ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ: КОНЦЕПТУАЛЬНО-МАТЕМАТИЧЕСКИЕ АСПЕКТЫ

Гончаров В.В.[1], Мишенина О.В.[2]

Ключевые слова: *комплексная защита информации, защищенность информации, качество информации, информационная безопасность, автоматизированная система, уязвимость и угрозы безопасности, системная классификация угроз, оценка угроз, информационный риск.*

Аннотация

Цель работы: совершенствование информационно-математического обеспечения комплексного подхода к решению задач защиты информации на основе диалектического единства взаимосогласованных процессов информатизации общества.

Методы: системный анализ и математическое моделирование, позволяющее обеспечить сведение многокритериальной задачи оптимизации к однокритериальной с последующим формированием итерационной процедуры.

Результаты: проведен системно-исторический анализ методов, средств и мероприятий обеспечения защищенности информации с учетом роста ее уязвимости в условиях развития современных информационных технологий и появления новых угроз; разработана математическая модель построения области допустимых решений задачи, границами которой служат аналитические выражения функций, полученные в результате интерполяции (аппроксимации) соответствующих исходных данных, при этом требования к значениям параметров, находящимся в области «насыщения», могут быть снижены с целью увеличения характеристик других; разработанная итерационная человеко-машинная процедура позволяет находить рациональный вариант решения задачи.

Полученные результаты являются основой для создания соответствующего эффективного информационно-математического обеспечения аппаратно-программного комплекса исследования информационной безопасности сложных динамических объектов.

DOI: 10.24682/1994-1404-2024-3-43-57

Введение

В настоящее время интенсивное развитие и использование современных информационных технологий привели к серьезным качественным изменениям в экономической, социально-политической и духовной сферах общественной жизни. Человечество фактически переживает этап формирования нового информационного общества. Феномен резко возрастающего влияния информационно-коммуникационных технологий на формирование общества XXI в. был отмечен в Окинавской хартии[3], принятой мировыми лидерами 22 июля 2000 г.

Вместе с тем, развитие информационного общества, помимо расширения созидательных возможностей, приводит к росту угроз национальной безопасности, связанных с нарушением установленных режимов использования информационных и ком-

[3] Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации : учебное пособие. СПб. : Питер, 2023. 384 с.

[1] ***Гончаров Владимир Васильевич,*** *доктор технических наук, профессор, заслуженный работник высшей школы Российской Федерации, заведующий кафедрой математики Военной академии имени Петра Великого, г. Москва, Российская Федерация.*

E-mail: v_v_goncharov@mail.ru

[2] ***Мишенина Ольга Викторовна,*** *кандидат педагогических наук, доцент, профессор кафедры математики Военной академии имени Петра Великого, г. Москва, Российская Федерация.*

E-mail: o.v.mishenina@gmail.com

муникационных систем, ущемлением конституционных прав граждан, распространением вредоносных программ, а также с использованием возможностей современных информационных технологий для осуществления враждебных, террористических и других преступных действий [14]. В связи с этим особую остроту сегодня приобретает проблема обеспечения информационной безопасности (*рис.* 1) и, прежде всего, надежной защиты информации (предупреждения ее искажения или уничтожения, несанкционированной модификации, злоумышленного получения и использования).

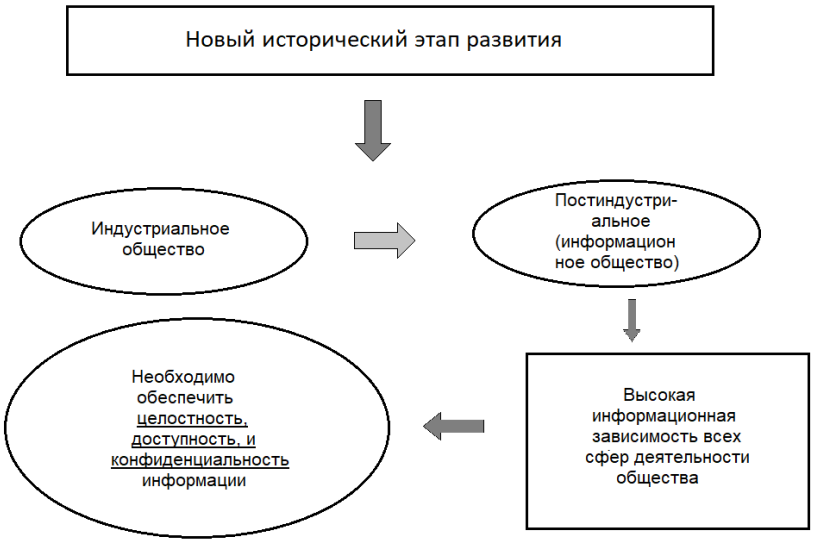

Рис. 1. Взаимосвязь информационного общества и информационной безопасности

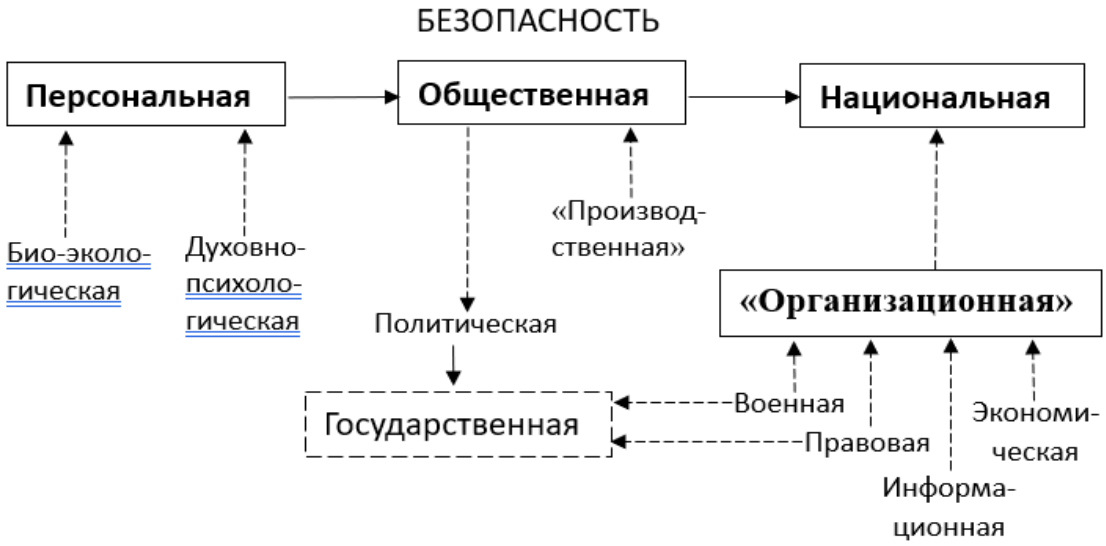

Рис. 2. Взаимосвязь видов национальной безопасности по сферам жизнедеятельности

Национальная безопасность государства, представляющая собой совокупность различных видов безопасности (экономической, военной, экологической и др.) существеннейшим образом будет зависеть от уровня *информационной безопасности* [8], поскольку все решения, принимаемые в этих областях, базируются на соответствующем информационном обеспечении, целостность, доступность и конфиденциальность которого должны быть надежным образом защищены[4] (*рис.* 2 [12]).

Проблема защиты информации, имеющая многовековую историю, приобрела самостоятельную актуальность только во второй половине XX в. Это связано

[4] Общая теория национальной безопасности : учебник / Под общ. ред. А.А. Прохожева. М. : РАГС, 2005. 344 с.

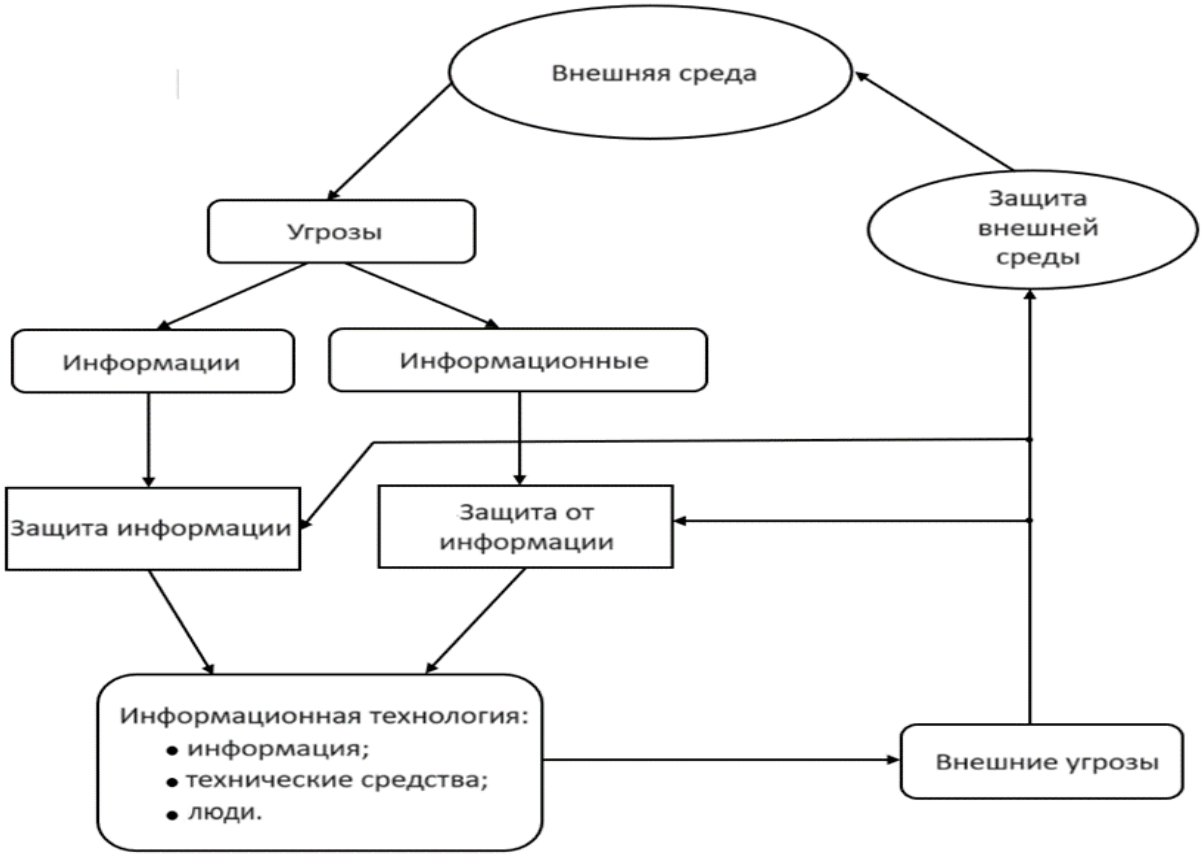

Рис. 3. Информационная безопасность как комплексная проблема

с бурным развитием средств вычислительной техники, применяющихся для обработки закрытой информации. Однако нередко проблему защиты связывают только с секретной информацией. Хотя, на сегодняшний день понятно, что это составляет лишь одну из частей гораздо более общей задачи обеспечения *целостности, доступности* и *конфиденциальности* [8] информации и защиты жизненно важных интересов личности, общества и государства в информационной сфере[5].

В настоящее время можно констатировать, что в процессе развития мировая «информационная» цивилизация пришла к формированию самостоятельного научно-технического направления «информационная безопасность», сфера деятельности и научного знания которого определяются терминологией и предметной областью [5].

Значение первой из них четко выражено формулой Декарта: «*Определяйте значения слов, и вы избавите мир от половины заблуждений*»[6]. Отсюда вытекает, что важнейшая проблема сегодняшнего дня — «совершенствование» глоссария в области информационной безопасности.

Для решения этой проблемы представим некоторый объект информатизации, в котором осуществляется генерация информации, ее хранение, обработка, передача и др. Очевидно, что информация, находящаяся в данном объекте, может подвергаться угрозам со стороны внешней среды. Однако данная информация, а также деятельность самого такого объекта могут создавать множество угроз для внешней среды[7].

В ряде работ как отечественных, так и зарубежных авторов даны определения защищенности и безопасности информации, информационной безопасности, защиты информации, защиты от информации. Однако данные определения не всегда учитывают сложной взаимосвязи всех охватываемых ими процессов, характер которой можно уяснить, рассмотрев, например, концептуальную структуру понятия «проблема информационной безопасности» (*рис*. 3). Из неё следует, что информационная безопасность — это состояние защищенности среды и информации от вредных информационных воздействий[8].

Именно такой трактовки этого понятия придерживается Доктрина информационной безопасности Россий-

[5] Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации : учебное пособие. М. : Инфра-М, 2001. 304 с.

[6] Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М. : ИЦ «Академия», 2009. 336 с.

[7] Малюк А.А., Горбатов В.С., Королев В.И., Фомичев В.М., Дураковский А.П., Кондратьева Т.А. Введение в информационную безопасность : учебное пособие. М. : Горячая линия-Телеком, 2022. 288 с.

[8] Шангин В.Ф. Защита информации в компьютерных системах и сетях. М. : ДМК Пресс, 2012. 592 с.

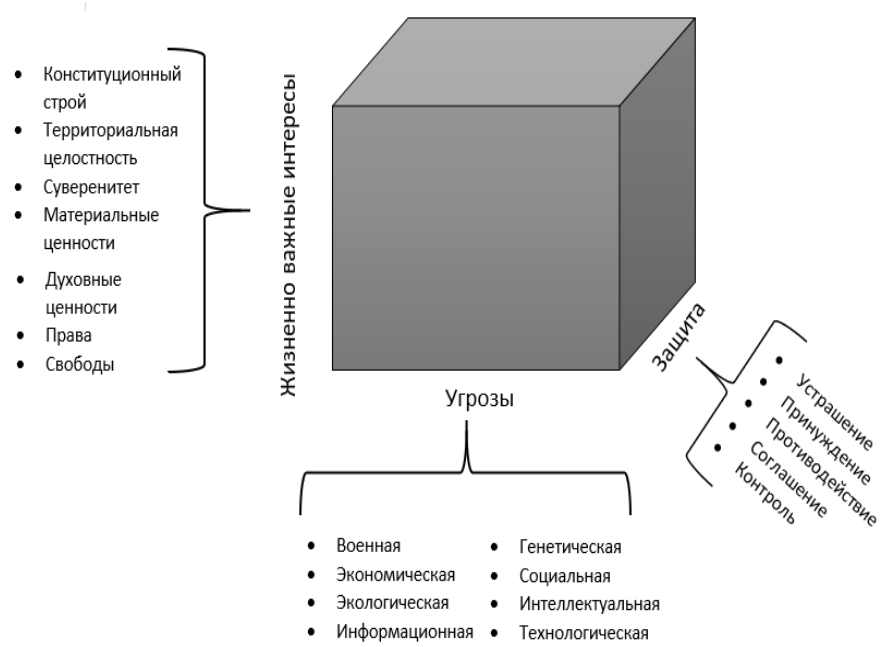

Рис. 4. Предметная область комплекса наук о безопасности

ской Федерации: «*Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства*».

Исходя из анализа множества нормативных документов[9], научных публикаций по вопросам обеспечения информационной безопасности, ряд определений были уточнены и существенно дополнены. Однако в последнее время определение, данное термину «информационная безопасность» в Доктрине информационной безопасности, подвергается критике, так как, по мнению ряда ученых и специалистов [8, 9], использование термина «состояние защищенности» не учитывает происходящих в последнее время изменений в подходах к созданию новых информационных технологий (например, технологии «облачных» вычислений). При этом безопасность рассматривается не как некоторая надстройка, а как изначальный базис технологии, т. е. непременное ее качество. Следовательно, представление безопасности как качества (свойства системы [9]) более объективно характеризует способность системы противостоять тем или иным угрозам как внешнего, так и внутреннего характера.

Что касается предметной области направления деятельности «Информационная безопасность», то основой здесь могут послужить исследования, проводившиеся Российской академией естественных наук (РАЕН) и посвященные определению предметной области комплекса наук о безопасности[10]. На *рис*. 4 в концентрированном виде показано представление предметной области «Безопасность», предложенное в трудах РАЕН.

Как видим, данная предметная область изображается в виде некоторого куба в трехмерном пространстве с координатами «Жизненно важные интересы», «Угрозы», препятствующие реализации данных интересов и основные методы «Защиты» от угроз. Кстати, данные исследования РАЕН, в значительной мере были стимулированы решениями Международного форума по проблемам безопасности, проводившегося в 1992 г. в Рио-де-Жанейро. В них констатировалось, что проблемы безопасности (в широком смысле) станут первостепенными проблемами XXI в., и от их решения напрямую будет зависеть дальнейшее существование мировой цивилизации [13].

Если представить сечение куба, показанного на *рис*. 5, на уровне информационных угроз, то получим предметную область сферы деятельности «Информационная безопасность» в виде некоторой плоскости в двумерном пространстве с координатами «Жизненно важные интересы», реализации которых препятствуют информационные угрозы» и Основные методы «Защиты» от информационных угроз.

Необходимо заметить, что в этом представлении предметной области «Информационная безопасность» жизненно важными являются интересы рассматриваемого объекта защиты [12].

[9] ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М. : Госстандарт России, 1996.

[10] Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. М. : Гелиос АРВ, 2006. 528 с.

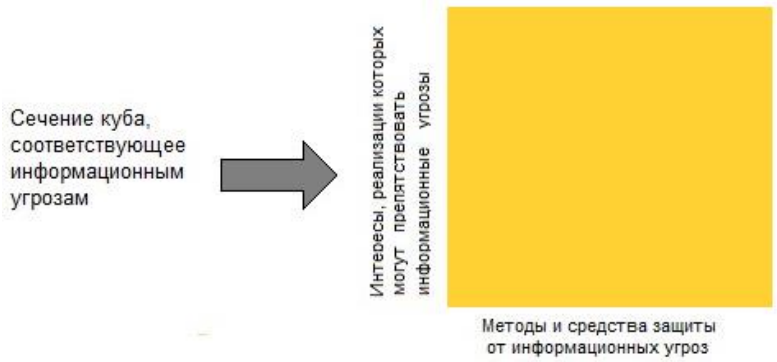

Рис. 5. Предметная область сферы деятельности «Информационная безопасность»

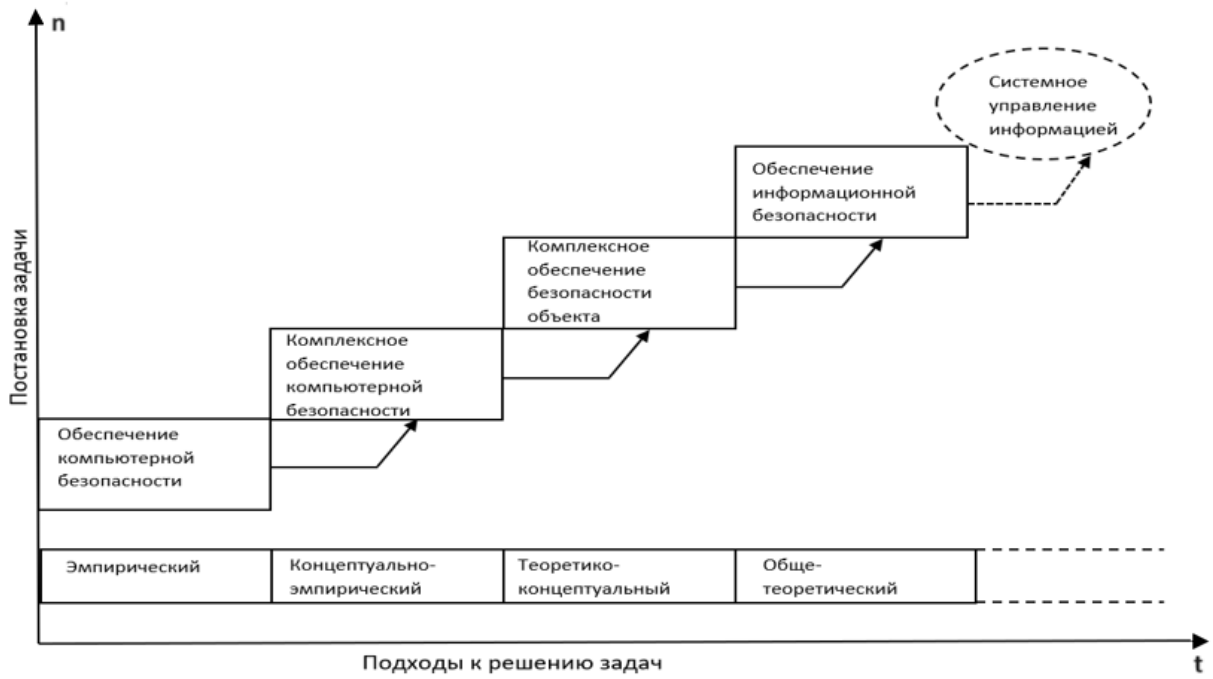

Рис. 6. Эволюция подходов к защите информации

Анализ этапов развития подходов к решению задачи защиты

Исторически начало работ по защите информации в автоматизированных системах как у нас в стране, так и за рубежом приходится на 1970—1980-е гг. в связи с появлением сетевых информационных технологий. Защита информации превратилась в одну из приоритетных областей деятельности, начали предприниматься активные попытки создания научно-методологической базы решения проблем защиты информации и обеспечения информационной безопасности систем[11].

Анализ опубликованных в этой области работ показывает стремление их авторов определенным образом исторически разделить развитие подходов к защите информации на несколько периодов. Для *первого* периода характерно стремление обеспечить надежную защиту информации чисто формальными механизмами, содержащими главным образом технические и программные средства, сосредоточенные в рамках системного программного обеспечения. *Далее* выделялся этап, на котором происходило активное развитие неформальных средств защиты, формирование концепции некоторого управляющего компонента — ядра безопасности. На *следующем* этапе сформировались взгляды на защиту как на непрерывный процесс, началось бурное развитие систем стандартизации в области защиты информации и обеспечения информационной безопасности. Основываясь на этом анализе, можно выделить ряд периодов развития подходов к защите информации и сформулировать некоторые их общие характеристики (*рис.* 6).

[11] Малюк А.А. Защита информации в информационном обществе : учебное пособие. М. : Горячая линия — Телеком, 2017. 230 с.

Первые попытки такой периодизации истории развития данной области, относящиеся к 1989 г., были основаны на критерии используемых средств защиты и способов их применения. В соответствии с этим принципом разными авторами выделялись три этапа: начальный, промежуточный и современный.

Если в качестве основного критерия периодизации принять определяющий для конкретного этапа методологический подход к защите информации (что больше соответствует современным взглядам на данную проблему), то эти три периода могут быть названы соответственно эмпирическим, концептуально-эмпирическим и теоретико-концептуальным. Обобщенные характеристики выделенных периодов при таком подходе приведены в *таблице*.

Обобщенные характеристики 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 комплексной защиты. 3. Введение понятия стратегии защиты. 4. Унификация концепции гарантированной защиты информации. 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

Суть ***эмпирического подхода*** к защите информации заключается в необходимости создания для этого механизмов на основе анализа ранее проявлявшихся угроз безопасности информации и накапливаемого опыта борьбы с ними. На этом этапе под защитой понималось, в основном, предупреждение несанкционированного получения информации лицами и процессами (программами), не имеющими на то полномочий. Хотя применялись и некоторые меры для обеспечения целостности информации, т. е. предупреждения ее уничтожения и искажения.

Следует заметить, что в это же время предпринимались попытки 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.

В целом последовательность процедур организации защиты информации на этапе эмпирического подхода может быть представлена в виде: изучение среды защиты; анализ уязвимости информации; определение требований к защите; построение механизмов защиты.

Основными характерными чертами эмпирического подхода являются: разовое включение в состав автоматизированной системы на этапе ее создания несложных механизмов защиты; использование формальных (программно-аппаратных) средств защиты; включение программных средств защиты в состав общесистемных компонентов (операционная система и система управления базами данных).

Сущность и содержание ***концептуально-эмпирического подхода*** к защите информации заключались в том, что на основе опыта, накопленного на этапе эмпирического подхода, удалось некоторым образом подойти к унификации используемого для решения этих задач методического и инструментального базиса.

Трансформация процедур организации защиты информации на этапе эмпирического подхода осуществлялась по следующим направлениям:

- в целях создания предпосылок для построения адекватных моделей защищаемых информационных систем и технологий предложена методология их структуризации;
- обеспечение объективной оценки уязвимости информации потребовало разработки системы показателей уязвимости, системной классификации угроз информации, методов и моделей определения и прогнозирования значений показателей уязвимости;

Рис. 7. Структура унифицированной концепции защиты информации

– построение механизмов защиты в качестве основы стали использовать цепочку концептуальных решений: определение функций и задач защиты, выбор средств и построение *системы*[12] защиты;
– в целях повышения эффективности защиты предусматривалась обратная связь концептуальных решений с той средой, в которой она осуществляется.

В результате сформировалась концепция защиты информации, которая получила название унифицированной (УКЗИ)[13]. В дальнейшем данная концепция получила новое развитие, и сегодня ее можно представить, как совокупность методологий оценки уязвимости информации, выработки требований и формирования оптимальной системы защиты информации. Таким образом, она приобрела вид, схематично показанный на *рис.* 7.

Отметим, однако, что УКЗИ и сегодня еще не имеет системной реализации всей совокупности содержащихся в ней положений. Это объясняется рядом серьезных трудностей, обусловленных, прежде всего, значительным своеобразием процессов защиты информации, связанным с решающим влиянием на них случайных и трудно предсказуемых факторов. В силу этого методы классической теории систем далеко не всегда адекватны характеру реальной ситуации защиты, что говорит о необходимости расширения формальной теории за счет привлечения неформальных методов [6].

Особое внимание на этапе концептуально-эмпирического похода уделялось техническим, программно-аппаратным и криптографическим средствам обеспечения безопасности информации[14].

Необходимо остановиться на предложенной тогда и сохраняющей актуальность и сегодня классификации средств защиты. Технические средства наиболее часто классифицируются по четырем критериям: функциональному назначению; типу, указывающему на принцип работы их элементов; уровню сложности (в том числе их практического использования); стоимости приобретения, установки и эксплуатации.

В отдельный класс обычно выделяются криптографические средства, которые в настоящее время составляют непременный компонент любой сколько-нибудь серьезной системы защиты информации, особенно в сетевых структурах, где они являются практически единственно надежными. Имея многовековую историю развития, к настоящему времени криптографические средства достигли весьма высокого уровня совершенства. Причем сегодня в связи с лавинообразным процессом внедрения юридически значимого электронного документооборота мощный импульс к дальнейшему развитию получили несимметричные системы с открытым ключом [7].

Весьма интенсивно на этапе концептуально-эмпирического подхода совершенствовались методы

[12] Ухлинов Л.М. Принципы построения системы управления безопасностью данных в информационно-вычислительных сетях // Автоматика и вычислительная техника. 1990. № 4. С. 11—17 .

[13] Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн. 1 и 2. М. : Энергоатомиздат, 1994. 401 с. и 176 с.

[14] Кульба В.В., Ковалевский С.С., Шелков А.Б. Достоверность и сохранность информации в АСУ. М., Синтег, 2004. 496 с.; Ловцов Д.А. Контроль и защита информации в АСУ. В 2-х кн. Кн. 1. Вопросы теории и применения. М. : ВА им. Петра Великого, 1991. 172 с.

и разрабатывались средства защиты от так называемых разрушающих закладок — вредоносных программ, под которыми понимаются «троянские кони», «компьютерные вирусы», «черви», «логические бомбы» и др. [2]. Такие закладки появились чуть ли не одновременно с актуализацией самой проблемы защиты. Борьба с ними первоначально носила оборонительный характер: после обнаружения закладки (нередко уже после осуществления ею разрушающего воздействия) изучался ее характер, после чего разрабатывались методы и средства борьбы с нею. Учитывая, что количество различных закладок растет лавинообразно, 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 их обнаружения и унификации способов и средств борьбы с ними. Появился даже термин «компьютерная вирусология». Создаваемые средства преследуют цели предупреждения заражения компьютера, лечения зараженного компьютера, а также создания программ, устойчивых к заражению[15].

В целом для концептуально-эмпирического этапа характерно существенное расширение функциональных возможностей защиты за счет комплексирования различных средств в многофункциональные механизмы. При этом наиболее удачные разработки принимались в качестве стандартов.

На этапе концептуально-эмпирического подхода впервые начали говорить о комплексном характере защиты информации. Наиболее ярко по этому поводу выразился известный американский криптограф, президент компании «*Counterpane Systems*» Брюс Шнайер, который в одном из своих выступлений сказал: «*Тот, кто думает, что может решить проблемы безопасности с помощью технологии, тот не понимает ни проблем безопасности, ни проблем технологии*»[16].

Это свидетельствует о комплексности проблемы защиты информации и необходимости учета технологического, организационно-правового и гуманитарного аспектов информационной безопасности. Тем более что, как показывает практика, причина подавляющего большинства инцидентов (до 80%) кроется именно в недостатках организации правовой и гуманитарной сфер[17].

Взгляд на защиту информации как на комплексную проблему на этапе концептуально-эмпирического подхода привел к значительному развитию арсенала средств, особенно неформальных (организационно-правовых), а также к выделению управляющего элемента (ядра безопасности) и назначению лица, имеющего специальную подготовку, в качестве ответственного за защиту (например, администратор безопасности — в России или офицер безопасности — в США).

Отличительная особенность ***теоретико-концептуального подхода*** к защите информации состоит в том, что на основе достижений концептуально-эмпирического подхода предпринимаются попытки разработать основы *целостной теории* (включая информационно-энтропийные формализмы[18]) и тем самым подвести под решение проблем защиты прочную научно-методологическую базу. При этом теория защиты информации определяется как совокупность основных идей в данной области знания. Главное предназначение рассматриваемой теории состоит в том, чтобы дать полное и адекватное представление о сущности и содержании проблемы и предложить научно-методологическую базу, обеспечивающую эффективное решение всех (или большинства) задач защиты с использованием доступных инструментальных средств. То есть на этапе теоретико-концептуального подхода осуществляется переход к интенсивным (основанным на научном знании) способам и методам защиты информации и, главным образом, *перерабатываемой*[19] [16] («динамической») в автоматизированных системах.

В качестве других отличительных особенностей теоретико-концептуального подхода можно выделить еще два принципиальных положения:

первое — защита информации рассматривается как непрерывный процесс, осуществляемый на всех этапах жизненного цикла автоматизированной системы, с помощью *комплексного* использования имеющихся средств защиты;

второе — основой функционирования средств защиты является созданная нормативная правовая база [9].

Сущность подходов к защите в течение этих периодов изменялась от выбора средств на основе опыта через все более настоятельные попытки разработки и научного обоснования методов оценки уязвимости информации и синтеза оптимальных механизмов к разработке в настоящее время основ теории защиты информации. Суть современного этапа заключается в постановке задачи *многоаспектной комплексной защиты*[20] и формировании для этого унифицированной

[15] Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М. : Горячая линия — Телеком, 2006. 544 с.

[16] Домарев В.В. Безопасность информационных технологий (системный подход). М. : ДиаСофт, 2004. 688 с.

[17] Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации : учебное пособие. СПб. : Питер, 2023. 384 с.

[18] Ловцов Д.А. Контроль и защита информации в АСУ. В 2-х кн. Кн. 2. Моделирование и разработки. М. : ВА им. Петра Великого, 1997. 252 с.; Князев В.В., Ловцов Д.А. Ситуационное планирование защищённой переработки информации в АСУ испытаниями сложных динамических объектов // Автоматика и Телемеханика. 1998. № 9. С. 166—181.

[19] Князев В.В., Ловцов Д.А. Защита перерабатываемой информации в АСУ // НТИ. Сер. 2. Информ. процессы и системы. 1996. № 7. С. 21—27; Оптимизация защищённой переработки формализованной информации в АСУ // НТИ. Сер. 2. Информ. процессы и системы. 1997. № 7. С. 23—30.

[20] Шангин В.Ф. Комплексная защита информации в корпоративных системах : учебное пособие. М. : ИНФРА-М, 2012. 592 с.

концепции *гарантированной*[21] защиты информации, т. е. защиты информации от деструктивных воздействий, как по традиционным, так и по *нетрадиционным* («*скрытым*»[22] [5, 7—11]) информационным каналам. Изменялись и необходимые для этой цели средства: от функционально ориентированных механизмов до *системы комплексной защиты* и создания изначально защищенных информационных технологий[23].

Знаменательно, что периодизация истории развития подходов к защите информации в основном соответствует сформулированной еще в XIX в. системе ступеней или фаз развития любой науки[24]. Предлагается пять ступеней формирования области научного знания: собирание материалов, искусственная система, естественная система, частные эмпирические законы, общий рациональный закон. В связи с этим можно считать, что эмпирический, концептуально-эмпирический и теоретико-концептуальный подходы соответствуют стадиям собирания материалов, искусственной и естественной системам. Можно *предположить*, что дальнейшее развитие теории защиты информации будет идти в направлении формулирования частных эмпирических законов и общего рационального закона, что соответствует созданию аксиоматической теории [7, 15].

На сегодняшний день удалось разработать основы целостной теории защиты информации и этим самым подвести под ее реализацию прочную научно-методологическую базу [7]. Вместе с тем следует заметить, что до последнего времени системная реализация всех положений данной теории сдерживается рядом серьезных трудностей, связанных с повышенным влиянием случайных факторов на процессы защиты информации, недостаточно четкой проработкой инструментальных средств решения задач анализа и синтеза систем и процессов защиты, с отсутствием значительной части исходных данных, необходимых для обеспечения решения названных задач.

Количественная и качественная оценка защиты информации

При решении практических задач защиты информации первостепенное значение имеет количественная оценка ее уязвимости и угроз. Изучение и классификация угроз безопасности проводились на протяжении всего периода существования проблемы защиты информации предпринимались попытки классифицировать источники угроз безопасности и сами угрозы с целью дальнейшей стандартизации средств и методов, применяемых для борьбы с ними.

Так, например, классификация угроз включала пять групп: хищение носителей, запоминание или копирование информации, несанкционированное подключение к аппаратуре, несанкционированный доступ к ресурсам системы, перехват побочных излучений и наводок[25].

В то же время встречается иная классификация, причем в качестве ее критерия выбран тип средства, с помощью которого может быть осуществлено несанкционированное получение информации: человек, аппаратура и программа[26].

Гостехкомиссией России, в свое время ответственной за техническую защиту информации, было введено понятие *модели нарушителя* в автоматизированной системе обработки данных, причем в этом качестве рассматривался субъект, имеющий доступ к работе со штатными средствами системы. Нарушители были классифицированы по уровню возможностей, предоставляемых им штатными средствами.

Достаточно детальный анализ угроз несанкционированного получения информации позволил ввести понятие *дестабилизирующих факторов*, источников их проявления и причин нарушения защищенности информации. Предложены подходы к формированию относительно полных множеств указанных причин и получена структура этих множеств, применительно к нарушению физической целостности информации и несанкционированному ее получению[27].

В процессе формирования множества угроз достаточно четко проявилась тенденция перехода от эмпирических к теоретико-концептуальным, научно обоснованным подходам. В этой связи может представлять интерес классификация угроз безопасности информации по способам их возможного негативного воздействия. Такой подход принят в Доктрине информационной безопасности Российской Федерации. Он заключается в подразделении угроз на информационные, программно-математические, физические и организационные.

В отличие от угрозы, уязвимость связана с недостатками защищаемой системы или объекта, облегчающими реализацию той или иной угрозы (осуществление атаки на систему или объект). Таким образом, уязвимость может быть определена как возможность возникновения на каком-либо этапе жизненного цикла автоматизированной системы такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

---

[21] Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М. : Яхтсмен, 1996. 302 с.

[22] ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. М. : Ростехрегулирование, 2008. 24 с.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 2. Рекомендации по организации защиты. М. : Ростехрегулирование, 2009. 26 с.

[23] Домарев В.В. Безопасность информационных технологий (системный подход). М. : ДиаСофт, 2004. 688 с.

[24] Данилевский Н.Я. Россия и Европа. М. : Книга, 1991. 574 с.

[25] Хоффман Л.Дж. Современные методы защиты информации. М. : Сов. радио, 1980. 262 с.

[26] Спесивцев А.В., Вегнер В.А., Крутиков А.Ю., Серегин В.В., Сидоров В.А. Защита информации в персональных ЭВМ. М. : Радио и связь, 1992. 192 с.

[27] Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий : учебное пособие. М. : МИФИ, 1995. 96 с.

Поскольку воздействие на информацию различных факторов в значительной мере является случайным, то в качестве количественной меры целесообразнее принять вероятность нарушения защищенности (изменения важнейших характеристик), а также потенциально возможные размеры наносимого ею ущерба. В совокупности эти параметры будут представлять собой не что иное, как оценку риска нарушения защищенности информации.

Какие факторы влияют на вероятность нарушения защищенности информации? Очевидно, к ним могут быть отнесены: количество и типы структурных компонентов защищаемой системы (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 довольно часто превращаются в неформальную задачу, которая может решаться на основе методов экспертных оценок.

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

Вопрос оценки ущерба представляет на сегодняшний день наиболее сложную задачу, зачастую не поддающуюся формализации. Исходной посылкой при оценке ущерба может явиться предположение, что полные ожидаемые затраты могут быть выражены суммой расходов на защиту и потерь от ее нарушения. При этом подходе оптимальным решением было бы выделение на защиту информации средств в размере C_{opt} (*рис*. 8), поскольку именно при этом обеспечивается минимизация общей стоимости защиты информации. Следовательно, целесообразный уровень затрат на защиту равен уровню ожидаемых потерь при нарушении защищенности. Это может явиться базой для обоснования размеров ресурсов, выделяемых на создание и реализацию систем обеспечения информационной безопасности в различных сферах деятельности.

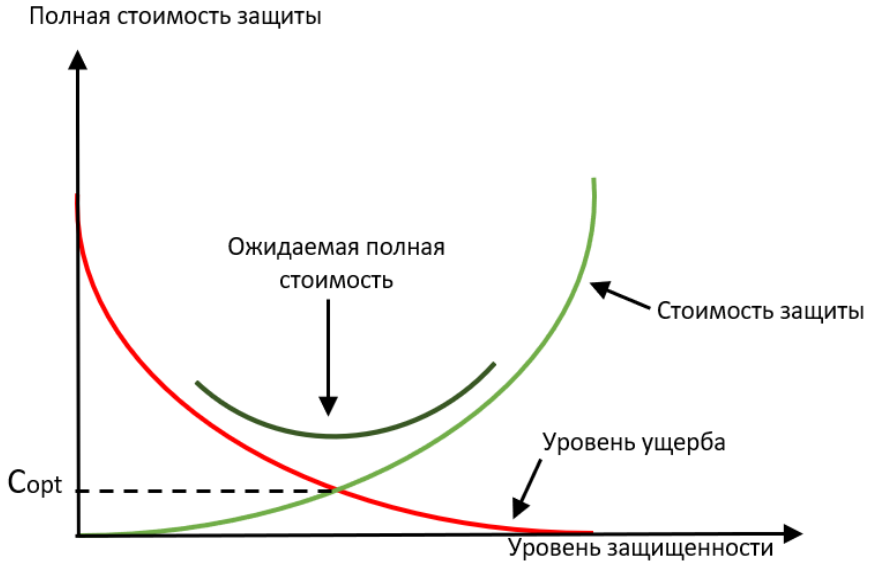

Рис. 8. Стоимостные зависимости защиты информации

В практических приложениях чаще всего риск оценивается в стоимостном выражении путем перемножения вероятности реализации той или иной угрозы и стоимости наносимого при этом ущерба [7].

Встречаются и другие подходы к оценке информационного риска, в том числе представляющие его в виде некоторой безразмерной величины. Наибольшего внимания среди них заслуживает предложение фирмы *IBM*, сделанное ею более десяти лет назад. Суть его состоит в определении двух ранговых констант P (вероятность проявления угрозы) и U (константа размера ущерба), связанных с частотой появления угроз и оцененными тем или иным способом размерами ущерба [1].

Формула определения безразмерной величины риска в этом случае будет иметь вид:

$$R = \frac{10^{P-3}}{5} 10^{U}. \quad (1)$$

Поскольку целью применения мер обеспечения защищенности информации является уменьшение риска либо за счет уменьшения вероятности осуществления угрозы, либо за счет уменьшения эффекта воздействия угрозы, то эффект защиты (уменьшение риска) может быть определен следующим образом:

$$\Delta R = R_2 - R_1, \quad (2)$$

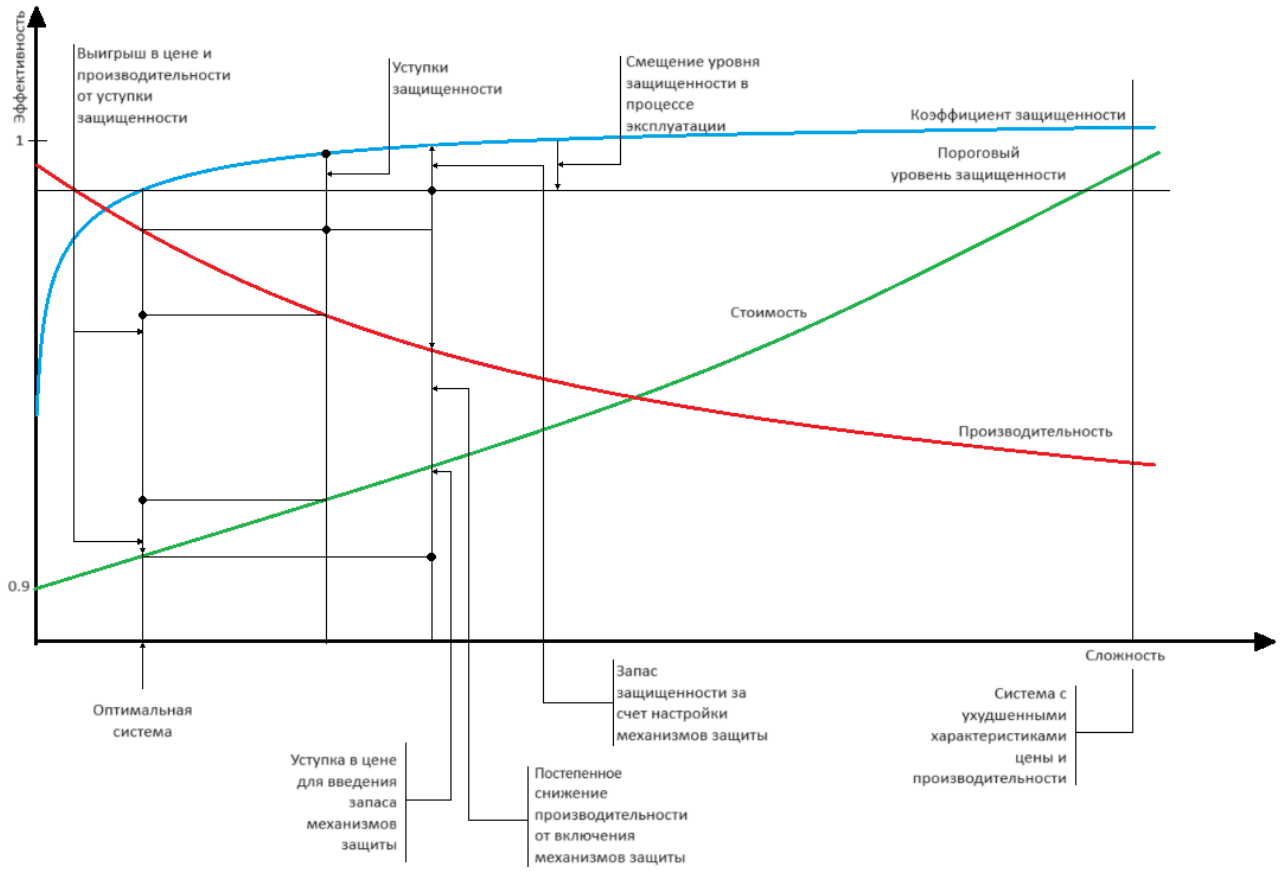

Рис. 9. Метод последовательного выбора уступок

где R_1 — риск без защиты; R_2 — риск с защитой (либо уменьшение вероятности угрозы, либо снижение ущерба).

Заметим, что с экономической точки зрения мера защиты оправдана, если эффект от ее применения, выраженный через уменьшение ожидаемого экономического ущерба, превышает затраты на ее реализацию.

Представленные на *рис*. 8 зависимости носят качественный характер, позволяющие понять существо процесса системы защиты, но никак не решить задачу оптимизации значения параметров ее механизмов. Задача проектирования системы защиты принципиально отличается от задач проектирования иных информационных систем, так как оно осуществляется с учетом статистических данных об уже существующих угрозах. В процессе функционирования системы защиты множество угроз может принципиально измениться. В частности, это связано с тем, что многие угрозы предполагают нахождение злоумышленниками ошибок в реализации системных и прикладных средств, которые могут быть неизвестны на момент создания системы защиты, но должны быть учтены в процессе ее функционирования[28].

Исходя из этого, проектирование системы защиты — процедура итерационная, в общем случае предполагающая следующие этапы:

- проектирование первоначальной системы защиты (исходный вариант);
- анализ защищенности на основе статистических данных, полученных в процессе эксплуатации системы защиты;
- модификация «узких мест» системы защиты (настройка/замена/дополнение отдельных механизмов защиты информации).

После модификации «узких мест» происходит возврат к эксплуатации системы защиты и накопление статистической информации. Вариант качественной зависимости изменения основных параметров, характеризующих систему защиты, от ее сложности — используемого набора механизмов защиты, представлена на *рис*. 9. Проанализировав характер зависимостей от сложности системы, можно заметить, что стоимость системы защиты возрастает неограниченно, а производительность снижается в пределе до нуля.

Получение аналитических зависимостей сложная и кропотливая работа, связанная с интерполированием исходных данных. Иногда, с целью улучшения точности для построения области допустимых решений задачи, ограниченной полученными кривыми, необходимо проводить аппроксимацию данных одним из ме-

[28] Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб. : Наука и техника, 2004. 384 с.

тодов *математической статистики*[29] [3]. Это необходимо, чтобы в точках (узлах) интерполяции обеспечивалось не только равенства полинома, но и совпадали производные полинома и функции до некоторого порядка. Доказано существование и единственность такого полинома, который «конструируется» подобно полиному Лагранжа, но в общем случае имеет весьма громоздкий вид. Такие полиномы часто называют полиномами с кратными узлами.

В то же время кривая коэффициента защищенности (D) стремится к предельному значению — к единице (100%) и в некоторый момент достигает насыщения. Это, в свою очередь, приводит к тому, что при дальнейшем нарастании сложности (и, соответственно, увеличении цены, а также снижении производительности) увеличение коэффициента защищенности происходит незначительно.

Следовательно, при проектировании системы защиты, параметры защищенности которой расположены в области насыщения, целесообразно проанализировать параметры альтернативных вариантов. То есть целесообразно исследовать возможность использования менее сложных систем защиты и, задав некоторый промежуток снижения коэффициента защищенности (ΔD), выбрать систему, уровень защищенности которой удовлетворяет полученному $(D - \Delta D)$. Конечно, если таковые имеются. При этом может быть получен ощутимый выигрыш в цене и производительности.

В этом и состоит суть известного метода последовательных уступок (иногда называют методом разумного компромисса) при выборе оптимальной системы защиты (набора реализуемых механизмов защиты при ее проектировании) [4]. Этот метод подразумевает сведение многокритериальной задачи оптимизации к однокритериальной.

Метод последовательных уступок представляет собою итерационную человеко-машинную процедуру, используя которую разработчик, давая допустимые приращения одним параметрам (в частности, задавая снижение коэффициента защищенности), анализирует изменение других, принимая решение о допустимости вводимых уступок.

Казалось бы, не теряя общности рассуждений, вместо аналитических выражений функций, ограничивающих область допустимых решений задачи защиты, можно было бы использовать хотя бы аналитические уравнения поверхностей 2-го порядка. К сожалению, в этом случае возникает ряд сложностей, связанных с проверкой замкнутости полученной области и нахождения рационального решения в ней. При этом вызывает определенные трудности сам процесс построения ограничивающих поверхностей[30].

Особо необходимо отметить одну принципиальную особенность функционирования системы защиты. Суть ее заключается в том, что коэффициент защищенности непрерывно снижается в процессе функционирования защищенной системы[31]. Это связано с накоплением информации злоумышленником о системе защиты, а также с накоплением статистики об ошибках реализации системных и прикладных средств.

Основой всякого развития любой системы, в соответствии с первым законом диалектики (единство и борьба противоположностей), является борьба противоположностей (*рис.* 4). То есть «угрозы» — «защита», являющиеся противоположностями, взаимосвязанными и взаимодействующими, причем эта взаимосвязь выражается в том, что каждая из них имеет собственную противоположность и только ограниченность человеческого знания не позволяет видеть все существующие связи.

Появившиеся в последнее время публикации позволяют судить о том, что имеется потенциальная возможность добиться такого состояния («угрозы» — «защита»), когда они будут управляемыми и/или не будут выходить из-под контроля[32]. Задача заключается в том, чтобы, зная множество показателей, характеризующих отдельные аспекты функционирования некоторой системы, получить обобщённую оценку ее состояния. По ряду частных показателей необходимо определить, насколько близко она находится к зоне риска (кризиса).

Математическое моделирование задачи защиты информации

Задача состоит в разработке математической модели, основанной на положениях теории нечетких множеств и логико-лингвистического моделирования, реализация которой позволит определить оценочную функцию диагностируемой системы при условии отказа от сформулированного допущения о независимости ее составляющих.

Идея построения эвристической модели сводится к имитации нестрогой (приближенной) логики мышления эксперта при оценке им качества управленческих решений, замене числовых (количественных) переменных на качественные (лингвистические, а также в использовании нечетких эвристических) критериев и алгоритмов для установления функциональных зависимостей между входными и выходными параметрами системы.

При этом используются следующие *допущения*:

– эксперт имеет представление о «важных» переменных, описывающих защищаемый объект, воспринимает взаимосвязи этих переменных и умеет

[29] Ловцов Д.А., Богданова М.В., Лобан А.В., Паршинцева Л.С. Статистика (компьютеризированный курс) / Под ред. проф. Д.А. Ловцова. М. : РГУП, 2020. 400 с. ISBN 978-5-93916-834-2.

[30] Копченова Н.В., Марон И.А. Вычислительная математика в примерах и задачах : учебн. пособие. СПб. : Лань, 2009. 308 с.

[31] Ветцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. М. : Высш. шк., 2007. 479 с.

[32] Новосельцев В. И., Тарасов Б. В. Системная теория конфликта : монография. М. : Майор, 2011. 336 с.

оперировать правилами, связывающими переменные с управляющими решениями;
- эксперт предпочитает использовать свои собственные интуитивные правила оценки обобщенных показателей и выбора управлений, не гарантирующих математической оптимальности, но позволяющих принимать достаточно эффективные решения в сложных управленческих ситуациях;
- любая лингвистическая переменная исчерпывающим образом описывается функцией принадлежности, а логический критерий выбора состоит в том, чтобы в качестве решения выбирать такое значение переменной, в котором функция принадлежности принимает максимальное значение.

Рассмотрим некоторую диагностируемую систему Q, для которой известны ее входы, выходы и внешние возбуждения (независимые внешние воздействия со стороны среды, в которой происходит ее функционирование).

Пусть $x = \{x_1, x_2, \dots, x_N\}$ — множество входных параметров, $y = \{y_1, y_2, \dots, x_K\}$ — множество выходных параметров, $z = \{z_1, z_2, \dots, z_M\}$ — множество внешних возбуждений, где x_n, y_k, z_m — числовые переменные.

Можно считать, что если заданы параметры $x_n \in X$, $y_k \in Y$, $z_m \in Z$, то известны их значения соответствующие определенному состоянию системы $s \in S$ в некоторый фиксированный момент времени t. Кроме того, для каждого параметра из множеств X, Y, Z известны их нормы и критические значение. Обозначим: $\delta x^*, \delta y^*, \delta z^*$ — критические отклонения параметров входа, выхода и внешних возбуждений от нормы; δx, δy, δz — фактические отклонения параметров от нормы.

Модель диагностируемой системы Q представляется кортежем:

$$M_Q = < \eta_x(X), \eta_y(Y), \eta_z(Z), \eta_s^{tec}(X,Y,Z) >, \quad (3)$$

где $\eta_x(X), \eta_y(Y), \eta_z(Z)$ — оценочные функции входных, выходных и внешних параметров соответственно; $\eta_s^{tec}(X,Y,Z) = \eta_s(\eta_x(X), \eta_y(Y), \eta_z(Z))$ — оценочная функция текущего состояния системы.

При выборе функций η_x, η_y, η_z, η_s исходим из того, что как сами функции, так и взаимные зависимости их аргументов нельзя задать количественно, но можно выразить качественно, используя нечеткое η-пространство со шкалами T, P, η, где T — оценочная лингвистическая шкала «часто-редко», значения которой определены на интервале от «никогда» до «всегда», с числовым представлением в интервале [0, 2]; P — метрическая числовая шкала, на которой измеряются фактические значения параметров x_n, y_k, z_m; η — оценочная лингвистическая шкала, элементы которой принимают значения на интервале от «хуже не бывает» до «лучше не может быть», с числовым представлением [–1, +1].

То есть, как модель диагностируемой системы, так и оценки ее состояния заданы на нечетком η-пространстве в виде логико-лингвистических представлений нечетких характеристик, при конструировании которых качественным образом учитываются взаимные связи между параметрами системы.

Введем *предположение*, что среди множества состояний $s \in S$ существует кризисное состояние $s^* \in S$, характеризующееся нахождением текущих параметров системы в зоне критических значений (ущерб превышает заданное значение). Оценочную функцию такого состояния обозначим η_s^*. Тогда интегральная оценочная функция W диагностируемой системы представляется как кортеж:

$$W = < \eta_s^{tec}(X,Y,Z), \eta_s^*, \rho(\eta_s^*, \eta_s^{tec}(X,Y,Z)) >, \quad (4)$$

где $\rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))$ — функция, выражающая степень близости текущего и кризисного состояний.

Итак, рассматривается цепочка $Q \to M_Q \to W$, первый компонент которой — есть диагностируемая система, второй — ее логико-лингвистическое представление в пространстве $\{T, P, \eta\}$, а третий — искомая интегральная оценочная функция.

Тогда задача сводится к определению модели системы M_Q через оценочные функции $\eta_x(X), \eta_y(Y), \eta_z(Z), \eta_s^{tec}(X,Y,Z)$ и к нахождению правил вычисления η_s^* и $\rho(\eta_s^*, \eta_s^{tec}(X,Y,Z))$.

Представленный подход позволит более точно определить область допустимых решений задачи в методе последовательных уступок, и существенно уточнить ее в процессе функционирования защищенной системы.

Заключение

Современный взгляд на защиту информации как на *комплексную проблему* неминуемо приводит к возрастанию значимости системных вопросов, связанных с этим процессом (формирование общей политики защиты, оптимизация процессов проектирования и функционирования комплексных систем, сбор и аналитическая обработка данных о функционировании реальных систем защиты информации). Таким образом, возникает *проблема системной согласованности* вопросов обеспечения информационной безопасности с остальными задачами решения информационных проблем общества. Она имеет как научно-методологические, так и организационные аспекты, и ее решение может базироваться на унифицированной концепции гарантированной защиты информации. Данная концепция применима на всех трех уровнях защиты: компьютерном, объектовом, региональном (государственном). Она создает необходимые объективные предпосылки для перехода к новому общетеоретическому этапу в решении возникающих при этом задач интенсификации процессов защиты информации.

Рассмотрев, по сути, этапы развития подходов к защите информации, анализируя весь многолетний опыт организации ее защиты в автоматизированных системах, представляется целесообразным сформулировать

следующие принципиальные ***выводы***, определяющие дальнейшие перспективы развития теории и практики защиты информации:

1. Проблемы обеспечения защищенности информации носит перманентный характер, вследствие чего необходима развитая и регулярно функционирующая система, обеспечивающая эффективное решение всей совокупности соответствующих задач.

2. Обеспечение защищенности информации в обязательном порядке должно носить комплексный характер.

3. Комплексность защиты информации может быть достигнута лишь при взаимосогласованных усилиях всех субъектов, участвующих в процессах сбора, передачи, хранения, логической обработки и использования информации.

4. Надежную защиту информации можно обеспечить лишь в том случае, если проблемы защиты будут решаться в тесной взаимосвязи с проблемами информатизации и автоматизации.

5. Эффективное решение проблем защиты информации в современной постановке возможно только при наличии развитого и адекватного научно-методологического базиса и формально-логического аппарата.

Рецензент: ***Алексеев Владимир Витальевич,*** *доктор технических наук, профессор, член-корреспондент РАЕН, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*
E-mail: vvalex1961@mail.ru

Литература

1. Астахов А.М. Искусство управления информационными рисками. М. : ДМК Пресс, 2010. 312 с.
2. Анин Б.Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2016. 384 с.
3. Демидович Б.П., Марон И.А., Шувалова Э.З. Методы приближенных вычислений. М. : ИД «Наука», 2015. 400 с.
4. Булатов В. Математическое моделирование сложных систем. Элементы теории и приложения. М. : LAP, 2014. 406 с.
5. Ловцов Д.А. Информационная безопасность и нетрадиционные угрозы // Федеральный справочник. Т. 8. Оборонно-промышленный комплекс России. М. : Центр стратег. исследований, 2013. С. 507—512.
6. Ловцов Д.А. Информационная теория эргасистем : монография. М. : РГУП, 2021. 314 с. ISBN 978-5-93916-887-8.
7. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
8. Ловцов Д.А. Информационная теория эргасистем. Тезаурус : монография. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
9. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере : монография. М. : РГУП, 2016. 316 с. ISBN 978-5-93916-505-1.
10. Ловцов Д.А., Ермаков И.В. Классификация и модели нетрадиционных информационных каналов в эргасистеме // Науч.-техн. инф. Сер. 2. Информ. процессы и системы. 2005. № 2. С. 1—7.
11. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // Науч.-техн. инф. Сер. 3. Информ. процессы и системы. 2006. № 9. С. 1—9.
12. Ловцов Д.А., Сергеев Н.А. Управление безопасностью эргасистем / Под ред. Д.А. Ловцова. М. : РАУ-Университет, 2001. 224 с.
13. Малюк А.А. Теория защиты информации : монография. М. : Горячая линия — Телеком, 2012. 184 с.
14. Расторгуев С.П. Информационная война. Проблемы и модели. М. : Гелиос АРВ, 2006. 221 с.
15. Сети следующего поколения NGN / Под ред. А.В. Рослякова. М. : Эко-Трендз, 2008. 420 с.
16. Knyazev V.V., Lovtsov D.A. Situation Oriented Planning of Protected Processing of the Measurement Information in the Automated Control Systems of Testing of Complex Dynamic Objects. Automation and Remote Control. 1998. Vol. 59, No 9. Part 2. Pp. 1336—1346.

INFORMATION PROTECTION IN AUTOMATED SYSTEMS: CONCEPTUAL AND MATHEMATICAL ASPECTS

Vladimir Goncharov, *Dr.Sc. (Technology), Professor, Honoured Figure of Higher School of the Russian Federation, Head of the Department of Mathematics of the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: v_v_goncharov@mail.ru

Ol'ga Mishenina, *Ph.D. (Paedagogy), Associate Professor, Professor at the Department of Mathematics of the Peter the Great Military Academy, Moscow, Russian Federation.*
E-mail: o.v.mishenina@gmail.com

Keywords: *versatile information protection, information protectedness, information quality, information security, automated system, vulnerability and security threats, system classification of threats, rating threats, information risk.*

Abstract

Purpose of the work: improving the information and mathematical support for a versatile approach to solving information security problems based on the dialectical unity of mutually agreed upon processes of informatisation of society.

Methods used in the study: system analysis and mathematical modelling allowing to reduce a multi-criteria optimisation problem to a single-criteria problem with a subsequent forming of an iterative procedure.

Study findings: a system and historical analysis of methods, means and measures for ensuring information protectedness was carried out considering an increase in its vulnerability in the conditions of development of modern information technologies and emergence of new threats. A mathematical model was developed for constructing a region of permissible problem solutions whose boundaries are analytical expressions (for functions) obtained as a result of interpolation (approximation) of the corresponding initial data, while the requirements as regards the values of parameters located in the "saturation" region can be reduced so as to increase the characteristics of others. The resulting iterative man-machine procedure allows to find a rational solution to the problem.

The obtained findings are the basis for setting up appropriate effective information and mathematical support for the hardware and software complex for studying the information security of complex dynamic objects.

References

1. Astakhov A.M. Iskusstvo upravleniia informatsionnymi riskami. M. : DMK Press, 2010. 312 pp.
2. Anin B.Iu. Zashchita komp'iuternoi informatsii. SPb. : BKhV-Sankt-Peterburg, 2016. 384 pp.
3. Demidovich B.P., Maron I.A., Shuvalova E.Z. Metody priblizhennykh vychislenii. M. : ID "Nauka", 2015. 400 pp.
4. Bulatov V. Matematicheskoe modelirovanie slozhnykh sistem. Elementy teorii i prilozheniia. M. : LAP, 2014. 406 pp.
5. Lovtsov D.A. Informatsionnaia bezopasnost' i netraditsionnye ugrozy. Federal'nyi spravochnik. T. 8. Oboronno-promyshlennyi kompleks Rossii. M. : Tsentr strateg. issledovanii, 2013, pp. 507–512.
6. Lovtsov D.A. Informatsionnaia teoriia ergasistem : monografiia. M. : RGUP, 2021. 314 pp. ISBN 978-5-93916-887-8.
7. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
8. Lovtsov D.A. Informatsionnaia teoriia ergasistem. Tezaurus : monografiia. M. : Nauka, 2005. 248 pp. ISBN 5-02-033779-Kh.
9. Lovtsov D.A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere : monografiia. M. : RGUP, 2016. 316 pp. ISBN 978-5-93916-505-1.
10. Lovtsov D.A., Ermakov I.V. Klassifikatsiia i modeli netraditsionnykh informatsionnykh kanalov v ergasisteme. Nauch.-tekhn. inf., ser. 2, Inform. protsessy i sistemy, 2005. No. 2, pp. 1–7.
11. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. Nauch.-tekhn. inf., ser. 3, Inform. protsessy i sistemy, 2006. No. 9, pp. 1–9.
12. Lovtsov D.A., Sergeev N.A. Upravlenie bezopasnost'iu ergasistem. Pod red. D.A. Lovtsova. M. : RAU-Universitet, 2001. 224 pp.
13. Maliuk A.A. Teoriia zashchity informatsii : monografiia. M. : Goriachaia liniia – Telekom, 2012. 184 pp.
14. Rastorguev S.P. Informatsionnaia voina. Problemy i modeli. M. : Gelios ARV, 2006. 221 pp.
15. Seti sleduiushchego pokoleniia NGN. Pod red. A.V. Rosliakova. M. : Eko-Trendz, 2008. 420 pp.
16. Knyazev V.V., Lovtsov D.A. Situation Oriented Planning of Protected Processing of the Measurement Information in the Automated Control Systems of Testing of Complex Dynamic Objects. Automation and Remote Control. 1998. Vol. 59, No 9. Part 2. Pp. 1336–1346.