общие гуманитарные и социально-экономические дисциплины	1800
ГСЭ.Ф.00	Федеральный компонент	1260
ГСЭ.Ф.01	Иностранный язык Специфика артикуляции звуков, интонации, акцентуации и ритма нейтральной речи в изучаемом языке; основные особенности полного стиля произношения, характерные для сферы профессиональной коммуникации, чтение транскрипции. Лексический минимум в объеме 4000 учебных лексических единиц общего и терминологического характера. Понятие дифференциации лексики по сферам применения (бытовая, терминологическая, общеначальная, официальная и другая). Понятие о свободных и устойчивых словосочетаниях, фразеологических единицах.	340

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.01	<p>Понятие об основных способах словообразования.</p> <p>Грамматические навыки, обеспечивающие коммуникацию общего характера без искажения смысла при письменном и устном общении, основные грамматические явления, характерные для профессиональной речи.</p> <p>Понятие об общедиалогическом, официально-деловом, научном стилях, стиле художественной литературы. Основные особенности научного стиля.</p> <p>Культура и традиции стран изучаемого языка, правила речевого этикета. Говорение. Диалогическая и монологическая речь с использованием наиболее употребительных и относительно простых лексико-грамматических средств в основных коммуникативных ситуациях неофициального и официального общения. Основы публичной речи (устное сообщение, доклад). Аудированием. Понимание диалогической и монологической речи в сфере бытовой и профессиональной коммуникации.</p> <p>Чтение. Виды текстов: несложные прагматические тексты и тексты по широкому и узкому профилю специальности.</p> <p>Письмо. Виды речевых произведений: аннотация, реферат, тезисы, сообщения, частное письмо, деловое письмо, биография.</p>	
ГСЭ.Ф.02	<p>Физическая культура</p> <p>Физическая культура в общекультурной и профессиональной подготовке студентов. Ее социально-биологические основы. Физическая культура и спорт как социальные феномены общества. Законодательство Российской Федерации о физической культуре и спорте. Физическая культура личности.</p> <p>Основы здорового образа жизни студента. Особенности использования средств физической культуры для оптимизации работоспособности.</p>	408

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.02	<p>Общая физическая и специальная подготовка в системе физического воспитания.</p> <p>Спорт. Индивидуальный выбор видов спорта или систем физических упражнений.</p> <p>Профессионально-прикладная физическая подготовка студентов.</p> <p>Основы методики самостоятельных занятий и самоконтроль за состоянием своего организма.</p>	408
ГСЭ.Ф.03	<p>Отечественная история</p> <p>Сущность, форма, функции исторического знания. Методы и источники изучения истории. Понятие и классификация исторического источника. Отечественная историография в прошлом и настоящем: общее и особенное. Методология и теория исторической науки. История России - неотъемлемая часть всемирной истории.</p> <p>Античное наследие в эпоху Великого переселения народов. Проблема этногенеза восточных славян. Основные этапы становления государственности. Древняя Русь и кочевники. Византийско-древнерусские связи. Особенности социального строя Древней Руси. Этно-культурные и социально-политические процессы становления русской государственности.</p> <p>Принятие христианства. Распространение ислама. Эволюция восточно-славянской государственности в XI-XII вв. Социально-политические изменения в русских землях в XIII-XV вв. Русь и Орда: проблемы и взаимовлияния.</p> <p>Россия и средневековые государства Европы и Азии. Специфика формирования единого российского государства. Возышение Москвы. Формирование сословной системы организации общества. Реформы Петра I. Век Екатерины. Предпосылки и особенности складывания российского абсолютизма. Дискуссии о генезисе самодержавия.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.03	<p>Особенности и основные этапы экономического развития России. Эволюция форм собственности на землю. Структура феодального землевладения. Крепостное право в России. Мануфактурно-промышленное производство. становление индустриального общества в России: общее и особенное.</p> <p>Общественная мысль и особенности общественного движения России XIX в. Реформы и реформаторы в России. Русская культура XIX века и ее вклад в мировую культуру.</p> <p>Роль XX столетия в мировой истории. Глобализация общественных процессов. Проблема экономического роста и модернизации. Революции и реформы. Социальная трансформация общества. Столкновение тенденций интернационализма и национализма, интеграции и сепаратизма, демократии и авторитаризма.</p> <p>Россия в начале XX века. Объективная потребность индустриальной модернизации России. Российские реформы в контексте общемирового развития в начале века. Политические партии России: генезис, классификация, программы, тактика.</p> <p>Россия в условиях мировой войны и общенационального кризиса. Революция 1917 г. Гражданская война и интервенция, их результаты и последствия. Российская эмиграция. Социально-экономическое развитие страны в 20-е гг. НЭП. Формирование однопартийного политического режима.</p> <p>Образование СССР. Культурная жизнь страны в 20-е гг. Внешняя политика. Курс на строительство социализма в одной стране и его последствия.</p> <p>Социально-экономические преобразования в 30-е гг. Усиление режима личной власти Сталина. Сопротивление сталинизму.</p> <p>СССР накануне и в начальный период второй мировой войны. Великая отечественная война.</p> <p>Социально-экономическое развитие, общественно-политическая жизнь, культура, внешняя политика СССР в послевоенные годы. Холодная война.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.03	<p>Попытки осуществления политических и экономических реформ. НТР и ее влияние на ход общественного развития. СССР в середине 60-80-х гг.: нарастание кризисных явлений.</p> <p>Советский Союз в 1985-1991 гг. Перестройка. Попытка государственного переворота 1991 г. и ее провал. Распад СССР. Беловежские соглашения. Октябрьские события 1993 г.</p>	
ГСЭ.Ф.04	<p>Культурология</p> <p>Структура и состав современного культурологического знания. Культурология и философия культуры, социология культуры, культурная антропология. Культурология и история культуры. Теоретическая и прикладная культурология. Методы культурологических исследований. Основные понятия культурологии: культура, цивилизация, морфология культуры, функции культуры, субъект культуры, культурогенез, динамика культуры, язык и символы культуры, культурные коды, межкультурные коммуникации, культурные ценности и нормы, культурные традиции, культурная картина мира, социальные институты культуры, культурная самоидентичность, культурная модернизация.</p> <p>Типология культур. Этническая и национальная, элитарная и массовая культуры. Восточные и западные типы культур. Специфические и «серединные» культуры. Локальные культуры. Место и роль России в мировой культуре. Тенденции культурной универсализации в мировом современном процессе.</p> <p>Культура и природа. Культура и общество. Культура и глобальные проблемы современности. Культура и личность. Инкультурация и социализация.</p>	
ГСЭ.Ф.05	<p>Политология</p> <p>Объект, предмет и метод политической науки. Функции политологии.</p> <p>Политическая жизнь и властные отношения. Роль и место политики в жизни современных обществ. Социальные функции политики.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.05	<p>История политических учений. Российская политическая традиция: истоки, социокультурные основания, историческая динамика. Современные политологические школы.</p> <p>Гражданское общество, его происхождение и особенности. Особенности становления гражданского общества в России.</p> <p>Институциональные аспекты политики. Политическая власть. Политическая система. Политические режимы, политические партии, электоральные системы.</p> <p>Политические отношения и процессы. Политические конфликты и способы их разрешения.</p> <p>Политические технологии. Политический менеджмент. Политическая модернизация.</p> <p>Политические организации и движения. Политические элиты. Политическое лидерство.</p> <p>Социокультурные аспекты политики.</p> <p>Мировая политика и международные отношения. Особенности мирового политического процесса. Национально-государственные интересы РОССИИ в новой геополитической ситуации.</p> <p>Методология познания политической реальности. Парадигмы политического знания. Экспертное политическое знание; политическая аналитика и прогнозистика.</p>	
ГСЭ.Ф.06	<p>Правоведение</p> <p>Государство и право, личность и общество.</p> <p>Структура права и его действия.</p> <p>Конституционная основа правовой системы.</p> <p>Частное право. Закон и подзаконные акты.</p> <p>Понятие преступления. Уголовная ответственность.</p> <p>Экологическое право.</p> <p>Правовое регулирование профессиональной деятельности.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.07	<p>Психология и педагогика</p> <p>Психология: предмет, объект и методы психологии. Место психологии в системе наук. История развития психологического знания и основные направления в психологии. Индивид, личность, субъект, индивидуальность.</p> <p>Психика и организм. Психика, поведение и деятельность. Основные функции психики.</p> <p>Развитие психики в процессе онтогенеза и филогенеза.</p> <p>Мозг и психика.</p> <p>Структура психики. Соотношение сознания и бессознательного. Основные психические процессы. Структура сознания.</p> <p>Познавательные процессы. Ощущение. Восприятие. Представление. Воображение. Мышление и интеллект. Творчество. Внимание.</p> <p>Мнемические процессы.</p> <p>Эмоции и чувства.</p> <p>Психическая регуляция поведения и деятельности.</p> <p>Общение и речь.</p> <p>Психология личности.</p> <p>Межличностные отношения.</p> <p>Психология малых групп.</p> <p>Межгрупповые отношения и взаимодействия.</p> <p>Педагогика: объект, предмет, задачи, функции, методы педагогики. Основные категории педагогики: образование, воспитание, обучение, педагогическая деятельность, педагогическое взаимодействие, педагогическая технология, педагогическая задача.</p> <p>Образование как общечеловеческая ценность. Образование как социокультурный феномен и педагогический процесс. Образовательная система России. Цели, содержание, структура непрерывного образования, единство образования и самообразования.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.07	<p>Педагогический процесс. Образовательная, воспитательная и развивающая функции обучения,</p> <p>Воспитание в педагогическом процессе.</p> <p>Общие формы организации учебной деятельности. Урок, лекция, семинарские, практические и лабораторные занятия, диспут, конференция, зачет, экзамен, факультативные занятия, консультация. Методы, приемы, средства организации и управления педагогическим процессом.</p> <p>Семья как субъект педагогического взаимодействия и социокультурная среда воспитания и развития личности. Управление образовательными системами.</p>	
ГСЭ.Ф.08	<p>Русский язык и культура речи</p> <p>Стили современного русского языка. Языковая норма, ее роль в становлении и функционировании литературного языка. Речевое взаимодействие. Основные единицы общения. Устная и письменная разновидности литературного языка. Нормативные, коммуникативные, этические аспекты устной и письменной речи.</p> <p>Функциональные стили современного русского языка. Взаимодействие функциональных стилей. Научный стиль. Специфика использования элементов различных языковых уровней в научной речи. Речевые нормы учебной и научной сфер деятельности.</p> <p>Официально-деловой стиль, сфера его функционирования, жанровое разнообразие. Языковые формулы официальных документов.</p> <p>Приемы унификации языка служебных документов.</p> <p>Интернациональные свойства русской официально-деловой письменной речи. Язык и стиль распорядительных документов. Язык и стиль коммерческой корреспонденции. Язык и стиль инструктивно-методических документов. Реклама в деловой речи. Правила оформления документов. Речевой этикет в документе.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.08	<p>Жанровая дифференциация и отбор языковых средств в публицистическом стиле. Особенности устной публичной речи. Оратор и его аудитория. Основные виды аргументов. Подготовка речи: выбор темы, цель речи, поиск материала, начало, развертывание и завершение речи. Основные приемы поиска материала и виды вспомогательных материалов. Словесное оформление публичного выступления. Понятливость, информативность и выразительность публичной речи.</p> <p>Разговорная речь в системе функциональных разновидностей русского литературного языка. Условия функционирования разговорной речи, роль внеязыковых факторов.</p> <p>Культура речи. Основные направления совершенствования навыков грамотного письма и говорения.</p>	
ГСЭ.Ф.09	<p>Социология</p> <p>Предыстория и социально-философские предпосылки социологии как науки. Социологический проект О.Конта. Классические социологические теории. Современные социологические теории. Русская социологическая мысль.</p> <p>Общество и социальные институты. Мировая система и процессы глобализации. Социальные группы и общности. Виды общностей. Общность и личность. Малые группы и коллективы. Социальная организация.</p> <p>Социальные движения.</p> <p>Социальное неравенство, стратификация и социальная мобильность. Понятие социального статуса.</p> <p>Социальное взаимодействие и социальные отношения. Общественное мнение как институт гражданского общества.</p> <p>Культура как фактор социальных изменений. Взаимодействие экономики, социальных отношений и культуры.</p> <p>Личность как социальный тип. Социальный контроль и девиация. Личность как деятельный субъект.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.09	<p>Социальные изменения. Социальные революции и реформы. Концепция социального прогресса. Формирование мировой системы. Место России в мировом сообществе.</p> <p>Методы социологического исследования.</p> <p>Философия</p> <p>Предмет философии. Место и роль философии в культуре. Становление философии. Основные направления, школы философии и этапы ее исторического развития. Структура философского знания.</p> <p>Учение о бытие. Монистические и плюралистические концепции бытия, самоорганизация бытия. Понятие материального и идеального. Пространство, время. Движение и развитие, диалектика. Детерминизм и индетерминизм.</p> <p>Динамические и статистические закономерности. Научные, философские и религиозные картины мира.</p> <p>Человек, общество, культура. Человек и природа. Общество и его структура. Гражданское общество и государство. Человек в системе социальных связей. Человек и исторический процесс; личность и массы; свобода и необходимость. Формационная и цивилизационная концепции общественного развития.</p> <p>Смысл человеческого бытия. Насилие и ненасилие. Свобода и ответственность. Мораль, справедливость, право. Нравственные ценности. Представления о совершенном человеке в различных культурах. Эстетические ценности и их роль в человеческой жизни. Религиозные ценности и свобода совести.</p> <p>Сознание и познание. Сознание, самосознание и личность. Познание, творчество, практика. Вера и знание. Понимание и объяснение. Рациональное и иррациональное в познавательной деятельности. Проблема истины. Деятельность, мышление, логика и язык. Научное и вненаучное знание. Критерии научности.</p>	
ГСЭ.Ф.10	<p>Философия</p> <p>Предмет философии. Место и роль философии в культуре. Становление философии. Основные направления, школы философии и этапы ее исторического развития. Структура философского знания.</p> <p>Учение о бытие. Монистические и плюралистические концепции бытия, самоорганизация бытия. Понятие материального и идеального. Пространство, время. Движение и развитие, диалектика. Детерминизм и индетерминизм.</p> <p>Динамические и статистические закономерности. Научные, философские и религиозные картины мира.</p> <p>Человек, общество, культура. Человек и природа. Общество и его структура. Гражданское общество и государство. Человек в системе социальных связей. Человек и исторический процесс; личность и массы; свобода и необходимость. Формационная и цивилизационная концепции общественного развития.</p> <p>Смысл человеческого бытия. Насилие и ненасилие. Свобода и ответственность. Мораль, справедливость, право. Нравственные ценности. Представления о совершенном человеке в различных культурах. Эстетические ценности и их роль в человеческой жизни. Религиозные ценности и свобода совести.</p> <p>Сознание и познание. Сознание, самосознание и личность. Познание, творчество, практика. Вера и знание. Понимание и объяснение. Рациональное и иррациональное в познавательной деятельности. Проблема истины. Деятельность, мышление, логика и язык. Научное и вненаучное знание. Критерии научности.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.10	<p>Структура научного познания, его методы и формы. Рост научного знания. Научные революции и смены типов рациональности. Наука и техника.</p> <p>Будущее человечества. Глобальные проблемы современности. Взаимодействие цивилизаций и сценарии будущего.</p>	
ГСЭ.Ф.11	<p>Экономика</p> <p>Введение в экономическую теорию. Блага. Потребности, ресурсы. Экономический выбор. Экономические отношения. Экономические системы. Основные этапы развития экономической теории. Методы экономической теории.</p> <p>Микроэкономика. Рынок. Спрос и предложение. Потребительские предпочтения и предельная полезность. Факторы спроса. Индивидуальный и рыночный спрос. Эффект дохода и эффект замещения. Эластичность. Предложение и его факторы. Закон убывающей предельной производительности.</p> <p>Эффект масштаба. Виды издержек. Фирма. Выручка и прибыль. Принцип максимизации прибыли. Предложение совершенно конкурентной фирмы и отрасли. Эффективность конкурентных рынков. Рыночная власть. Монополия. Монополистическая конкуренция. Олигополия. Антимонопольное регулирование. Спрос на факторы производства. Рынок труда. Спрос и предложение труда. Заработная плата и занятость. Рынок капитала. Процентная ставка и инвестиции. Рынок земли. Рента. Общее равновесие и благосостояние. Распределение доходов. Неравенство. Внешние эффекты и общественные блага. Роль государства.</p> <p>Макроэкономика. Национальная экономика как целое. Кругооборот доходов и продуктов. ВВП и способы его измерения. Национальный доход. Располагаемый личный доход. Индексы цен. Безработица и ее формы. Инфляция и ее виды. Экономические циклы. Макроэкономическое равновесие.</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ГСЭ.Ф.11	Совокупный спрос и совокупное предложение. Стабилизационная политика. Равновесие на товарном рынке. Потребление и сбережения. Инвестиции. Государственные расходы и налоги. Эффект мультипликатора. Бюджетно-налоговая политика. Деньги и их функции. Равновесие на денежном рынке. Денежный мультипликатор. Банковская система. Денежно-кредитная политика. Экономический рост и развитие. Международные экономические отношения. Внешняя торговля и внешняя политика. Платежный баланс. Валютный курс. Особенности переходной экономики России. Приватизация. Формы собственности. Предпринимательство. Теневая экономика. Рынок труда. Распределение и доходы. Преобразования в социальной сфере. Структурные сдвиги в экономике. Формирование открытой экономики.	
ГСЭ.Р.00	Национально-региональный (вузовский) компонент	270
ГСЭ.В.00	Дисциплины и курсы по выбору студента, устанавливаемые вузом	270
ЕН	Общие математические и естественнонаучные дисциплины	1400
ЕН.Ф.00	Федеральный компонент	950
ЕН.Ф.01	Концепции современного естествознания: основные понятия: концепция, научные знания и их уровни; естествознание, его состав, основные черты и закономерности развития; роль и значение физики на различных этапах развития естествознания; сущность современных концепций релятивистской и квантовой физики и их значимость для развития химии, биологии и других наук о природе; этапы развития и возраст вселенной; сущность механизма взаимодействия и основные виды силовых полей; смысл и фундаментальность законов сохранения; иерархия строения вещества и естествознание; космос и биосфера; информация и ее роль в природе и обществе.	140

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН.Ф.02	<p>Математика</p> <p>Математический анализ: вещественные и комплексные числа; последовательности и их пределы; свойства пределов последовательностей; непрерывные функции и их основные свойства; основные элементарные функции; производные и дифференцируемые функции; производные высших порядков; формула Тейлора; первообразные и неопределенные интегралы; числовые ряды, признаки сходимости; абсолютно сходящиеся ряды; функциональные последовательности и ряды; признаки равномерной сходимости; степенные ряды и их свойства; ряд Тейлора; интеграл Римана-Стильтеса; интеграл Римана; критерии интегрируемости; метрические пространства; фундаментальные последовательности; полные пространства; компактные множества; связные множества; равномерная непрерывность; дифференцируемые отображения; полная производная; дифференциал; дивергенция, ротор, градиент, якобианы; формула и ряд Тейлора для вещественной функции многих переменных; интегралы Фурье; ряды Фурье; признаки сходимости; понятие меры; измеримые функции и их свойства; абстрактный интеграл Лебега и его основные свойства; связь интегралов Лебега и Римана.</p> <p>Алгебра:</p> <p>элементы комбинаторики; внутренние бинарные операции на множестве; основные алгебраические структуры: полугруппы, группы, кольца, поля и их простейшие свойства; операции над матрицами; элементарные преобразования матриц; определители матриц; обратимые матрицы; ранг матрицы над полем; система линейных уравнений над полем; делимость и деление с остатком в кольце целых чисел; основная теорема арифметики; поле комплексных чисел; кольца вычетов; уравнения в кольце вычетов и сравнения; кольцо многочленов;</p>	450

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН.Ф.02	<p>каноническое разложение многочлена; свойства элементов группы, подгруппы группы; разложение группы в смежные классы и классы сопряженных элементов; произведение подгрупп; группа подстановок; нормальные делители группы; конечные абелевы группы; векторное пространство; конечномерные векторные пространства; подпространства; линейные преобразования векторных пространств; подобие матриц над полем; евклидовы и унитарные пространства; квадратичные формы; основные свойства элементов кольца, подкольца и идеалы кольца; прямые суммы колец и идеалов; простые поля; поле разложения многочлена; конечные поля; многочлены над конечными полями; нормальные формы матрицы над полем.</p> <p>Геометрия:</p> <p>векторная алгебра; системы координат на плоскости и в пространстве; прямая линия на плоскости; кривые второго порядка на плоскости; прямая линия и плоскость в пространстве; поверхности второго порядка.</p> <p>Теория вероятностей и математическая статистика:</p> <p>аксиоматика теории вероятностей; комбинаторно-вероятностные схемы; биномиальная и полиномиальная схемы; случайные величины и их распределения; случайные векторы и их распределения; многомерное нормальные распределение; виды сходимости последовательностей случайных величин; характеристические функции и их свойства; закон больших чисел; локальная предельная теорема для решетчатых случайных величин; центральная предельная теорема; дискретные цепи Маркова; дискретные марковские процессы с непрерывным временем; пуссоновский процесс и его свойства; стационарные случайные процессы; точечное и доверительное оценивание параметров распределений; методы получения оценок; критерии согласия; проверка статистических гипотез; последовательный анализ; метод</p>	

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН.Ф.02	<p>наименьших квадратов; основы статистической теории распознавания образов; основы статистической теории выделения сигналов на фоне помех.</p> <p>Теория функций комплексного переменного: голоморфные функции; условия Коши-Римана; степенные ряды в комплексной области; аналитические функции и их основные свойства.</p>	
ЕН.Ф.03	<p>Физика</p> <p>Физические основы механики: понятие состояния в классической механике, законы поступательного и вращательного движения тел; законы сохранения; силы в механике: упругость, трение, тяготение; статическое силовое поле, напряженность и потенциал, связь между ними; электричество и магнетизм:</p> <p>электростатика; электрические свойства вещества; постоянный ток в различных средах; законы электромагнетизма; движение заряженных частиц в электрических и магнитных полях; магнитные свойства вещества; уравнения Максвелла в интегральной и дифференциальной форме, материальные уравнения, квазистационарные токи; физика колебаний и волн: гармонический и ангармонический осциллятор, физический смысл спектрального разложения; свободные и вынужденные колебания механических и электрических осцилляторов, электромеханические аналогии; цепи переменного тока; кинематика волновых процессов; поляризация, интерференция и дифракция волн, основы голографии; тепловое излучение; квантовая физика: корпускулярно-волновой дуализм, принцип неопределенности, квантовые состояния, принцип суперпозиции, волновые функции, туннельный эффект, энергетический спектр атомов и молекул; основы термодинамики: три начала, термодинамические функции состояния, энтропия; фазовые равновесия и фазовые превращения, элементы неравновесной термодинамики; физические основы защиты информации:</p>	550

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН.Ф.03	поля объектов и проблема защиты информации, физические поля различной природы как носители информации об объектах, общие принципы регистрации информативных характеристик полей; электрические, магнитные и электромагнитные поля объектов, электромагнитные волны, их характеристики, свойства и особенности распространения, в различных средах, ближняя и дальняя зоны излучателя, распространение полей в неоднородных средах, принципы экранирования статических и динамических полей; упругие волны, их характеристики, основы акустики речи и слуха, специфика акустики помещений, звукоизоляция, инфразвук, ультразвук.	
ЕН.Ф.04	Информатика научно-технический прогресс и информатизация постиндустриального общества; основные проблемы информационного обеспечения науки, техники, производства и управления; информационный ресурс, его потенциал и возможности использования; информационная модель объекта деятельности специалиста; информатизация управленческого решения; семантика и формализация в информатизации (источники информации, потребительские свойства, семантико-лингвистические и терминологические проблемы, системы классификации, кодирования и организации информации); информационные системы - основной инструмент информатизации; взаимосвязь процессов компьютеризации и информатизации; информационные технологии; информационные системы (классификация, структуры, назначение, общая характеристика, эффективность); основные формы, принципы, организация личного и корпоративного информационного обеспечения; организационно-экономические аспекты информатизации; понятие технико-экономического обоснования информатизации; маркетинг информационных продуктов и услуг; системно-информационный анализ и синтез в информатизации.	200

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН.Ф.05	Экология биосфера и человек: структура биосферы; экосистемы; взаимоотношения организма и среды; экология и здоровье человека; глобальные проблемы окружающей среды; экологические принципы рационального использования природных ресурсов и охраны природы; основы экономики природопользования; экозащитная техника и технологии; основы экологического права, профессиональная ответственность; международное сотрудничество в области окружающей среды.	60
ЕН Ф.06	Математическая логика и теория алгоритмов формулы алгебры высказываний; представление булевых функций формулами; критерии полноты систем булевых функций; псевдобулевые функции и их представление рядами Фурье; критерии полноты систем функций К-значной логики; классификация функций К-значной логики; минимизация булевых функций; исчисления высказываний и предикатов, их полнота и непротиворечивость; основные подходы к формализации понятия алгоритма; понятие о сложности алгоритмов; вычислительные алгоритмы.	50
ЕН Ф.07	Дискретная математика конечные автоматы; автоматные базисы и проблема полноты; эквивалентность в автоматах; автоматные языки; понятие формальной грамматики; применение грамматик для построения языков высокого уровня; эксперименты с автоматами; тестирование автоматов; вероятностные автоматы; графы и орграфы; изоморфизмы; деревья; эйлеровы графы; планарные графы; покрытия и независимые множества; сильная связность в орграфах; анализ графа цепи Маркова; алгоритмы поиска кратчайших путей в графах; задача поиска гамильтонова цикла в графе; задача о коммивояжере; принцип включения-исключения; рекуррентные соотношения исключения; рекуррентные соотношения и	100

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ЕН Ф.07	производящие функции; трансверсали; латинские прямоугольники и квадраты; комбинаторные конфигурации, блок-схемы; конечные проективные плоскости; ортогональные латинские квадраты; матрицы Адамара; перечисление графов и отображений; экстремальные задачи; оптимизационные задачи; универсальные задачи; метод ветвей и границ; теоретико-автоматные модели протоколов взаимодействия компонент вычислительной сети; модели шифрсистем; потоковые модели безопасности компьютерных систем.	
ЕН Ф.08	Теория информации энтропия вероятностной схемы; аксиомы Хинчина и Фаддеева; условная энтропия; взаимная информация и ее свойства; источники информации; энтропия источников; дискретный источник без памяти; теоремы Шеннона об источниках; марковские и эргодические источники; информационная дивергенция; граница Симмонса; оптимальное кодирование; префиксные коды; неравенство Крафта; линейные коды; параметры кодов и их границы; корректирующие свойства кодов; циклические коды; БЧХ - коды; код Хемминга; сверточные коды; математическая модель канала связи; пропускная способность канала связи; прямая и обратная теоремы кодирования.	50
ЕН.Р.00	Национально-региональный (вузовский) компонент	200
ЕН.В.00	Дисциплины и курсы по выбору студента, устанавливаемые вузом	150
ОПД	Общие профессиональные дисциплины	3440
ОПД.Ф.00	Федеральный компонент	250
ОПД.Ф.01	Введение в специальность Сущность специальности 075400 - «Комплексная защита объектов информатизации», характеристика ее составляющих; взаимосвязь специальности с другими специальностями в области информационной безопасности; место	50

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.01	специальности в области науки и техники; объекты и виды профессиональной деятельности выпускника по специальности; требования Государственного образовательного стандарта к уровню подготовки специалиста; содержание образовательной программы, сущность и краткая характеристика дисциплин, входящих в образовательную программу, их взаимосвязь и место в подготовке специалистов; особенности организации образовательного процесса по дисциплинам специальности.	
ОПД.Ф.02	<p>Аппаратные средства вычислительной техники</p> <p>системы счисления; форматы представления данных и кодирование информации; выполнение арифметических операций; элементы и узлы ЭВМ; структура центрального процессора; организация и структура памяти; системы прерывания; системы ввода-вывода; периферийные устройства; микропроцессорная техника: понятие микропроцессора (МП); виды технологии производства МП, поколения МП и их основные характеристики; обобщенная структура МП; основные промышленные линии микропроцессоров; перспективные МП; ПЭВМ, рабочие станции и серверы: архитектура ПЭВМ, рабочих станций и серверов, системная магистраль, буферизация шин, управление системной магистралью, подключение дополнительных и интерфейсных схем;</p> <p>универсальные и специализированные ЭВМ высокой производительности; архитектура специализированных вычислительных комплексов: архитектура комплексов, ориентированных на программное обеспечение, машины баз данных, объектно-ориентированная архитектура.</p>	130
ОПД.Ф.03	<p>Методы программирования и прикладные алгоритмы</p> <p>современные технологии программирования; оценка качества программного обеспечения; общие принципы методы и средства проекти-</p>	160

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОГД.Ф.03	<p>рования архитектуры и структуры, проектирования логики, тестирования и отладки, документирования и сопровождения программного обеспечения с учетом повышенных требований к надежности программ и их защищенности от несанкционированного доступа; САЗЕ-технологии, технологии виртуального программирования и объектно-ориентированного программирования; применение математических методов в проектировании надежного и защищенного программного обеспечения: функциональное программирование, логическое программирование; структуры данных и абстракции данных; оценка сложности алгоритмов; модели вычислений; алгоритмы сортировки, алгоритмы поиска; алгоритмы на графах; генерация случайных последовательностей; алгоритмы на подстановках; параллельные алгоритмы: методы проектирования параллельных алгоритмов, оценки сложности.</p>	
ОГД.Ф.04	<p>Электротехника и электроника Основные положения теории электрических цепей: электрические цепи при гармоническом и импульсном воздействии, частотные характеристики электрических цепей, фильтры; многофазные электрические системы; цепи с распределенными параметрами: основные характеристики, распространение гармонических и импульсных сигналов; основы полупроводниковой электроники: принцип действия, характеристики, особенности практического применения полупроводниковых диодов, биполярных, полевых транзисторов, тиристоров и оптоэлектронных приборов; основные типы электронных устройств, особенности схемотехники и принципы функционирования усилителей и генераторов электрических колебаний; особенности аналоговой и цифровой микросхемотехники; основы функциональной схемотехники логических элементов; функциональный и схемотехнический анализ цифровых устройств: сумматор, дешифраторы, логические коммутаторы,</p>	250

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.04	преобразователи кодов; триггеры, регистры, счетчики; функциональные особенности микропроцессоров; устройства формирования, преобразования и хранения сигналов, компараторы сигналов, цифро-аналоговые и аналого-цифровые преобразователи информации; системы питания электронных устройств; электронные приборы отображения информации; основные понятия конструкции и технологии электронных устройств; основы электромеханики, электромеханические приборы ввода, вывода и обработки информации; причины образования возможных каналов утечки информации в электронных устройствах.	
ОПД Ф.05	Основы радиотехники излучение электромагнитных волн; направляющие системы и направляемые волны; резонаторы; распространение радиоволн; передающие и приемные антенные системы различных диапазонов радиоволн: методы формирования и преобразования сигналов; основы оптимальной фильтрации; помехоустойчивость; многоканальный прием; принципы построения передающей и приемной аппаратуры; структурные схемы радиоприемников; специализированные радиоприемники: особенности телевизионных радиосистем.	80
ОПД.Ф.06	Метрология и электрорадиоизмерения физические поля - носители информации, основные информативные параметры полей, принципы наблюдения, регистрации и анализа структуры физических полей объектов; место процессов измерения в исследовательской и производственной деятельности, методы измерения электрических величин, оптические измерения, акустические измерения, электрические методы измерения неэлектрических величин, аналого-цифровые и цифро-аналоговые преобразования, методы и средства измерения сигналов в процессах формирования, обработки и передачи информации, основы метрологии, теория погрешностей измерений.	120

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.07	<p>Структура и основы деятельности предприятий различных форм собственности: структура и назначение государственных предприятий, правовые основы их деятельности; структура, назначение и правовые основы деятельности коллективных и частных предприятий; организационно-правовые формы предприятий; профиль предприятий; особенности организационной структуры и содержание деятельности предприятий различного профиля; структуры и основы деятельности общественных объединений.</p>	80
ОПД.Ф.08	<p>Документоведение понятие документа; функции и признаки документа; конфиденциальность документов; способы и средства документирования; классификация носителей документной информации; составление и оформление деловых (управленческих), технических, технологических и научно-технических документов; классификация документов и систем документации; проектирование типового состава документов предприятий различных форм собственности и профиля.</p>	100
ОПД.Ф.09	<p>Теория информационной безопасности и методология защиты информации сущность и понятие информационной безопасности, характеристика ее составляющих; значение информационной безопасности для субъектов информационных отношений; место информационной безопасности в системе национальной безопасности; современная концепция информационной безопасности; понятие и сущность защиты информации, ее место в системе информационной безопасности; цели и концептуальные основы защиты информации; критерии, условия и принципы отнесения информации к защищаемой; носители защищаемой информации; классификация конфиденциальной информации по видам тайны и степеням конфиденциальности; понятие и структура угроз защищаемой информации; источники,</p>	140

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.09	виды и методы дестабилизирующего воздействия на защищаемую информацию; причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию; виды уязвимости информации и формы ее проявления; каналы и методы несанкционированного доступа к конфиденциальной информации; направления, виды и особенности деятельности спецслужб по несанкционированному доступу к конфиденциальной информации; методологические подходы к защите информации и принципы ее организации; объекты защиты; виды защиты; классификация методов и средств защиты информации; кадровое и ресурсное обеспечение защиты информации; системы защиты информации.	
ОПД.Ф.10	Правовое обеспечение информационной безопасности назначение и структура правового обеспечения защиты информации; методы правовой защиты информации; правовые основы защиты государственной, коммерческой, служебной, профессиональной и личной тайны, персональных данных; правовая основа допуска и доступа персонала к защищаемым сведениям; система правовой ответственности за утечку информации и утрату носителей информации; правовые основы деятельности подразделений защиты информации; роль права в регулировании комплекса отношений в сфере защиты информации; отрасли права, обеспечивающие законность в области защиты информации; основные законодательные акты, правовые нормы и положения; назначение и задачи подзаконных правовых актов, регулирующих процессы защиты информации в отраслях, на предприятиях различных форм собственности; закрепление права предприятия на защиту информации в нормативных документах; правовое регулирование взаимоотношений администрации и персонала в области защиты информации; виды и условия применения правовых норм	200

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.10	уголовной, гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и не выполнение правил ее защиты; правовые проблемы, связанные с защитой прав обладателей собственности на информацию и распоряжением информацией; понятие интеллектуальной собственности, ее виды и основные объекты образования; интеллектуальный продукт как объект интеллектуальной собственности и предмет защиты; содержание гражданско-правовых норм в области защиты интеллектуальной собственности; авторское право; патентное право; товарный знак; договорное право, авторские и лицензионные договоры.	
ОПД.Ф.11	<p style="text-align: center;">Организационное обеспечение информационной безопасности</p> <p>принципы, силы, средства и условия организационной защиты информации; порядок засекречивания и рассекречивания сведений документов и продукции; допуск и доступ к конфиденциальной информации и документам; организация внутриобъектового и пропускного режимов на предприятиях; организация подготовки и проведения совещаний и заседаний по конфиденциальному вопросам; организация охраны предприятий; защита информации при публикаторской и рекламной деятельности; организация аналитической работы по предупреждению утечки конфиденциальной информации; направления и методы работы с персоналом, обладающим конфиденциальной информацией.</p>	120
ОПД.Ф.12	<p style="text-align: center;">Защита и обработка конфиденциальных документов</p> <p>структура защищенного документооборота, документпотоки, состав технологических этапов и операций; подготовка и издание конфиденциальных документов; учет конфиденциальных документов; порядок рассмотрения и исполнения документов; копирование и размножение</p>	120

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.12	<p>документов; контроль исполнения документов; составление и оформление номенклатуры дел; формирование и хранение дел, содержащих конфиденциальные документы; уничтожение конфиденциальных документов; проверка наличия конфиденциальных документов; порядок комплектования ведомственного архива и классификация хранилищ документов; учет конфиденциальных деловых (управленческих), технических, технологических и научно-технических документов в архиве; обеспечение сохранности конфиденциальных документов; научно-справочный аппарат к архивам конфиденциальных документов; порядок использования конфиденциальных архивных документов; оборудование архивохранилищ; организационные и методические проблемы автоматизации делопроизводственных операции по документам; машиноориентация содержания и форм конфиденциальных документов; принципы включения различных типов автоматизированных систем в традиционный документооборот; безбумажный документооборот; локальная и комплексная автоматизация процессов обработки документов в документационной службе; домашинная и постремашинная технология выполнения операций по блокам: блоку подготовки и издания документов, справочно-информационному блоку, блоку оперативного хранения и использования документов; состав конфиденциальных документов вычислительного центра, их обработка и хранение.</p>	
ОПД.Ф.13	<p>Инженерно-техническая защита информации виды информации, защищаемой техническими средствами; демаскирующие признаки объектов защиты; источники и носители информации, защищаемой техническими средствами; принципы записи и съема информации с носителей; виды угроз безопасности информации, защищаемой техническими средствами; принципы добывания и обработки информации техническими средствами; классификация и структура технических</p>	150

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.13	каналов утечки информации; основные способы и принципы работы средств наблюдения объектов, подслушивания и перехвата сигналов; системный подход к инженерно-технической защите информации; основные этапы проектирования системы защиты информации техническими средствами; принципы моделирования объектов защиты и технических каналов утечки информации; способы оценки угроз безопасности информации и расходов на техническую защиту; способы и принципы работы средств защиты информации от наблюдения, подслушивания и перехвата; организационные и технические меры инженерно-технической защиты информации в государственных и коммерческих структурах; контроль эффективности защиты информации.	
ОПД.Ф.14	<p>Технические средства защиты информации</p> <p>технические средства добывания информации; назначение и функции видов разведки; принципы оптической разведки, основные показатели технических средств визуальной, фотографической, телевизионной, инфракрасной и лазерной разведки и каналов информации; общая характеристика радиоэлектронной разведки, ее особенности, основные показатели технических средств радио, радиотехнической, радиолокационной и радиотепловой разведки и каналов утечки информации; технические средства акустической разведки, их функции; радиационная, химическая и магнитометрическая разведка; способы доступа к источникам конфиденциальной информации без нарушения государственной границы, без проникновения на объект защиты; комплексное использование технических средств разведки; способы и средства защиты конфиденциальной информации техническими средствами;</p> <p>защита объектов от наблюдения в оптическом диапазоне электромагнитных волн, от радиолокационного и радиотеплополокационного наблюдения; способы защиты линий связи учреждений</p>	200

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.14	и предприятий государственных и коммерческих структур от утечки конфиденциальной информации; способы устранения (снижения) утечки информации за счет паразитных электромагнитных излучений и наводок, активное радиоэлектронное противодействие средствам радио и радиотехнической разведки; способы и средства защиты акустической информации, меры по скрытию объектов от акустической, гидроакустической и сейсмической разведки; защита объектов от химической, радиационной и магнитометрической разведки; организация работ по инженерно-технической защите на предприятиях и в учреждениях государственных и коммерческих структур, основные руководящие документы по защите предприятий и учреждений от технической разведки, контроль эффективности мер по защите информации техническими средствами.	
ОПД.Ф.15	Технические средства охраны роль и место технических средств в организации режима охраны, современная концепция защиты объектов; основные составляющие систем ТСО: датчики, приборы визуального наблюдения, системы сбора и обработки информации, средства связи, питания и тревожно-вызывной сигнализации; практическая реализация систем ТСО: охрана режимных помещений, проект охраны объектов.	100
ОПД.Ф.16	Математические основы криптологии алгебраические методы в криптологии: алгебраические модели систем шифрования: полиномиальные функции; псевдослучайные последовательности, линейные рекуррентные последовательности над полем и кольцом, смешанный конгруэнтный метод и его обобщения; функции усложнения и равновероятные функции.	100
ОПД.Ф.17	Криптографические методы и средства обеспечения информационной безопасности Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования	120

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.17	<p>ния и колонной замены, современные системы шифрования (симметричные и асимметричные); основные принципы построения криптоалгоритмов (выбор группы шифра, параметров псевдослучайной последовательности, параметров функции усложнения, секретных характеристик в системах с открытым ключом, односторонние функции и методы их построения); основные методы дешифрования; стандарты систем шифрования (DES, ГОСТ 28147-89); сложность криптографических алгоритмов (теорема Кука, NP-полнота); вероятностное шифрование; криптографические протоколы, протоколы с нулевым разглашением.</p>	
ОПД.Ф.18	<p>Программно-аппаратная защита информации предмет и задачи программно-аппаратной защиты информации; идентификация субъекта, понятие протокола идентификации, идентифицирующая информация; основные подходы к защите данных от НСД; шифрование, контроль доступа и разграничение доступа, иерархический доступ к файлу, защита сетевого файлового ресурса, фиксация доступа к файлам; доступ к данным со стороны процесса; способы фиксации факта доступа; надежность систем ограничения доступа; защита файлов от изменения; электронная цифровая подпись (ЭЦП); программно-аппаратные средства шифрования; построение аппаратных компонент криптозащиты данных; защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа, необходимые и достаточные функции аппаратного средства криптозащиты; методы и средства ограничения доступа к компонентам ЭВМ; защита программ от несанкционированного копирования; пароли и ключи, организация хранения ключей; защита программ от излучения; защита от отладки, защита от дизассемблирования, защита от трасировки по прерываниям; защита от разрушающих программных воздействий (РПВ); компьютерные вирусы как особый класс РПВ;</p>	120

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.18	необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды.	
ОПД.Ф.19	<p>Защита информационных процессов в компьютерных системах</p> <p>основные угрозы информации в компьютерных системах; параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера; специфика возникновения угроз в открытых сетях; особенности защиты информации на узлах компьютерной сети; системные вопросы защиты программ и данных; основные категории требований к программной и программно-аппаратной реализации средств защиты информации; требования к защите автоматизированных систем от НСД.</p>	120
ОПД.Ф.20	<p>Комплексные системы защиты информации на предприятии</p> <p>сущность и задачи комплексной системы защиты информации (КСЗИ); принципы организации и этапы разработки КСЗИ; факторы, влияющие на организацию КСЗИ; определение и нормативное закрепление состава защищаемой информации; определение объектов защиты; анализ и оценка угроз безопасности информации: выявление и оценка источников, способов и результатов destabilizирующего воздействия на информацию; определение потенциальных каналов и методов несанкционированного доступа к информации; определение возможностей несанкционированного доступа к защищаемой информации; определение компонентов КСЗИ; определение условий функционирования КСЗИ; разработка модели КСЗИ; технологическое и организационное построение КСЗИ; кадровое обеспечение функционирования КСЗИ; материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ; назначение, структура и содержание управления КСЗИ; принципы и методы</p>	120

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ОПД.Ф.20	планирования функционирования КСЗИ; сущность и содержание контроля функционирования КСЗИ; управление КСЗИ в условиях чрезвычайных ситуаций; состав методов и моделей оценки эффективности КСЗИ	
ОПД.Ф.21	Экономика защиты информации экономические проблемы информационных ресурсов; экономическая безопасность; информация как важнейший ресурс экономики; информация как товар, цена информации; основные подходы к определению затрат на защиту информации; система ресурсообеспечения защиты информации и эффективность ее использования; управление ресурсами в процессе защиты информации; виды ущерба, наносимые информации; степень наносимого ущерба информации; методы и способы страхования информации; формирование бюджета службы защиты информации; оценка эффективности защиты и страхования информации.	120
ОПД.Ф.22	Безопасность жизнедеятельности безопасность труда как составная часть антропогенной экологии; человек - основной объект в системе обеспечения безопасности жизнедеятельности; среда обитания человека; опасные, вредные и поражающие факторы, их классификация и характеристика; принципы классификации и возникновения чрезвычайных ситуаций; организация и проведение защитных мер при чрезвычайных ситуациях; методы и средства обеспечения безопасности жизнедеятельности в чрезвычайных ситуациях; основы обеспечения безопасности технологических процессов; правовые и социально-экономические основы обеспечения безопасности жизнедеятельности в чрезвычайных ситуациях; основы управления обеспечением безопасности жизнедеятельности.	90
ОПД.Р.00	Национально-региональный (вузовский) компонент	200
ОПД.В.00	Дисциплины и курсы по выбору студента, устанавливаемые вузом	200

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ДС	Дисциплины специализации	870
ДС.01	<p>Вычислительные сети</p> <p>задачи и проблемы распределенной обработки данных; классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей; основы организации и функционирования сетей; сетевые операционные системы; основные сетевые стандарты; средства взаимодействия процессов в сетях; распределенная обработка информации в системах клиент-сервер; одноранговые сети; средства идентификации и аутентификации; средства повышения надежности функционирования сетей; интеграция локальных сетей в региональные и глобальные сети; неоднородные вычислительные сети; сетевые средства UNIX: основные протоколы, службы, функционирование, сопровождение и разработка приложений, особенности реализации на различных платформах; сетевая операционная система Novell NetWare: основные протоколы, службы, функционирование, генерация, сопровождение и разработка приложений; сетевая операционная система Windows NT: основные протоколы, службы, функционирование, генерация, сопровождение и разработка приложений; глобальные сети: Internet, основные службы и предоставляемые услуги, стандарты, перспективы развития.</p>	130
ДС.02	<p>Системы и сети связи</p> <p>классификация систем связи; кодирование информации в системах связи; помехоустойчивое кодирование; схемная реализация; алгоритмы декодирования; методы модуляции в системах связи; основные типы модемов; уплотнение информации в системах связи; цифровая обработка аналоговых сигналов; дискретные вокодеры; особенности цифровых систем многоканальных передач сообщений; способы объединения цифровых потоков; особенности передачи дискретных</p>	160

Приложение

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ДС.02	сообщений по цифровым каналам; системы телефонной связи; цифровая телефония; системы телеграфной связи; коротковолновые и ультракоротковолновые системы связи; радиорелейные системы связи; телевизионные системы; спутниковые системы связи; волоконно-оптические системы связи; современные виды информационного обслуживания; факсимильная передача информации; электронная почта; телеконференция; видеотекс; телетекс; сети связи; структура сетей связи; методы коммутации информации; особенности сетей с коммутацией каналов, сообщений и пакетов; эталонная модель взаимодействия открытых систем; общие сведения о протоколах эталонной семиуровневой модели; глобальные и локальные сети; особенности современных сетевых архитектур; архитектурные особенности современных локальных сетей; протоколы физического и канального уровней; технические характеристики и принципы функционирования современных модемов; маршрутизация и управление потоками в сетях связи; сети интегрального обслуживания.	
ДС.03	Организация и управление службой защиты информации на предприятии место и роль службы защиты информации в системе защиты информации; задачи и функции службы; структура и штаты службы; организационные основы и принципы деятельности службы; подбор, расстановка и обучение сотрудников службы; организация труда сотрудников службы; принципы, методы и технология управления службой.	180
ФТД	Факультативы	450
ФТД.01	Военная подготовка	450

Всего часов теоретического обучения - **8260.**

Практики - не менее 12 недель.

Приложение

5. СРОКИ ОСВОЕНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 075400 - КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

5.1. Срок освоения основной образовательной программы подготовки специалиста по защите информации при очной форме обучения составляет 256 недель, в том числе:

- теоретическое обучение, включая научно-исследовательскую работу студентов, практикумы, в том числе лабораторные, а также экзаменационные сессии - 190 недель;
- практики - не менее 12 недель;
- итоговая государственная аттестация, включая подготовку и защиту выпускной квалификационной работы - не менее 14 недель;
- каникулы (включая 8 недель последипломного отпуска) - не менее 40 недель.

5.2. Для лиц, имеющих среднее (полное) общее образование сроки освоения основной образовательной программы подготовки специалиста по защите информации по очно-заочной (вечерней) и заочной формам обучения, а также в случае сочетания различных форм обучения увеличиваются вузом до 1 года относительно нормативного срока, установленного п. 1.2 настоящего государственного образовательного стандарта.

5.3. Максимальный объем учебной нагрузки студента устанавливается 54 часа в неделю, включая все виды его аудиторной и внеаудиторной (самостоятельной) учебной работы.

5.4. Объем аудиторных занятий студента при очной форме обучения не должен превышать в среднем за период теоретического обучения 27 часов в неделю. При этом в указанный объем не входят обязательные практические занятия по физической культуре и занятия по факультативным дисциплинам.

5.5. При очно-заочной (вечерней) форме обучения объем аудиторных занятий должен быть не менее 10 часов в неделю.

5.6. При заочной форме обучения студенту должна быть обеспечена возможность занятий с преподавателем в объеме не менее 160 часов в год.

5.7. Общий объем каникулярного времени в учебном году должен составлять 7-10 недель, в том числе не менее 2-х недель в зимний период.

6. ТРЕБОВАНИЯ К РАЗРАБОТКЕ И УСЛОВИЯМ РЕАЛИЗАЦИИ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 075400 - КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

6.1 Требования к разработке основной образовательной программы подготовки специалиста по защите информации.

6.1.1. Высшее учебное заведение самостоятельно разрабатывает и утверждает основную образовательную программу вуза для подготовки специалиста по защите информации на основе настоящего государственного образовательного стандарта.

Дисциплины по выбору студента являются обязательными, а факультативные дисциплины, предусматриваемые учебным планом высшего учебного заведения, не являются обязательными для изучения студентом.

Курсовые работы (проекты) рассматриваются как вид учебной работы по дисциплине и выполняются в пределах часов, отводимых на ее изучение.

По всем дисциплинам и практикам, включенным в учебный план высшего учебного заведения, должна выставляться итоговая оценка (отлично, хорошо, удовлетворительно, неудовлетворительно или зачленено).

Специализации являются частями специальности, в рамках которой они создаются, и предполагают получение более углубленных профессиональных знаний, умений и навыков в различных областях деятельности по профилю данной специальности.

6.1.2. При реализации основной образовательной программы высшее учебное заведение имеет право:

- изменять объем часов, отводимых на освоение учебного материала для циклов дисциплин, в пределах 10%;
- формировать цикл гуманитарных и социально-экономических дисциплин, который должен включать из одиннадцати базовых дисциплин, приведенных в настоящем государственном образовательном стандарте, в качестве обязательных следующие 4 дисциплины: «Иностранный язык» (в объеме не менее 340 часов), «Физическая культура» (в объеме не менее 408 часов), «Отечественная история», «Философия». Остальные базовые дисциплины могут реализовываться по усмотрению вуза. При этом возможно их объединение в междисциплинарные курсы при сохранении обязательного минимума содержания. Если дисциплины являются частью общепрофессиональной или специальной подготовки (для гумани-

тарных и социально-экономических направлений подготовки и специальностей), выделенные на их изучение часы могут перераспределяться в рамках цикла ГСЭ;

- предусматривать занятия по дисциплине «Физическая культура» при очно-заочной (вечерней), заочной формах обучения и экстернате с учетом пожелания студентов;
- осуществлять преподавание гуманитарных и социально-экономических дисциплин в форме авторских лекционных курсов и разнообразных видов коллективных и индивидуальных практических занятий, заданий и семинаров по программам, разработанным в самом вузе и учитывающим региональную, национально-этническую, профессиональную специфику, а также научно-исследовательские предпочтения преподавателей, обеспечивающих квалифицированное освещение тематики дисциплин цикла;
- устанавливать необходимую глубину преподавания отдельных разделов дисциплин, входящих в циклы гуманитарных и социально-экономических, математических и естественнонаучных дисциплин, в соответствии с профилем цикла дисциплин специализации;
- устанавливать наименования специализаций по специальностям высшего профессионального образования, наименования дисциплин специализаций, их объем и содержание, сверх установленного настоящим государственным образовательным стандартом, а также форму контроля за их освоением студентами;
- реализовывать основную образовательную программу подготовки специалиста по защите информации в сокращенные сроки для студентов высшего учебного заведения, имеющих среднее профессиональное образование соответствующего профиля или высшее профессиональное образование. Сокращение сроков проводится на основе имеющихся знаний, умений и навыков студентов, полученных на предыдущих этапах профессионального образования. При этом продолжительность обучения должна составлять не менее 3-х лет. Обучение в сокращенные сроки допускается также для лиц, уровень образования или способности которых являются для этого достаточным основанием.

6.2. Требования к кадровому обеспечению учебного процесса. Реализация основной образовательной программы подготовки дипломированного специалиста должна обеспечиваться педагогическими кадрами, имеющими, как правило, базовое образование, соответствующее профилю преподаваемых дисциплин, и систематически занимающимися научной и/или научно-методической деятельностью. Преподаватели специальных дисциплин, как правило,

Приложение

должны иметь ученую степень и/или опыт деятельности в соответствующей профессиональной сфере. Желательно, чтобы доля преподавателей, имеющих ученую степень и звание, составляла не менее 50% от общего числа преподавателей.

6.3. Требования к учебно-методическому обеспечению учебного процесса. Реализация основной образовательной программы подготовки дипломированного специалиста должна обеспечиваться доступом каждого студента к библиотечным фондам и базам данных, по содержанию соответствующим полному перечню дисциплин основной образовательной программы, наличием методических пособий и рекомендаций по всем дисциплинам и по всем видам занятий - практикумам, курсовому и дипломному проектированию, практикам, а также наглядными пособиями, мультимедийными и аудио-видеоматериалами.

Лабораторными практикумами должны быть обеспечены следующие дисциплины: математика, дополнительные главы математики, математические основы защиты информации, физика, физические основы защиты информации, информатика, аппаратные средства вычислительной техники, методы программирования и прикладные алгоритмы, вычислительные сети, электротехника и электроника, системы и сети связи, метрология и электрорадиомерения, защита и обработка конфиденциальных документов, инженерно-техническая защита информации, технические средства защиты информации, технические средства охраны, криптографические методы и средства обеспечения информационной безопасности, программно-аппаратная защита информации, защита информационных процессов в компьютерных системах, комплексные системы обеспечения информационной безопасности, а также дисциплины специализации. Лабораторная база высшего учебного заведения должна быть оснащена современными стендами и оборудованием.

Практические и семинарские занятия должны быть предусмотрены по дисциплинам в соответствии с примерным учебным планом по специальности 075400 - Комплексная защита объектов информатизации.

Компьютерные классы должны быть оснащены современной вычислительной техникой.

Библиотечный фонд вуза должен быть укомплектован учебниками, учебными пособиями, монографиями, учебно-методической документацией, руководствами к лабораторным работам и соответствующими задачниками, включая литературу для выполнения

Приложение

курсовых, дипломных и научно-исследовательских работ. В библиотечном фонде должны быть «свежие» научно-технические и реферативные журналы по направлению «Информационная безопасность». Перечень рекомендуемой литературы и рекомендуемых к подписке периодических изданий формирует УМС УМО и ежегодно доводит до сведения вузов, имеющих лицензию на специальность 075400 - Комплексная защита объектов информатизации.

6.4. Требования к материально-техническому обеспечению учебного процесса. Высшее учебное заведение, реализующее основную образовательную программу подготовки дипломированного специалиста, должно располагать материально-технической базой, соответствующей действующим санитарно-техническим нормам и обеспечивающей проведение всех видов лабораторной, практической, дисциплинарной и междисциплинарной подготовки, предусмотренных примерным учебным планом, и научно-исследовательской работой студентов.

6.5. Требования к организации практик. Практика студента является средством связи теоретического обучения с практической деятельностью, обеспечивающим прикладную направленность и специализацию обучения.

7. ТРЕБОВАНИЯ К УРОВНЮ ПОДГОТОВКИ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 075400 - КОМПЛЕКСНАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

7.1. Требования к профессиональной подготовленности специалиста.

Выпускник должен уметь решать задачи, соответствующие его квалификации, указанные в п. 1.3 настоящего государственного образовательного стандарта.

Специалист по защите информации должен

знать и уметь использовать:

- основные понятия и методы математического анализа, геометрии, алгебры, теории функций комплексного переменного, теории вероятностей и математической статистики;
- основные понятия, законы и модели механики, электричества и магнетизма, колебаний и волн, квантовой физики, статистической физики и термодинамики, методы теоретического и экспериментального исследования в физике;
- основные положения теории информации, принципы построения систем обработки и передачи информации, основы семантиче-

Приложение

ского подхода к анализу информационных процессов;

- современные аппаратные и программные средства вычислительной техники;
- принципы организации информационных систем в соответствии с требованиями информационной защищенности, в том числе в соответствии с требованиями по защите государственной тайны;
- конструкцию и основные характеристики технических устройств хранения, обработки и передачи информации, потенциальные каналы утечки информации, характерные для этих устройств, способы их выявления и методы оценки опасности, основную номенклатуру и характеристики аппаратуры, используемой для перехвата и анализа сигналов в технических каналах утечки информации, методы и средства инженерно-технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;
- принципы построения современных криптографических систем, стандарты в области криптографической защиты информации;
- основные правовые положения в области информационной безопасности и защиты информации.

владеТЬ:

- методами организации и управления деятельностью служб защиты информации на предприятиях;
- технологией проектирования, построения и эксплуатации комплексных систем защиты информации;
- методами научного исследования уязвимости и защищенности информационных процессов;
- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Дополнительные требования к специальной подготовке специалиста по защите информации определяются высшим учебным заведением с учетом специализации.

7.2. Требования к итоговой государственной аттестации специалиста.

7.2.1. Итоговая государственная аттестация специалиста по защите информации включает квалификационную работу (дипломная работа или дипломный проект) и государственный экзамен по специальности, позволяющий выявить теоретическую готовность выпускника к решению профессиональных задач.

Приложение

Выпускная квалификационная работа специалиста по защите информации (дипломная работа или дипломный проект) имеет целью систематизировать и углубить знания, совершенствовать навыки и умения выпускника в решении сложных комплексных научно-технических задач с элементами научного исследования, а также проявить степень профессиональной подготовленности выпускника, ее соответствие данному образовательному стандарту. Дипломная работа представляет собой теоретическое или экспериментальное исследование одной из актуальных проблем по специальности (специализации). Результаты работы оформляются в виде текста с приложением графиков, таблиц, чертежей, карт, схем. Дипломный проект представляет собой решение конкретной практической задачи, имеющей прикладной характер, или инженерной проблемы с проведением проекто-конструкторских расчетов и разработок, теоретических и экспериментальных исследований. Он оформляется в виде чертежей, расчетно-графических и иных материалов, моделей и пояснительной записи к ним.

7.2.3. Государственный экзамен по специальности имеет целью определение степени соответствия уровня подготовленности выпускников требованиям данного образовательного стандарта. При этом проверяются как теоретические знания, так и практические навыки выпускника в соответствии со специальностью (Комплексная защита объектов информатизации), квалификацией (специалист по защите информации) и специализацией полученного образования.

СПИСОК ЛИТЕРАТУРЫ

1. Герасименко В.А., Малюк А.А., Горбатов В.С., Кондратьева Т.А., Петров В.А., Погожин Н.С., Толстой А.И. Проблемные вопросы информационной безопасности // Безопасность информационных технологий. - 1996. - № 1.
2. Беляев Е.А. Становление и развитие государственной системы защиты информации. // Безопасность информационных технологий. - 1995. - № 3.
3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. -М.: Энергоатомиздат, кн. 1 и 2, 1994.
4. Малюк А.А. Современные проблемы защиты информации и пути их решения // Безопасность информационных технологий. -1999. - №3.
5. Герасименко В.А. Основы информационной грамоты. -М.: Энергоатомиздат, 1996.
6. Герасименко В.А., Малюк А.А. Сущность и пути перевода процессов защиты информации на интенсивные способы// Безопасность информационных технологий. - 1998. - №4.
7. Хоффман Л.Дж. Современные методы защиты информации. Пер. с англ. -М.: Советское радио, 1980.
8. Уолкер Б.Дж., Блейк Д.Ф. Безопасность ЭВМ и организация их защиты. Пер. с англ. - М.: Связь, 1980.
9. Сяо Д., Кэрр Д., Мэдник С. Защита ЭВМ. Пер. с англ. -М.: Мир, 1982.
10. Шураков В.В. Обеспечение сохранности информации в автоматизированных системах обработки данных. -М.: Финансы и статистика, 1985.
11. Мамиконов А.Г., Кульба В.В., Шелков А.Б. Достоверность, защита и резервирование информации в АСУ. -М.: Энергоатомиздат, 1986.
12. Растворгувев С.П., Дмитриевский Н.Н. Искусство защиты и «раздевания» программ. -М.: Совмаркет, 1991.
13. Спесивцев А.В., Ветер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. -М.: Радио и связь, ВЕСТА, 1992.
14. Растворгувев С.П. Программные методы защиты информации в компьютерах и сетях. -М.: Яхтсмен, 1993.
15. Гайкович В.Ю., Першин А.В. Безопасность электронных банковских систем. -М.: Единая Европа, 1994.
16. Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации. -М.: Яхтсмен, 1996.
17. Зегжда П.Д. Способы защиты информации. -М.: Яхтсмен, 1996.
18. Алексеенко В.Н. Современная концепция комплексной защиты. Технические средства защиты. - М.: МИФИ, 1994.

Список литературы

19. **Расторгуев С.П.** Вирусы: биологические, социальные, психические, компьютерные. - М.: Яхтмен, 1996.
20. **Проблемы** безопасности программного обеспечения / Под ред. П.Д.Зегжды, Санкт-Петербургский гос. тех. университет, 1995.
21. **Петров В.А., Пискарев А.С., Шеин А.В.** Защита информации от несанкционированного доступа в автоматизированных системах. - М.: МИФИ, 1995.
22. **Левкин В.В., Шеин А.В.** Система защиты информации от несанкционированного доступа «Снег». - М.: МИФИ, 1996.
23. **Варфоломеев А.А., Пеленицын М.Б.** Методы криптографии и их применение в банковских технологиях. - М.: МИФИ, 1995.
24. **Безруков Н.Н.** Компьютерная вирусология. Справочное руководство. - Киев: Укр. сов. энциклопедия, 1991.
25. **Дмитриевский Н.Н.** Компьютерные вирусы и борьба с ними. - М.: МИФИ, 1995.
26. **Тихонов А.Н.** О состоянии работ по совершенствованию подготовки кадров по проблеме информационной безопасности // Безопасность информационных технологий. - 1995. - №4.
27. **Дружинин Г.В.** Надежность автоматизированных систем. - М.: Энергия, 1997.
28. **Самойленко С.И., Давыдов Д.А., Золотарев В.В., Третьякова В.Н.** Вычислительные сети (адаптивность, помехоустойчивость, надежность). - М.: Наука, 1981.
29. **Пивоваров А.Н.** Методы обеспечения достоверности информации в АСУ. М.: Радио и связь, 1982.
30. **Герасименко В.А.** Основы управления качеством информации. - М.: Московский историко-архивный институт, 1989, деп. в ВИНИТИ 26.06.89, №5392 В89.
31. **Герасименко В.А., Малюк А.А.** Основы защиты информации. - М.: МИФИ, 1997.
32. **Малюк А.А.** Проблемы кадрового обеспечения информационной безопасности // Безопасность информационных технологий. -1998 -№2.
33. **Шершнев Л.И.** Информационная безопасность в общей совокупности проблем безопасности России // Безопасность информационных технологий, 1996, №4.
- 34 **Проблемы** создания и организации работы центров защиты информации /под ред. А.А.Малюка // Безопасность информационных технологий.-1997.-№4.
35. **Малюк А.А.** Теоретические основы формирования прогнозной оценки уровня безопасности информации в системах обработки данных // Книжная серия журнала «Безопасность информационных технологий». - М.:МИФИ, 1998.
36. **Перфильева И.Г.** Приложения теории нечетких множеств // Итоги науки и техники, т. 29. - М.: ВИНИТИ, 1990.

Список литературы

37. **Нечеткие множества и теория возможностей.** / Под ред. Р.Р. Ячера. Пер. с англ. - М.: Радио и связь, 1986.
38. **Поспелов Д.А.** Большие системы (ситуационное управление). - М.: Знание, 1971.
39. **Букатова И.Л.** Эволюционное моделирование и его приложение. - М.: Наука, 1979.
40. **Громов Г.Р.** Национальные информационные ресурсы: проблемы промышленной эксплуатации. - М.: Наука, 1985.
41. **Вильсон А.** Энтропийные методы моделирования сложных систем / Пер. с англ. - М.: Наука, 1978.
42. **Михайлов С.Ф., Петров В.А., Тимофеев Ю.А.** Информационная безопасность. Защита информации в автоматизированных системах. Основные концепции: Учебное пособие. - М.: МИФИ, 1995.
43. **Гостехкомиссия России.** Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. - М.: Военное издательство, 1992.
44. **Гайкович В.Ю., Ершов Д.В.** Основы безопасности информационных технологий: Учебное пособие. - М.: МИФИ, 1995.
45. **Скородумов Б.И.** Информационная безопасность. Обеспечение безопасности информации электронных банков: Учебное пособие. - М.: МИФИ, 1995.
46. **Зельнер А.** Байесовские методы в эконометрии. - М.: Статистика, 1980.
47. **Гришин Ю.П., Казаринов Ю.М.** Динамические системы, устойчивые к отказам. - М.: Радио и связь, 1985.
48. **Глушков В.М., Иванов В.В.** Моделирование развивающихся систем. - М.: Наука, 1983.
49. **Кини Р.Л., Райфа Х.** Принятие решений при многих критериях: предпочтения и замещения. Пер. с англ. - М.: Радио и связь, 1981.
50. **Роль системы рискового бизнеса в ускорении НТП. Роль организационных нововведений в ускорении НТП промышленных фирм Запада.** - М.: ЦООНТИ «ЭКОС», 1987.
51. **Малюк А.А.** Научные основы интенсификации процессов защиты информации // Безопасность информационных технологий. - 1998. - №3.

ОГЛАВЛЕНИЕ

Предисловие.....	3
Введение.....	5
Глава первая. Проблемы обеспечения информационной безопасности.....	12
1.1. Определение и место информационной безопасности в общей совокупности информационных проблем современного общества.....	12
1.2. Ретроспективный анализ развития подходов к защите информации.....	19
1.3. Современная постановка задачи защиты информации.....	30
1.4. Сущность, необходимость, пути и условия перехода к интенсивным способам защиты информации.....	37
Краткие выводы.....	43
Глава вторая. Основы теории защиты информации.....	45
2.1. Особенности и состав научно-методологического базиса решения задач защиты информации.....	45
2.2. Общеметодологические принципы формирования теории защиты информации.....	47
2.3. Методологический базис теории защиты информации.....	52
2.4. Принципы автоформализации профессиональных знаний эксперта-аналитика.....	62
2.5. Моделирование процессов защиты информации.....	68
2.6. Основное содержание теории защиты информации.....	79
Краткие выводы.....	90
Глава третья. Угрозы и оценка уязвимости информации.....	93
3.1. Понятие угрозы безопасности информации.	
Ретроспективный анализ подходов к формированию множества угроз.....	93
3.2. Системная классификация угроз безопасности информации ...	97
3.3. Методы оценки уязвимости информации.....	100
3.4. Методы оценки достоверности информационной базы моделей прогнозирования значений показателей уязвимости информации.....	105
3.5. Модели оценки ущерба от реализации угроз безопасности информации.....	120
Краткие выводы.....	126
Глава четвертая. Требования к защите информации.....	128
4.1. Постановка задачи и анализ существующих методик определения требований к защите информации.....	128
4.2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты.....	131
4.3. Определение весов вариантов потенциально возможных условий защиты информации.....	152
4.4. Методы деления поля значений факторов на типовые классы.....	153

Краткие выводы.....	165
Глава пятая. Системы защиты информации.....	168
5.1. Определение, типизация и стандартизация систем защиты информации.....	168
5.2. Система защиты информации как многокритериальный развивающийся объект.....	175
5.3. Проектирование систем защиты информации.....	180
5.4. Управление процессами функционирования систем защиты.....	186
Краткие выводы.....	202
Глава шестая. Развитие теории и практики защиты информации.....	205
6.1. Основные выводы из истории развития теории и практики защиты информации.....	205
6.2. Перспективы развития теории и практики защиты информации.....	207
6.3. Проблемы создания и организации работы центров защиты информации.....	214
6.4. Подготовка кадров в области обеспечения информационной безопасности.....	226
Краткие выводы.....	228
Заключение.....	231
Приложение. Государственный образовательный стандарт высшего профессионального образования.....	233
Список литературы.....	276

А. А. Малюк

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: КОНЦЕПТУАЛЬНЫЕ И МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Изложены основы теории защиты информации, объединяющие широкий спектр проблем, связанных с обеспечением информационной безопасности в процессе генерирования, обработки, хранения и передачи информации в автоматизированных системах и на объектах информатизации. Анализируются различные подходы к моделированию систем и процессов защиты информации в условиях неполноты и недостоверности исходных данных. Особое внимание уделяется эвристической составляющей процесса поиска наиболее рациональных решений в различных ситуациях защиты информации.

Для студентов обучающихся по специальности «Комплексная защита объектов информатизации». Может использоваться при обучении по специальностям группы «Информационная безопасность». Будет полезна разработчикам и пользователям комплексных систем обеспечения информационной безопасности.

**Книги издательства «Горячая линия – Телеком»
можно заказать через почтовое агентство DESSY: 107113, г.Москва, а/я 10,
а также интернет-магазины: www.dessy.ru www.top-kniga.ru**

Сайт издательства:

www.techbook.ru

