ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

А. И. КУПРИЯНОВ, А. В. САХАРОВ, В. А. ШЕВЦОВ

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Допущено
Учебно-методическим объединением
по образованию в области авиации, ракетостроения и космоса
в качестве учебного пособия для студентов, обучающихся
по специальностям «Радиоэлектронные системы», «Средства радиоэлектронной борьбы» и «Информационные системы и технологии»

3-е издание, стереотипное

ACADEMIA

Москва
Издательский центр «Академия»
2008

УДК 621.37(075.8)
ББК 32.84я73
К924

Рецензенты:
д-р техн. наук, проф. кафедры «Защита информации»
Московского государственного технического университета им. Н.Э. Баумана
П.Б.Петренко;
д-р техн. наук, проф., заслуженный деятель науки и техники РФ *Е.М. Сухарев*

Куприянов А.И.
К924 Основы защиты информации : учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов. — 3-е изд., стер. — М. : Издательский центр «Академия», 2008. — 256 с.
ISBN 978-5-7695-5761-3

Рассмотрены основные проблемы, теоретические положения, потенциальные и технически достижимые характеристики качества, а также технические решения при построении систем защиты важнейшего современного ресурса — информационного — от негативных и деструктивных воздействий, характеризующих конфликт информационных систем с техническими средствами разведки.

Для студентов высших учебных заведений. Может быть полезно специалистам в области защиты информации.

УДК 621.37(075.8)
ББК 32.84я73

ISBN 978-5-7695-5761-3

Посвящается 75-летию
Московского авиационного института
(Государственного технического университета)
и 60-летию факультета радиоэлектроники
летательных аппаратов МАИ

ПРЕДИСЛОВИЕ

Разными аспектами проблемы защиты информации занимаются юристы, экономисты, связисты, военные, программисты и, разумеется, инженеры. Именно инженерам, точнее — молодым людям, изучающим основы инженерного дела в высших технических учебных заведениях, адресована эта книга.

Труд современного инженера протекает в информационной среде, а информация является основным предметом и продуктом инженерного труда. Поэтому безопасные приемы труда в информационном пространстве также важны для инженера, как выполнение требований техники безопасности в процессе работы по преобразованию вещества и энергии. В силу целого ряда причин, о которых речь пойдет ниже, именно проблемы безопасного обращения с информацией в процессе инженерного труда и творчества приобрели особую актуальность для современного этапа развития нашей технической цивилизации.

Проблема защиты информации возникает там, где есть противоречия, конфликт интересов в информационной среде. Изучая методы и средства защиты, всегда приходится иметь в виду информационные угрозы, их вид, характер и условия проявления. В учебном пособии рассматриваются информационные конфликты и угрозы, характерные для той среды, где функционируют современные технические и организационно-технические системы. Для подобных систем характерны большое разнообразие целей, задач и способов функционирования, значительное структурное разнообразие а также широкий спектр проявлений информационных конфликтов.

Требование широты охвата проблемы защиты информации вступает в противоречие с подробным изучением конкретных методов и средств информационной защиты. Поэтому в название книги внесено уточняющее дополнение «Основы». По той же причине из рассмотрения исключены весьма важные вопросы организации и управления информационной безопасностью предприятия (фирмы), т.е. менеджмент информационной безопасности. Не рассматриваются структура системы законов и подзаконных нормативных актов, регулирующих взаимоотношения в информаци-

онной сфере, а также особенности крайних проявлений информационных конфликтов в форме информационных войн (не путать со скандалами в журналистских тусовках, которые иногда и совершенно неправомерно именуют тем же термином), т.е. вопросы проектирования и применения информационного оружия (как оборонительного, так и наступательного), и некоторые другие вопросы, без которых можно обойтись при первоначальном ознакомлении с проблемой защиты информации.

Учебное пособие написано по материалам лекционных курсов, которые вели авторы на разных факультетах Московского авиационного института (Государственного технического университета).

Глава 1

ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Современное состояние, перспектива и ретроспектива

Очень велико искушение начать ретроспективу проблемы информации и информационной безопасности с истории о том, как сказалась надежность априорных данных на оптимизации стратегии поведения в ходе такой глобальной экологической катастрофы, как Великий Потоп или с того, как и к чему привела информационная незащищенность Адама и Еву. Но, избегая подобных банальностей, все-таки приходится утверждать, что если историю земной цивилизации положить на логарифмическую временну́ю шкалу (рис. 1.1), можно выявить любопытные закономерности.

С давних времен человечество обеспечивало свое существование за счет эксплуатации природных ресурсов, и в этой сфере (собирательство, охота, затем сельское хозяйство) было занято подавляющее большинство населения. На индустриальном этапе развития цивилизации определяющим в жизни человечества было промышленное производство (переработка вещества и энергии). Наконец на современном этапе постиндустриального общества определяющей формой трудовой деятельности стала переработка информации.

В экономически развитых обществах примерно 2 % населения заняты в сельском хозяйстве, 12 % — в промышленности (переработка вещества и энергии), 70 % — в информационной сфере.

Отечественная статистика не дает такой стратификации общества, традиционно разделяя население только по классовым, половым и возрастным признакам. Но есть все основания предполагать, что и для современной России занятость населения в сфере

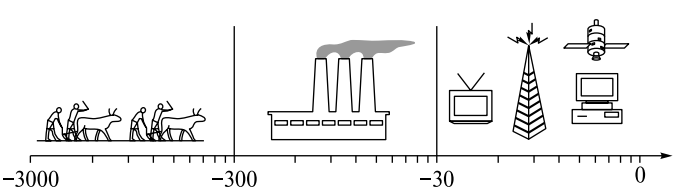

Рис. 1.1. Временна́я шкала смены доминант цивилизации на планете Земля

обслуживания национального информационного ресурса весьма значительна.

Даже исключив из рассмотрения такие высокоинформатизованные области, как управление (государственное, региональное, муниципальное и местное, в военной сфере и экономике). Не рассматривая масс-медиа, образование и науку, функционирующие исключительно в информационном пространстве, можно утверждать, что современные инженеры создают не вещи, а проектную документацию, т.е. информацию. Современные финансисты осуществляют информационное сопровождение финансовых потоков.

Если учесть все сказанное, не покажется большим преувеличением утверждение о том, что XXI в. войдет в историю как век информации и телекоммуникаций, подобно тому, как XX в. был веком электроэнергетики, XIX в. — веком пара, а XVI в. — веком великих географических открытий. Инфокоммуникации уже в самом начале XXI в. достигли высокой степени мобильности (сотовые сети связи). Они приобрели новое системное качество мультимедийности. В XXI в. человечество вступило, имея реальную возможность для создания общедоступной глобальной инфокоммуникационной инфраструктуры.

Такое положение информационной сферы современного постиндустриального информационного общества обусловливает целый ряд его специфических черт.

Во-первых, информация, в процессе получения и распространения которой занято большинство экономически активного населения, стала товаром, причем товаром массового производства и потребления. Но товаром весьма специфическим. На этот товар (информационный продукт) должны распространяться права собственности. Но если традиции и нормы, регулирующие права собственности на вещи, выработаны веками, то с информационными продуктами дело гораздо сложнее. Если некто имеет вещь и передает эту вещь другому, он эту вещь теряет, утрачивая права на нее. По меньшей мере он теряет одно или несколько звеньев триады «владеть — пользоваться — распоряжаться», составляющей основное содержание понятия собственности. Но если он передает некую сумму сведений (информацию, знания), то у него эти сведения тоже остаются. Значит, нужны какие-то иные регуляторы отношений в информационном пространстве.

Во-вторых, массовый характер получения и потребления информации требует разработки методов безопасного обращения с ней. Подобно тому, как массовое участие людей в процессе переработки вещества и энергии требовало массового образования в области безопасных методов труда. Пренебрежение требованиями безопасного обращения с информацией может привести к весьма негативным последствиям. Кто знает, не грозят ли информацион-

ному пространству техногенные катастрофы, подобные экологическим, вызванным нарушениями правил природопользования. Поэтому защита информации, которая должна не только разоблачать, но и предотвращать неправомерное, несанкционированное обращение с ней, приобретает особую актуальность.

В-третьих, в СССР существовала более или менее надежная государственная система мер защиты информации. Она иногда отставала от потребностей жизни, но, в целом, обеспечивала решение поставленных перед ней задач. Преобразования последних лет изменили отношения собственности (в том числе и собственности на информацию). И эти изменения потребовали кардинального пересмотра и значительного совершенствования мер и средств, направленных на обеспечение безопасности информационного ресурса, находящегося в распоряжении государства, отдельных предприятий и организаций, граждан.

В-четвертых, специфические требования к информационной безопасности предъявляются со стороны нынешнего уровня и темпов технического прогресса. За последние 30 лет количество физических процессов и объектов, используемых при подготовке, хранении, распределении и потреблении информации, увеличилось в несколько раз. Появление в информационной сфере каждого нового технического и технологического процесса предъявляет новые специфические требования к обеспечению информационной безопасности.

По современным воззрениям проблема информационной безопасности распадается на две, равноправные и диалектически связанные (рис. 1.2). Это проблема защиты информации (от утраты, искажения, несанкционированного доступа и использования) и защиты от информации (ложной, избыточной).

В мировое информационное пространство могут входить только развитые страны. Государства, не имеющие таких предпосылок всестороннего развития, все дальше отодвигаются на обочину социального и технического прогресса и становятся вечными маргиналами цивилизации. Подобная неравномерность прежде всего и определяет противостояние развитых стран и остального мира, стимулирует углубление противоречий, чревата нестабильностью и угрозами новых войн. Без подключения к мировому информационному пространству страну ожидает экономическое прозяба-

Рис. 1.2. Структура проблемы информационной безопасности

ние. Однако следует отчетливо представлять себе, что участие России в глобальных информационных процессах невозможно без комплексного решения проблем информационной безопасности, предполагающего как рациональное использование мирового информационного ресурса, так и защиту собственного национального информационного пространства от возможности деструктивного и негативного воздействия.

В настоящее время мир озабочен состоянием защиты национальных информационных ресурсов в связи с расширением доступа к ним через открытые информационные сети типа Internet. Кроме того что повсеместно увеличивается число компьютерных преступлений, реальной стала угроза информационных атак на более высоком уровне для достижения политических и экономических целей.

Для предотвращения или нейтрализации последствий таких атак необходимо:

- защищать материально-технические объекты, составляющие физическую основу информационных ресурсов;
- обеспечить нормальное и бесперебойное функционирование баз и банков данных;
- защитить информацию от несанкционированного доступа, искажения, уничтожения;
- сохранить качество информации (своевременности, точности, полноты и необходимой доступности).

Поскольку информационная сфера охватывает все области жизни, постольку информационная безопасность структурируется в

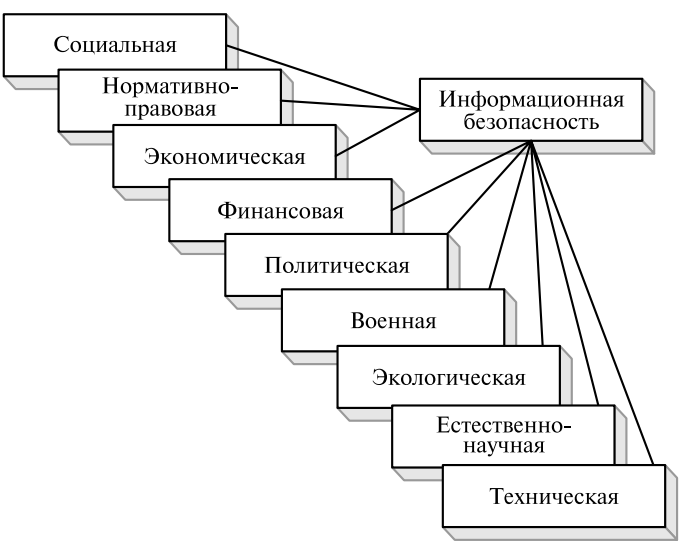

Рис. 1.3. Аспекты проблемы информационной безопасности

совершенно разных, но связанных аспектах (рис. 1.3). Совершенно определенно можно выделить социальные, нормативно-правовые, экономические, финансовые аспекты, информационную безопасность политической и военной сфер, безопасность экологической информации, естественно-научные и технические аспекты информационной безопасности.

Социальный аспект. Показателем цивилизованности общества и уровнем развития демократии является не только свобода доступа к любой информации, но и надежная защита информации ограниченного доступа. Сейчас мы довольно уверенно движемся от всеобщей секретности к информационной культуре. Именно этой идеей проникнута «Концепция информационной безопасности России», утвержденная Президентом России в 2000 г. Общественное мнение продвинуто от тотальных информационных ограничений в сторону информационной культуры гораздо меньше, чем законы РФ и «Концепция информационной безопасности России». Говоря о легком доступе к информации (особенно в Internet), мы прежде всего выделяем его негативные стороны и для борьбы с негативом соглашаемся на применение запретительных методов. Большинство режимных предприятий (кстати, разной формы собственности) не выработали мер безопасности обращения с информацией в условиях применения современных сетевых информационных технологий и пошли по простому, чисто формальному пути. Запретили Internet и e-mail в сфере своей юрисдикции.

Но это частности, а в целом приходится сознавать, что наше общество не вполне готово существовать и нормально функционировать в условиях возможных негативных и деструктивных информационных воздействий, информационно не защищено. Достаточно вспомнить, как население восприняло такое явление, как финансовые пирамиды. Люди всех социальных слоев с удовольствием и даже с азартом бросились исполнять предписания недобросовестных информационных (рекламных) воздействий на массовое сознание. Это наводит на грустные мысли о том, какие беды стране может принести применение информационного оружия массового поражения, если общество не выработает иммунитета к негативным информационным воздействиям, т.е. не научится приемам безопасного обращения с информацией.

Можно доискиваться до причин этого явления, ссылаясь на менталитет, многолетние традиции тотальной пропаганды, некритическое отношение к печатному (и произнесенному по каналам массового воздействия) слову, возможность некого заговора. Сейчас важен факт социальной неустойчивости против деструктивных информационных воздействий.

Нормативно-правовой аспект. Специалисты в области права и информатизации, особенно последние, в настоящее время все чаще

говорят об информационном законодательстве как самостоятельной отрасли права. Эта отрасль должна регулировать общественные отношения по реализации порядка защиты информации как объекта общественных отношений, прав граждан и юридических лиц на владение, использование и распоряжение информационными продуктом и услугами. Однако до сих пор нет достаточно четкого представления о том, что такое информационное законодательство, не определена сфера его правового регулирования, и придание самостоятельности такой отрасли законодательства пока вызывает возражения.

На сегодняшний день законы РФ, прямо или косвенно связанные с информационной сферой, немногочисленны и не образуют целостной системы, обеспечивающей регулирование всего спектра отношений в этой сложной и комплексной сфере.

Проблемы защиты информации регулируются Законами РФ «О государственной тайне», «Об информации, информатизации и информационной безопасности», «О правовой охране программ для электронных вычислительных машин и баз данных», «О правовой охране топологий интегральных микросхем», «Об авторском праве и смежных правах», «О федеральных органах правительственной связи и информации», «Об Архивном фонде Российской Федерации и архивах», «О средствах массовой информации» с последними дополнениями.

В Уголовном кодексе (УК) РФ, вступившем в действие 1 января 1997 г., за преступления в сфере компьютерной информации предусмотрена уголовная ответственность (гл. 28, ст. 272—274). Самая серьезная санкция — лишение свободы на срок от трех до семи лет за создание, использование и распространение вредоносных программ для ЭВМ, повлекших тяжкие последствия. Таким образом, новый УК вводит в употребление новое понятие: «вредоносные программы», под которыми понимаются программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также приводящие к нарушению работы ЭВМ, системы ЭВМ или их сети. В настоящее время такие программы общепринято называть программными закладками и компьютерными вирусами.

В целом, принятие нового УК является шагом вперед в определении понятия «компьютерные преступления» и квалификации отдельных правонарушений. Но пока этот шаг очень робкий и наивный. Юристы считают, что для вхождения России в мировое информационное пространство в качестве полноправного члена нужно:

• разработать национальное законодательство в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей открытых мировых сетей;

• установить перечень информации, не подлежащей передаче по открытым сетям, и обеспечить систему действенных мер контроля за соблюдением установленного статуса информации;

• активно участвовать в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей.

Создание корректной, полной системы обеспечит сохранение национальных информационных ресурсов России и ее равноправное вхождение в мировое информационное сообщество.

Базовыми для такой системы могут стать федеральные законы, регламентирующие вопросы:

формирование информационных ресурсов Российской Федерации;

перемещение информационных ресурсов и информационных технологий через таможенную границу Российской Федерации;

ответственность за неправомерное использование информационных ресурсов, составляющих национальное достояние или ущемляющих конституционные права граждан Российской Федерации.

В развитие этих законов подзаконными правовыми актами еще только предстоит определить:

порядок проведения официальной регистрации, экспертизы, сертификации и оценки информационных ресурсов, созданных технологическим путем;

права и обязанности субъектов, ответственных за сбор, обработку и предоставление государственных информационных ресурсов;

порядок регламентации доступа к государственным информационным ресурсам;

перечень информационных ресурсов, предоставляемых бесплатно или за плату, не компенсирующую расходы;

создание нормативно-правовой базы для развития системы страхования информационных рисков, направленных на гарантированное обеспечение страховой защиты имущественных интересов хозяйственных субъектов различных форм собственности в виде полного или частичного возмещения ущерба, организацию системы обязательного страхования информационных систем федеральных органов государственной власти, органов исполнительной власти субъектов Российской Федерации и организаций кредитно-финансовой сферы.

Экономический аспект. Он не менее важен, чем социальный и юридический, и в неменьшей степени касается современного специалиста, профессиональная деятельность которого неизбежно протекает в информационном пространстве. Экономические проблемы информационной безопасности можно условно разбить на два подмножества: информационные аспекты безопасности экономики и собственно экономика защиты информации.

Общепризнанно, что современная эффективная рыночная экономика немыслима вне достоверной и надежной информационной среды.

В основе теории экономического равновесия лежит постулат о том, что необходимым условием оптимизации поведения любой фирмы и вообще экономической структуры на рынке и обеспечения максимума прироста общественного продукта, является точное знание, во-первых, своих производственных возможностей, во-вторых, всех условий, которые существуют на рынке, и, в-третьих, всех норм государственного регулирования экономической деятельности.

Если таковых знаний нет, то поведение экономических агентов отклоняется от оптимального и может наносить даже вред экономике общества. Также очевидно, что чем выше информационная обеспеченность деятельности участников социально-экономических отношений, тем выше конкурентоспособность национальной экономики, социальная и политическая стабильность.

Сегодня многие предприятия не имеют возможности получить достоверную информацию о той среде, в которой они работают, тех возможностях, которыми они располагают, о конкурентах и своих конкурентных преимуществах. Во многом поэтому они не в состоянии выдерживать конкуренцию и вынуждены сдавать свои рыночные позиции.

Нынешнее состояние информационного обеспечения хозяйственных отношений неудовлетворительно по целому ряду причин.

Необходимо констатировать, что в информационном пространстве крутится огромное количество недостоверной информации, которая циркулирует сегодня даже по официальным государственным информационным каналам. Достаточно вспомнить те же финансовые пирамиды, когда при помощи средств массовой информации, принадлежащих государству, тиражировалась заведомо ложная, недостоверная информация.

Современная информационная среда характеризуется чрезвычайной неопределенностью. До недавнего времени невозможно было предсказать даже на 3—4 месяца вперед какие будут цены, какая будет ставка процента; на полгода вперед невозможно было точно предсказать, какая будет налоговая система. Столь высокая неопределенность экономической среды ведет к тому, что и экономические субъекты не могут планировать свою хозяйственную деятельность более чем на полгода, на год вперед. Значит, не могут развиваться те секторы экономики, которые требуют долгосрочного планирования.

В экономической среде просто отсутствуют целые сегменты крайне важной для нормального экономического поведения информации. Это касается, прежде всего, информации о распределении прав собственности. Крайне сложно, а иногда и просто не-

возможно получить информацию о том, кто же является собственником тех или иных предприятий, какие права и возможности у этих предприятий и их владельцев.

Серьезную проблему представляет неадекватность информационных показателей, которыми сегодня оперируют участники социально-экономических отношений. Мы очень много сегодня говорим о банкротствах предприятий как необходимом условии оздоровления общества и микроэкономической среды. Но совершенно очевидно, что в условиях информационного хаоса точных и простых критериев признания или не признания того или иного предприятия банкротом просто не существует. И в условиях, когда по формальным показателям неплатежеспособности примерно половина предприятий производственной сферы сегодня могут быть объявлены банкротами, оперирование крайне простыми и примитивными показателями прибыльности, рентабельности не могут дать достоверную оценку состоянию того или иного предприятия.

Это досадное перечисление информационной незащищенности хозяйствующих субъектов можно продолжить. Такая государственная политика в области информационного обеспечения экономической деятельности в системах государственного управления ведет к весьма негативному явлению приватизации информации. Многие информационные потоки, которые должны быть общественным благом и общедоступными, искусственно закрываются и используются в частных интересах.

Другой экономический аспект защиты информации — собственно экономика безопасной информационной деятельности — тоже никак не представлен в нашем образовательном процессе. Даже дипломники, которые решают задачи из области защиты информации или радиоэлектронной борьбы (или из области конфликтных взаимодействий в информационном пространстве), экономические разделы проектов и работ выполняют по типовым заданиям на расчет некой экономической эффективности разработки. Хотя эффективность того, что мешает работать, требует дополнительного и более корректного определения.

Экономика защиты информации требует пристального внимания. И многие аспекты этой проблемы еще не разработаны. Действительно, если рассматривать некий изолированный хозяйствующий субъект (фирму, предприятие и т.п.), можно утверждать, что отсутствие у него адекватной защиты информации (ноу-хау, интеллектуальной собственности) неизбежно приведет к экономическим потерям. Но гипертрофированные меры защиты потребуют такого расхода ресурсов (временных, трудовых, финансовых), при котором упадет эффективность основной хозяйственной деятельности. Значит, между этими крайними условиями где-то должен быть оптимум расходов на обеспечение защиты инфор-

мации. Но методы нахождения этого оптимума пока не известны. В частности, еще и потому, что совершенно не разработана конструктивная теория ценности информации. Отдельные этюды к этой теории, созданные в свое время Р.Л.Стратоновичем, А.А.Харкевичем, В.И.Сифоровым, их последователями и другими учеными, не дают практического методического аппарата измерения семантической ценности информации.

Финансовый аспект. Финансовая составляющая информационной безопасности вплотную примыкает к экономической, но не тождественна ей. Известны истории с чеченскими авизовками, которые нанесли урон финансовой системе страны, соизмеримый с бюджетами регионов. Причина этих коллизий состоит, прежде всего, в довольно тривиальном отсутствии протоколов обеспечения аутентификации информации в финансовых потоках. Сейчас эти задачи решены, разработаны и законодательно внедрены методы использования электронной подписи. Но проблемы здесь еще остаются. Известны факты компьютерных атак на финансовую информацию (хотя банки довольно тщательно скрывают эти факты, как вредящие их коммерческому имиджу). И это далеко не все проблемы, грозящие финансовой сфере, не защищенной со стороны возможной информационной агрессии. Преступные посягательства в финансово-кредитной и банковской сферах за последние годы стали разнообразнее и изощреннее.

Ущерб от различных видов преступных посягательств, связанных с нарушением информационной безопасности в автоматизированных платежных системах, может быть не меньше чем при прямом хищении денег и ценностей. Актуальность этой проблемы возрастает по мере расширения внедрения новых автоматизированных платежных систем. При охвате автоматизированной платежной системой всех регионов страны любая дестабилизация в ее функционировании может нарушить безопасность финансово-платежной системы страны и, как следствие, проявится в сбое всего хозяйственного механизма государства.

Актуальной проблемой организации банковской безопасности является практическое воплощения стратегии и тактики обеспечения информационной безопасности в сфере технологии кредитно-финансовой и банковской деятельности. В этой стержневой проблеме есть целый комплекс вопросов. Одним из важнейших направлений работ по обеспечению информационной безопасности в банковской системе является создание системы защищенных телекоммуникаций, базирующейся на системе спутниковой связи, наземной коммутируемой сети телефонной связи, выделенных каналах передачи данных.

Политический аспект. Анализ его, с точки зрения проблемы информационной безопасности, дает возможность констатировать все большее смещение центра тяжести от силовых факторов к более

скрытым и тонким, базирующимся на информационном воздействии.

Несмотря на прекращение холодной войны ведущие страны мира продолжают модернизировать свои разведывательные службы, совершенствуют техническую разведку, наращивают ее возможности. Внимание к России как объекту разведки усилилось. При этом главными приоритетами иностранных разведок являются процессы становления России как самостоятельного государства в структуре мирового сообщества, ее внутренние и внешние политические ориентиры, военная политика и пути ее практической реализации, происходящие экономические преобразования, направленность научных исследований и технических экспериментов, оценка российского рынка во всех его составляющих. Значительно расширились и облегчились условия ведения разведки на территории России. Фактически договор ОСВ-2, наложив ограничения на развитие и совершенствования средств вооружений, снял ограничения на ведение разведки. Более того, одна из статей этого договора прямо гласит, что «контроль за выполнением соглашений возлагается на национальные средства контроля» (следует читать — «средства разведки»). Россия присоединилась к международному Договору по открытому небу. На очереди Договор по открытому морю. Эти договоры имеют целью контроль за военной деятельностью, но технические средства, используемые в соответствии с этими договорами, конечно, имеют более широкие возможности.

Разведывательная деятельность иностранных государств в настоящее время отличается большим разнообразием используемых сил и средств. Многофункциональные разведывательные космические системы, наземные центры радиотехнической и радиолокационной разведки, стратегические самолеты-разведчики, морские системы и комплексы технической разведки действуют в настоящее время против России непрерывно. При этом расходы на разведывательную деятельность иностранных государств не сокращаются (например, в США они составляют ежегодно около 30 млрд долларов). В сферу интересов технических разведок попадают даже союзники. Достаточно вспомнить обеспокоенность европейских партнеров и союзников США тем, сколь активно внедряется в их политическую, экономическую и, возможно, частную жизнь пресловутая американская система «Эшелон», использующая глобальную сеть космической радио- и компьютерной разведки.

Военный аспект. Информационная безопасность в военном деле — это довольно традиционная область. Военные структуры всегда защищались от средств разведки всеми способами: пассивными и активными.

По мнению отечественных и зарубежных специалистов, боевые действия в современных (и будущих) войнах прежде всего

ведутся не для разгрома сухопутных войсковых группировок противника. Они имеют целью дезорганизацию политического, экономического и военного управления соответствующими структурами противоборствующей стороны. О том, что изменились цель и характер боевых действий, свидетельствует опыт локальных войн последнего времени (после Вьетнама). Сейчас наступает новый этап. Наметилась тенденция перехода от оружия массового уничтожения к высокоточному «информационному оружию». Это не пустые слова. Так, в США создан центр по реализации концепции «Информационная война». Новый орган будет разрабатывать положения по организации и ведению борьбы в новой сфере военного противоборства, решать задачи по подготовке специалистов в данной области, а также определять приоритеты в НИОКР и закупках предназначенных для этих целей вооружений и аппаратуры.

Информационное оружие может существенно изменить характер будущих войн. Иногда утверждается, что будущие войны могут превратиться по существу в «компьютерные войны» с массовым применением компьютеризированных роботов, роботизированного оружия и военной техники. Предполагается, что основу боевой экипировки солдата в будущем образует боевой компьютер. Кроме анализа окружающей обстановки компьютер за счет соответствующего программного обеспечения и сенсоров будет осуществлять медицинский контроль за состоянием солдата и выдавать лечебные рекомендации.

В свою очередь, элементом воздействия на силы и средства противника в будущей войне может стать компьютерное оружие. Оно может быть реализовано, в частности, в виде деструктивных программ, которые могут изменять или уничтожать программы компьютеров, управляющих оружием, военной техникой и войсками.

Опыт военных действий последних лет (на Ближнем Востоке, в Югославии, Ираке) показал, что резко возросшие технические возможности средств разведки сделали неэффективными многие традиционные методы и средства защиты информации. Например, данные космических средств разведки оперативно использовались непосредственно на поле боя, для управления высокоточным оружием, даже для борьбы с иракскими оперативно-тактическими ракетами СКАД. Это значит, что такие традиционные методы скрытия информации о дислокации ракетных комплексов, как пространственное маневрирование в позиционном районе, уже неэффективны.

Возросшие оперативные возможности технических разведок и использование их данных позволило отнести радиоэлектронную борьбу уже не к средствам боевого обеспечения, а к этапу боевых действий. Соответственно возросла роль защиты информации.

Сегодня одним из наиболее существенных объектов безопасности в оборонной сфере являются информационные ресурсы и

информационная структура оборонного потенциала страны (вооруженных сил и военно-промышленного комплекса). Важно, что все современные средства вооружения, военной техники, системы управления войсками и оружием являются системами критических приложений с высоким уровнем компьютеризации. Эти системы могут оказаться весьма уязвимыми с точки зрения воздействия информационного оружия как в военное, так и в мирное время. Последнее может привести к тому, что к угрожаемому периоду оружие сдерживания страны окажется полностью или частично заблокированным за счет скрытого внедрения в программное обеспечение систем управления им программных закладок. О реальности такой ситуации свидетельствует опыт локальных войн последних лет.

Экологический аспект. Проблема экологической безопасности является сегодня одной из важнейших в глобальном масштабе. Она связана с защитой интересов личности, общества и государства от потенциальных и реальных угроз, создаваемых последствиями антропогенного воздействия на среду, а также от природных стихийных бедствий и катастроф.

Экологическая проблема является весьма сложной, многоплановой, комплексной. Она неразрывно связана с экономикой, техникой, правом, военным делом и другими сферами общественной деятельности. Но существенно важны и информационные аспекты проблемы экологической безопасности. Три причины определяют наличие корреляции между экологической и информационной безопасностью:

ощущается недостаточная информированность широких слоев населения об угрозах экологической безопасности, источниках этой угрозы, последствиях экологических бедствий и катастроф т.д. Наиболее характерным примером этого является Чернобыльская катастрофа;

решение большинства экологических проблем и задач связано со сбором и обработкой информации о состоянии окружающей среды (с экологическим мониторингом), моделированием и изучением моделей масштабных глобальных процессов природных явлений. Надежность и безопасность информации в этой сфере экологической деятельности трудно переоценить;

целый ряд систем управления (транспортом, связью, атомной энергетикой, опасными производствами) относится к «критическим». Очевидно, что недооценка вопросов информационной безопасности этих систем может привести к непредсказуемым экологическим последствиям, огромным материальным потерям и человеческим жертвам.

Естественно-научный аспект. Здесь проблемы информационной безопасности легче всего иллюстрировать на примере того, как информационная сфера впитывает и использует новейшие дости-

жения прикладных и фундаментальных научных дисциплин. Так, для реализации информационной агрессии, несанкционированного доступа к охраняемым сведениям и данным могут использоваться все без изъятия физические поля: во всех полях могут существовать процессы переноса вещества и энергии, используемые для передачи и извлечения информации. Не составляют исключения и такие экзотические для использования в приложениях к информационной сфере физические поля, как гравитационное, сейсмическое. Естественно, что использование всех известных и мыслимых физических полей в информационном конфликте предполагает реализацию диалектического баланса мер и контрмер. Необходимо защищать информацию, которая может переноситься сигналами во всех физических полях.

Немаловажно использование достижений информатики и математики в интересах обеспечения информационной безопасности.

Технический аспект. Технический аспект защиты информации тоже приходится рассматривать по-разному. Во-первых, это защита информации, циркулирующей в технических системах, точнее, в организационно-технических, поскольку именно технические средства информационного обмена составляют основное по сложности, стоимости и, возможно, по уязвимости наполнение большинства организационных структур. Во-вторых, это защита информации, основанная на использовании специальных технических средств.

Область технической защиты информации сейчас наиболее продвинута. Уже можно говорить о заложенных основах теории технической защиты информации, т.е. о том, что данная предметная область в своем развитии доросла до некоторых теоретических обобщений, понимания предельных (потенциально достижимых) уровней информационной безопасности и формулировок решаемых задач оптимизации стратегии обеспечения безопасности информации.

Работу всех технических систем сопровождает появление технических каналов утечки информации, т.е. каналов несанкционированного доступа (НСД) к информации (утечка — это очень специфический термин, пришедший из предметной области организационных средств и методов защиты информации, но он все прочнее укореняется и в области информационной безопасности). При этом технические каналы утечки информации могут порождаться вовсе и не информационными системами. Например, спектр излучения факела ракетного двигателя (совсем не информационная система) способен сообщить информацию о том, какой это двигатель (ЖРД или ТРД), о компонентах ракетного топлива, степени отработки, жизненном цикле изделия и совместно с другими разведывательными признаками технической политике в области развития вооружений.