ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

В. Г. ГРИБУНИН, В. В. ЧУДОВСКИЙ

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Рекомендовано
Учебно-методическим объединением
вузов Российской Федерации по образованию
в области историко-архивоведения в качестве
учебного пособия для студентов высших учебных заведений,
обучающихся по специальностям «Организация и технология
защиты информации», «Комплексная защита объектов
информатизации» направления подготовки
«Информационная безопасность»

ACADEMIA

Москва
Издательский центр «Академия»
2009

УДК 621.38(075.8)
ББК 32.81я73
Г827

Рецензенты:
канд. техн. наук *В. Б. Кравченко* (директор Института информационных наук и технологий безопасности Российского государственного гуманитарного университета);
канд. техн. наук *М. В. Мецатунян* (зав. кафедрой методологии защиты информации Российского государственного гуманитарного университета)

Грибунин В. Г.
Г827 Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.
ISBN 978-5-7695-5448-3

В учебном пособии раскрыты научные, методологические и законодательные основы организации комплексной системы защиты информации на предприятии, а также основные аспекты практической деятельности по ее созданию, обеспечению функционирования и контроля эффективности.

Для студентов высших учебных заведений. Может быть использовано в практической работе сотрудниками предприятий и организаций независимо от их организационно-правовой формы и ведомственной принадлежности.

УДК 621.38(075.8)
ББК 32.81я73

ISBN 978-5-7695-5448-3

ПРЕДИСЛОВИЕ

Принятие решений во всех сферах жизнедеятельности предприятия или организации все в большей степени базируется на информационных процессах. Анализ этих процессов с последующей выработкой управляющих решений осуществляется на основе информационных моделей, построенных на современных информационно-телекоммуникационных технологиях. Поэтому защита информации представляет собой самостоятельную составляющую безопасности предприятия в целом, значение которой с каждым годом растет.

Информационный ресурс становится одним из главных источников экономической эффективности предприятия. Фактически наблюдается тенденция, когда все сферы жизнедеятельности предприятия становятся зависимыми от информационного развития, в процессе которого они сами порождают информацию и сами же ее потребляют.

На современном этапе развития основными угрозами безопасности предприятия являются угрозы в сфере информационного обеспечения. Последствиями успешного проведения информационных атак могут стать компрометация или искажение конфиденциальной информации, навязывание ложной информации, нарушение установленного регламента сбора, обработки и передачи информации, отказы и сбои в работе технических систем, вызванные преднамеренными и непреднамеренными действиями как со стороны конкурентов, так и со стороны преступных сообществ, организаций и групп. К одной из наиболее важных задач в области безопасности предприятия следует отнести создание комплексной системы защиты информации (КСЗИ). Различным аспектам этой проблемы посвящено данное учебное пособие.

ВВЕДЕНИЕ

Необходимость защиты информации осознавалась с глубокой древности. Недаром до нас дошли сведения о применявшихся в прошлом методах защиты — технических (например, шифр Цезаря, различные виды стеганографии) и организационных (зачастую они сводились к физическому устранению людей — носителей сведений, когда необходимость в них миновала).

Шло время, совершенствовались не только методы защиты, но и методы нападения. В Советском Союзе обеспечению безопасности информации уделялось большое внимание. Но решать эти вопросы, когда «все вокруг народное, все вокруг ничье», было сравнительно несложно. Иное дело — современная экономическая обстановка, когда в ожесточенной конкурентной схватке борется множество больших и малых организаций. В борьбе, как известно, все средства хороши, а тем более эффективные. К таким, без сомнения, можно причислить нападение на информацию конкурента с целью завладеть ею, исказить, сделать недоступной и т.д. Поэтому вопросы защиты информации в современном обществе имеют первостепенное значение.

Особенно облегчается задача злоумышленника в связи с повсеместным внедрением автоматизированной обработки информации. Степень автоматизации фирмы определяет зачастую ее конкурентоспособность и в то же время является источником многочисленных угроз безопасности. Неслучайно в сознании многих людей защита информации — это прежде всего защита информации в компьютерных системах от несанкционированного доступа. Конечно, эта точка зрения неверна точно так же, как неверна и точка зрения другой полярности: все определяется организационно-режимными мерами.

Надежное обеспечение безопасности информации немыслимо без реализации комплексного подхода к решению этой задачи. Отсюда и потребность как в создании комплексной системы защиты информации на предприятии, так и в подготовке специалистов по данному профилю. Поэтому и была разработана программа специальностей 075300, 075400, которая включила и дисциплину «Комплексная система защиты информации на предприятии».

Построение глав учебного пособия соответствует плану этой дисциплины. В *первой главе* рассмотрены основные понятия и

определения изучаемой дисциплины, ее задачи и функции, во *второй главе* — принципы организации и этапы разработки комплексной системы защиты информации (КСЗИ), ее взаимосвязь с другими системами предприятия. С учетом того что КСЗИ является сложной системой, здесь же приведены основные положения теории сложных систем. На построение КСЗИ предприятия влияют множество факторов, которые подробно рассмотрены в *третьей главе*.

Прежде чем защищать что-либо, нужно ответить на вопросы: «Что защищать?», «От кого защищать?», «В соответствии с какими требованиями строить защиту?». Для ответа на последний вопрос необходимо четко представлять себе классификацию информации по видам тайн, нормативно-правовые аспекты ее защиты, методику определения состава защищаемой информации. Все это входит в содержание *четвертой главы* книги. В *пятой главе* приведены подлежащие защите объекты, которые являются носителями информации, либо на которых защищаемая информация обрабатывается, объясняется необходимость защиты тех или иных объектов. Факторы и угрозы безопасности информации, а также модели нарушителей рассмотрены в *шестой главе*.

Защиту информации техническими средствами можно разделить на два больших направления: защита от утечки информации по техническим каналам и защита от несанкционированного доступа к информации в автоматизированных системах. Технические каналы утечки информации, а также меры по их нейтрализации рассмотрены в *седьмой главе*. *Восьмая глава* посвящена защите информации (ЗИ) от несанкционированного доступа (НСД) к ней в автоматизированных системах (АС).

В *девятой главе* приведен общий подход к субоптимальному выбору компонентов системы. В качестве иллюстрации данного подхода решается задача выбора компонентов подсистемы КСЗИ, связанной с защитой информации от НСД в АС, но аналогичным образом можно решать и другие задачи по определению компонентов КСЗИ. На этот выбор большое влияние оказывают условия функционирования КСЗИ, рассмотренные в *десятой главе*. Изучение ведется на основе концепции безопасности информации в автоматизированной системе предприятия, разработанной в одной из фирм. *Одиннадцатая глава* посвящена моделям КСЗИ. Особое внимание уделяется формальным моделям безопасности. На практическом примере показан принцип формализации требований безопасности и условий функционирования системы. Построенная формальная модель используется в девятой главе при обосновании выбора средств защиты информации.

В *двенадцатой главе* рассмотрены технологические и организационные аспекты построения КСЗИ. Приведены стадии создания КСЗИ, основное содержание технического задания на ее по-

строение. В *тринадцатой главе* затронут важнейший аспект обеспечения безопасности информации — кадровый, а в *четырнадцатой главе* — вопросы материально-технического обеспечения КСЗИ.

Эффективность КСЗИ во многом определяется эффективностью управления системой. В *пятнадцатой главе* подробно рассмотрены вопросы, связанные с организацией управления КСЗИ, а в *шестнадцатой главе* — не менее важные аспекты планирования функционирования КСЗИ. Обратная связь в контурах управления основана на результатах контроля. Связанные с этим вопросы освещены в *семнадцатой главе*. *Восемнадцатая глава* посвящена вопросам управления КСЗИ в чрезвычайных ситуациях. Наконец, в *девятнадцатой* и *двадцатой главах* подробно рассматриваются различные подходы к сложной и неоднозначной проблеме оценки эффективности КСЗИ.

Глава 1

Сущность и задачи комплексной защиты информации

1.1. Понятийный аппарат в области обеспечения безопасности информации

Изучение любой дисциплины необходимо начинать с освоения понятийного аппарата ее предметной области. Раскрытие значений некоторых ключевых терминов позволяет сформировать начальные представления о целях и задачах защиты информации. Терминология в области защиты информации изложена в федеральных законах, указах Президента, постановлениях Правительства, государственных и отраслевых стандартах, руководящих документах ФСТЭК России.

Прежде всего определимся с объектом защиты. Согласно [22], под информацией понимается:

1) сообщение, осведомление о положении дел, сведения о чем-либо, передаваемые людьми;

2) [в теории вероятности] уменьшаемая, снимаемая неопределенность в результате получения сообщений;

3) [с точки зрения математических подходов] сообщение, неразрывно связанное с управлением, сигналы в единстве синтаксических, семантических и прагматических характеристик;

4) передача, отражение разнообразия в любых объектах и процессах (неживой и живой природы).

Трудно переоценить роль информации в современном мире. По мнению многих ученых, именно информация является решающим фактором в конкурентной борьбе государств. Так, на Западе пользуется популярностью классификация, в соответствии с которой все страны делятся по уровню их развития следующим образом [1]:

- страны, способные производить и продавать информационные услуги;
- страны, не производящие информационных услуг на продажу, но создающие и продающие промышленные товары;
- страны, не производящие ни информационных услуг, ни товаров и являющиеся поставщиками сырья и рабочей силы в страны первых двух классов.

Важность информации как локомотива развития отчетлива видна на примере Индии. Да и в США более 50 % национального дохода обеспечивает продажа информационных услуг. Владение информацией необходимого качества в нужное время и в нужном месте является залогом успеха в любом виде хозяйственной деятельности. Монопольное обладание определенной информацией оказывается зачастую решающим преимуществом в конкурентной борьбе, именно поэтому собственнику необходимо ее защищать.

Выделяются два вида собственной информации у предпринимателя [42]: техническая (технологическая) и деловая информация. К первому типу относятся, например, методы производства продукции, программное обеспечение, рецепты лекарств и т. п. Ко второму типу относятся, например, бизнес-планы предприятия, списки клиентов, материалы различных заказных исследований.

Уточним, что понимается под *безопасностью информации*. Определение понятия «безопасность» наиболее полно выражено в Федеральном законе от 5 марта 1992 г. «О безопасности». В трактовке закона безопасность — это «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Понятие защищенности указывает на способность (степень, уровень) противостояния конкретным, четко сформулированным угрозам.

В прикладном аспекте, на более низком уровне, чем государство и общество в целом, безопасность определяется как состояние защищенности жизненно важных интересов человека, общества, государства и субъекта защиты в определенной сфере отношений при соблюдении баланса интересов между ними.

Анализ отечественных и зарубежных источников показывает, что в основном все определения понятия безопасности включают следующие основные положения: наличие внутренних и внешних угроз, наличие жизненно важных интересов и соблюдение баланса интересов. Первичным в определениях безопасности является наличие угроз и опасностей, наличие жизненно важных интересов вторично.

Под безопасностью информации понимается такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права, а также утечки за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники [30].

Защита информации подразумевает совокупность мероприятий, направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также доступности ин-

формации для пользователей [13]. Более того, далее мы увидим, что защита информации — это целенаправленный, непрерывно продолжающийся процесс.

Приведем определения конечных целей защиты информации.

Конфиденциальность — свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам [16].

Целостность — свойство, при выполнении которого информация сохраняет заранее определенные вид и качество. Целостность можно подразделить на *статическую* (понимаемую как неизменность информационных объектов) и *динамическую* (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Статическую целостность можно разделить на понятия целостности данных и целостности информации. *Целостность данных* — способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа. *Целостность информации* — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) [3].

Доступность — такое состояние информации, когда она находится в виде и месте, необходимом пользователю, и в то время, когда она ему необходима [16].

Защита информации осуществляется на объекте, которым может быть как все предприятие, так и некоторая его часть. Объект информатизации — это (1) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или (2) помещения и объекты, предназначенные для ведения конфиденциальных переговоров [14].

Большое значение имеет понятие контролируемой зоны. *Контролируемая зона* — это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей контролируемой зоны могут являться: периметр охраняемой территории предприятия (учреждения); ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения. В отдельных случаях на период обработки техническими средствами секретной информации (проведения закрытого мероприятия) контролируемая зона временно может устанавливаться большей, чем охраняемая территория предприятия. При этом должны приниматься организационно-режимные и техни-

ческие меры, исключающие или существенно затрудняющие возможность перехвата информации в этой зоне [15].

Главным критерием в выборе средств защиты информации следует считать ее *ценность* (реальную или потенциальную). Иногда легко определить ценность информации в денежном выражении. Так, утечка копии снятого фильма приведет к его распространению на пиратских дисках, следовательно, в кинотеатрах не досчитаются зрителей, а фирма-производитель недополучит прибыль. В других случаях стоимость информации определить сложно. Например, сколько стоит информация о кодах блокировки ядерных ракет? Поэтому для определения ценности информации в таких случаях вводят систему грифов секретности информации, предусматривая для различных грифов различные меры обеспечения безопасности. Ценность информации позволяет установить возможный ущерб от овладения информацией конкурентами или ее искажения.

Для обеспечения эффективной защиты информации кроме оценки ценности необходимо провести анализ ее уязвимости. *Уязвимость* — это некая слабость, которая дает возможность выявить характерные особенности и недостатки объекта защиты, облегчающие проникновение злоумышленника к охраняемым сведениям. Главный результат анализа уязвимостей — выявление источников информации и возможных каналов ее утечки или других нежелательных воздействий на нее. Эти воздействия (атаки) являются реализацией угроз безопасности, которые носят потенциальный характер.

При построении и эксплуатации систем безопасности большое значение имеют методы оценки *риска*, под которым обычно понимается произведение вероятности реализации угрозы и наступившего в результате ущерба.

1.2. Цели, задачи и принципы построения КСЗИ

К настоящему времени в ведущих странах мира сложилась достаточно четко очерченная система концептуальных взглядов на проблемы обеспечения информационной безопасности. Тем не менее, как свидетельствует реальность, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Понимая это, большинство руководителей предприятий и организаций принимают меры по защите важной для них информации.

Для решения задач защиты информации на предприятии создается *комплексная система защиты информации* (КСЗИ).

Имеются работы, в которых термин КСЗИ понимается в «узком» смысле, т.е. как система защиты информации от несанкционированного доступа в автоматизированных системах (АС). В настоящей книге принято «широкое» понимание КСЗИ как системы обеспечения безопасности предприятия в целом. Вместе с тем защита информации в АС является важнейшей составной частью КСЗИ, поскольку подавляющая часть информационных ресурсов присутствует в электронном виде. Поэтому в некоторых главах книги речь идет именно об обеспечении безопасности информации в автоматизированных системах. КСЗИ предприятия есть совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации предприятия [42].

Главной целью КСЗИ является обеспечение непрерывности бизнеса, устойчивого функционирования коммерческого предприятия и предотвращения угроз его безопасности.

КСЗИ направлена:

- на защиту законных интересов организации от противоправных посягательств;
- охрану жизни и здоровья персонала;
- недопущение: 1) хищения финансовых и материально-технических средств; 2) уничтожения имущества и ценностей; разглашения, утечки и несанкционированного доступа к служебной информации; 4) нарушения работы технических средств обеспечения производственной деятельности, включая информационные технологии.

Исходя из целей КСЗИ, можно определить стоящие перед ней задачи. К ним относятся:

- прогнозирование, своевременное выявление и устранение угроз безопасности персоналу и ресурсам коммерческого предприятия, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов — к различным уровням уязвимости (опасности), подлежащих сохранению;
- создание механизма и условий оперативного реагирования на угрозы безопасности проявления негативных тенденций в функционировании предприятия;
- эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями

физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности предприятия.

Обеспечение безопасности предприятия должно основываться на следующих *основных принципах*: системности; комплексности; своевременности; непрерывности защиты; разумной достаточности; гибкости; специализации; взаимодействия и координации — должно осуществляться планирование; совершенствования; централизации и управления (процесс управления всегда централизован); активности; экономической эффективности; простоты применяемых защитных мер и средств.

Раскроем некоторые принципы построения КСЗИ подробнее.

Принцип системности требует применения системного подхода в качестве методологической базы при анализе и синтезе комплексной системы защиты информации. Основная цель системного подхода — формализация вербальных описаний и составление алгоритма деятельности. Суть его заключается в том, что при оценке эффективности мероприятий безопасности не ограничиваются рассмотрением только самой системы, но и учитывают влияния на нее внешних факторов. Применение системного подхода при разработке технологий управления безопасностью позволяет реализовать синергетический эффект, являющийся результатом упорядочения организационных структур управления, взаимодействия, кооперации и интеграции с другими подсистемами анализируемой системы, устранения ненужных процедур, а в итоге — результатом достижения равновесного состояния функционирования системы.

Системный подход к построению КСЗИ предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности предприятия.

При создании системы защиты необходимо учитывать все слабые, наиболее уязвимые места предприятия, а также характер, возможные объекты и направления атак на КСЗИ со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Принцип комплексности предполагает, что система защиты предприятия должна включать *совокупность* объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности персонала, материальных и финансовых средств от возможных угроз всеми доступными законными средствами, методами и мероприятиями. Принцип ком-

плексности позволяет оценить в целом главные вопросы защиты: что защищается, кто защищает и как защищается? В распоряжении специалистов по безопасности имеется широкий спектр мер, методов и средств защиты. Комплексность системы защиты информации достигается охватом всех возможных угроз и согласованием между собой разнородных методов и средств, обеспечивающих защиту всех элементов предприятия.

Защита должна строиться эшелонированно. Внешняя защита обеспечивается физическими средствами, организационными мерами и правовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, образует внутренний рубеж обороны. Так, одной из наиболее укрепленных линий обороны должны быть средства защиты в автоматизированных системах.

Принцип своевременности означает, что меры защиты не должны «запаздывать». Например, бесполезно выводить охранную сигнализацию на пульт дежурного, который сможет прибыть в случае тревоги на объект охраны лишь спустя полчаса.

Принцип непрерывности: в настоящее время общепринятым является процессный подход к обеспечению безопасности информации. Защита информации — это не совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла систем предприятия, начиная с самых ранних стадий проектирования, а не только на этапе их эксплуатации.

Во многих зарубежных стандартах зафиксирована циклическая схема процесса обеспечения безопасности информации PDCA (Plan-Do-Check-Act). Кроме того, принцип непрерывности подчеркивает недопустимость перерывов в работе средств защиты, устанавливая повышенные требования к их надежности.

Принцип разумной достаточности учитывает тот факт, что создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть мощности и ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

Часто приходится создавать систему защиты в условиях большой неопределенности, поэтому принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный

уровень защиты. Естественно, что для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда средства защиты необходимо устанавливать на работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости спасает владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

Принцип простоты применения состоит в том, что механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не следует требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм представителей службы безопасности, подготовка пользователей средств вычислительной техники и соблюдение ими всех установленных правил сохранения конфиденциальности, взаимная ответственность персонала и руководства, взаимодействие с государственными правоохранительными органами.

1.3. О понятиях безопасности и защищенности

Изложенные ранее принципы лежат в основе организации и функционирования КСЗИ, но в полной мере не отражают процессы управления экономически эффективной безопасностью коммерческого предприятия.

Обеспечение безопасности информации можно представить как деятельность, направленную на снижение риска, — от ее утраты, разглашения, искажения и т.д. Повышенные требования к снижению степени риска обусловили необходимость обоснования и вскрытия новых принципов в процессе организации экономически эффективного управления коммерческим предприятием, в том числе на основе принципа оптимальности Парето, рассмотренного далее. Данный принцип гарантирует баланс интересов, без которого не может быть достигнуто состояние экономически эффективной защиты коммерческого предприятия.

Обеспечение безопасности информации есть целенаправленная деятельность, а защищенность указывает на уровень подготовленности коммерческого предприятия противостоять любым

попыткам внутренних и внешних угроз нанести ущерб ее законным интересам.

Поскольку безопасность определяется как состояние защищенности, можно говорить о наличии спектра возможных состояний: от опасного до состояния, соответствующего полной безопасности [24]. При опасном состоянии защита объекта находится на таком уровне, когда возможность причинить вред, вызвать несчастье, нанести ущерб не представляет особых затруднений. Близкая к такому состоянию защищенность характерна для этапов создания и становления коммерческих предприятий. В это время руководство предприятия основное внимание уделяет первоначальному накоплению прибыли, обороту финансовых ресурсов. Вопросам же безопасности, как правило, уделяется недостаточное внимание. Низкое состояние защищенности характерно для предприятий и на этапе перехода государства к рыночной экономике. Огромное количество образовавшихся источников поставки сырья, оборудования (товаров), отсутствие устойчивых партнерских отношений между клиентами, желание как можно быстрее перехватить каналы поставок, накопить первоначальный капитал вытеснили вопросы безопасности на второй план.

На другом конце спектра находится состояние защищенности, соответствующее полной безопасности. Теоретически можно утверждать, что такое состояние защищенности соответствует уровню, когда никакие самые изощренные угрозы и опасности не смогут причинить вред объекту защиты. Состояние полной (идеальной) защищенности теоретически может быть достигнуто разработкой и внедрением системы защиты, обеспечивающей своевременное выявление, отражение и ликвидацию любых угроз деятельности предприятия. Создание такой системы защиты будет сопровождаться большими материальными и финансовыми затратами.

На практике ни одно крайнее состояние не встречается в чистом виде. Большинство коммерческих предприятий не могут обеспечить такую защиту, как, например, в Форт Кноксе, где хранятся золотые запасы США и где, как показывает практика, также не всегда может быть достигнуто состояние полной защиты.

Таким образом, понятие безопасности предпринимательской деятельности указывает на конкретную оцененную способность коммерческого предприятия (юридического или физического лица) противостоять определенным угрозам своему развитию и оценивается одним из возможных фиксированных состояний спектра в пределах от опасного состояния до полной безопасности. При этом зона каждого состояния будет зависеть от множества факторов как субъективного, так и объективного характера. Данные факторы будут определяться не только индивидуальными способностя-

ми руководства предприятия, но и состоянием и уровнем экономического развития, как предприятия, так и рыночных отношений в целом.

Состояние защищенности не является постоянным и находится в прямой зависимости от уровня экономического развития, прибыли (дохода), стоимости материальных ценностей коммерческого предприятия. При этом существуют следующие связи объективной действительности:

- увеличение прибыли, материальных ценностей влечет необходимость увеличения состояния защищенности;
- с увеличением прибыли увеличиваются опасности и угрозы;
- увеличение опасностей и угроз вызывает необходимость улучшения качества защиты предприятия;
- с улучшением защищенности предприятия увеличиваются затраты на ее обеспечение;
- увеличение уровня защиты коммерческого предприятия снижает уровень воздействия угроз.

Таким образом, состояние защищенности коммерческого предприятия находится в объективной связи как с уровнем экономического развития, так и с возможностями угроз по нанесению ему материального ущерба. Перечисленные выше связи могут использоваться как отдельные законы их состояния и развития.

1.4. Разумная достаточность и экономическая эффективность

Достаточность защиты конкретного предприятия определяет его руководство, исходя из своего представления и оценки защиты, наличия необходимых ресурсов, перспектив и тому подобных факторов. В этом случае говорят о принимаемых мерах защиты по нейтрализации возможных угроз и опасностей. Считается, что состояние будет достаточным, если предпринимаемые меры защиты будут адекватными характеру и действиям возможных угроз.

Организация защиты коммерческого предприятия представляется процессом, включающим оценки двух противоборствующих враждующих сторон: с одной стороны — это угрозы и опасности, а с другой — силы и средства защиты.

Критерием уровня взаимодействия между силами является состояние защищенности, зависящее от факторов:

- состояние производственной, хозяйственной и финансовой деятельности предприятия;
- уровень обеспеченности системы защиты материальными, техническими, людскими и прочими ресурсами;

• степень подготовленности кадров;

• состояние и уровень развития преступности в регионе и государстве и др.

Кривая *1* на рис. 1.1 характеризует зависимость состояния защищенности от уровня экономического развития предприятия [24]. В соответствии с принципом защищенности кривая *1* направлена вверх: с увеличением уровня экономического развития предприятия защищенность увеличивается. Кривая *2* характеризует зависимость возможностей угроз по нанесению ущерба предприятию от уровня его экономического развития. Закон изменения кривой *2* выбран при условии, что уровень развития возможностей угроз в процессе экономического развития коммерческого предприятия остается неизменным. Особенностью графика на рис. 1.1 является то, что оси S и N положительно направлены в противоположные стороны.

Кривая *3* — результирующая; она отражает разность взаимодействия сил: $d = S - N$ и указывает на степень достаточности защиты коммерческого предприятия. Из рис. 1.1 следует, что в точке равновесия сил (R_a) $S_i = N_j$, а поэтому $d = 0$. Данное состояние для коммерческого предприятия экономически эффективно, так как при этом обеспечивается соответствующая (адекватная) угрозам защита.

На участке [0, R_a] $N > S$, $d < 0$. Заштрихованная область указывает на преобладание возможностей сил угроз над способностями предприятия им противостоять. Данный участок соответствует

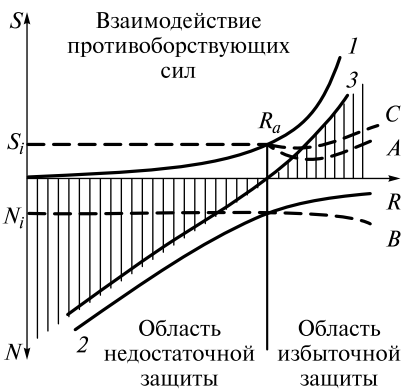

Рис. 1.1. Разумная достаточность защищенности предприятия:

ось S — защищенность; ось N — реализация угроз; ось R — уровень экономического развития предприятия; R_a — состояние, при котором защищенность предприятия S_i такова, что отражает все угрозы N_i; кривая *1* характеризует защищенность предприятия; кривая *2* — возможности по нанесению ущерба; кривая *3* — результирующая кривая