О НЕКОТОРЫХ ПРОТИВОРЕЧИЯХ В РЕШЕНИИ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Р. М. Юсупов[1], В. М. Шишкин[2]

[1,2]Санкт-Петербургский институт информатики и автоматизации РАН

[1,2]СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

[1]<spiiran@iias.spb.su>, [2]<vms@iias.spb.su>

УДК 004.056

Юсупов Р. М, Шишкин В. М. **О некоторых противоречиях в решении проблем информационной безопасности** // Труды СПИИРАН. Вып. 6. — СПб.: Наука, 2008.

Аннотация. *Обращается внимание на противоречивый характер современного этапа развития теории и практики информационной безопасности. Обсуждаются некоторые проявления и аспекты противоречий, в том числе технические, экономические, инфраструктурные и другие. Утверждается, что для решения проблем в данной области необходимо понимание их природы, фундаментальных причин, анализ более общих, в том числе институциональных противоречий и закономерностей, приводящих к видимым негативным проявлениям. Отмечается тенденция к инфраструктурному характеру современных проблем информационной безопасности, необходимость нелинейного подхода к их анализу.* — Библ. 7 назв.

UDC 004.056

Yusupov R. M., Shishkin V. M. **About some contradictions in the decision of information security problems** // SPIIRAS Proceedings. Issue 6. — SPb.: Nauka, 2008.

Abstract. *Attention to inconsistent character of present stage of information security theory and practice development is paid. Some displays and aspects of contradictions, including, technical, economic, infrastructural and others are discussed. Understanding nature of problems in given area, their fundamental reasons and analysis of more general contradictions, including institutional ones and regularities, that lead to visible negative displays, are stated as necessary to solve these problems. Infrastructural character tendency of modern information security problems and necessity of nonlinear approach to their analysis are.* — Bibl. 7 items.

1. Введение

История развития предметной области, которая получила к настоящему времени собирательное наименование информационной безопасности, едва ли не уникальна, и всё более заметным становится противоречивый характер этого развития. За короткое время произошли столь масштабные и беспрецедентные изменения, что узкоспециальные вопросы защиты информации — предмет интереса преимущественно государственных органов и ограниченного количества технических специалистов, математиков — превратились даже не в междисциплинарные, а в глобальные проблемы информационной безопасности. Но интеграционный период уже сменяется новой дифференциацией: безопасность компьютерных технологий или, в американизированной терминологии, кибербезопасность, становясь в свою очередь предметно-многообразной, обособляется от множества нетехнологических проблем. Активно формируется и выходит на первый план претендующий на интегрирующую функцию юридический аспект.

Всё в большей мере вопросы информационной безопасности обращают на себя внимание широкого круга специалистов гуманитарной сферы. Даже технические аспекты во многих случаях становятся актуальными по гуманитарным мотивам (например, активно обсуждаемая, но так и не получившая достаточно удовлетворительного разрешения проблема защиты персональных данных или исследования частотных характеристик телевизионного изображения с

точки зрения влияния на психику и сознание человека). Не случайно, наверное, «Доктрина информационной безопасности РФ» посвящена в первую очередь, прямо или косвенно, гуманитарным аспектам.

При этом работы в области технических аспектов обеспечения информационной безопасности по естественным причинам, как всякая инженерная деятельность, самодостаточны и традиционно ориентированы прежде всего на защиту информационных активов, процессов, коммуникаций. Защиту от чего? Конечно, прежде всего от злоумышленных и стихийных воздействий на них. Но воздействовать непосредственно на человека-оператора или ЛПР, может быть, более эффективно, чем по техническим каналам на собственно информационные системы, не говоря уже об использовании так называемых инсайдеров, техническая защита от которых порождает порочный круг.

Очевидно, что мы имеем дело здесь с частным проявлением более общего, фундаментального и закономерного для современной цивилизации противоречия между человеком и созданной им техносферой. Однако в отличие от давно обозначенных техносферных рисков, угрожающих физическому здоровью, угрозы, имеющие информационную природу, часто воздействуют на сущность человеческой личности — духовную и психологическую сферы, что обостряет указанное противоречие. При этом инфокоммуникационные технологии (ИКТ) в свою очередь усугубляют традиционные техносферные риски, поскольку современные технические и организационные системы уже немыслимы без использования ИКТ. Они же способны в значительной мере уменьшить эти риски, если сами ИКТ будут безопасными. Таким образом, человечество близко подошло к той черте, когда безопасность ИКТ окажется решающим фактором в обеспечении его безопасного существования.

Технологический прогресс существенно обгоняет теоретическое осмысление происходящего в области создания и применения информационных технологий, использования новых коммуникационных возможностей. Но такое положение, когда быстро развивающиеся технологии, имеющие тотальный характер, стимулируемые рыночными критериями, слишком долго остаются теоретически неосознанными, чревато непредсказуемыми последствиями.

Необходимо понять природу противоречий, какие из них являются объективными и закономерными, а какие — результатом неадекватных решений (в том числе принимаемых под действием внешних по отношению к данной проблеме факторов иной природы, экономических и политических, в частности). Понимание природы противоречий, их идентификация, будет способствовать безопасному развитию как самих ИКТ, так и всей техносферы.

2. Динамика соотношения защиты и нападения

Обратимся теперь к прагматике информационной безопасности. «Расширяющаяся пропасть» («Report on Widening Gap») — так в широко цитируемом (например, в [1]) докладе аудиторской компании Ernst&Young эмоционально обозначается тенденция, которая отчётливо проявилась к настоящему времени. Пропасть между угрозами ИТ-безопасности и тем, что делается для защиты от них, становится всё шире. И это несмотря на то что имеются безусловные успехи в разработке методов и средств защиты информации, практически сложились их индустриальное производство и рынок консалтинговых услуг, производители аппаратных и программных средств заявляют о создании безопасных

платформ и сред, всё больше средств расходуется на защиту корпоративных ресурсов. Тем не менее пропасть расширяется.

Впрочем, новые факты лишь подтверждают устойчивость тенденции. Уже достаточно давно было отмечено, что в традиционной «борьбе брони и снаряда» в современных условиях «информационный снаряд» в своем развитии побеждает «информационную броню» [2]. В чем же причина этого явного противоречия? Ответ на такой вопрос, конечно же, не простой и предоставляет широкое поле для дискуссий. Для начала, нужно попытаться выявить основные объективные факторы.

В первую очередь обращает на себя внимание очевидная разномасштабность процессов, происходящих по разные стороны «фронта», существенная разница жизненных циклов средств нападения и защиты (найти проход в заборе всегда проще и быстрее, чем его построить). Соответственно интенсивность деструктивных процессов превосходит интенсивность процессов, им противодействующих. Динамика роста обнаруженных уязвимостей начинает приобретать нелинейный характер, специалисты по ИТ-безопасности не успевают адекватно отреагировать на эволюцию рисков. При этом производители средств защиты информации, подчиняясь законам рыночного производства, заинтересованы в сокращении издержек путем тиражирования или адаптации уже готовых решений и на рынок продвигаются неизбежно отстающие продукты и системы. Проактивность, которая могла бы компенсировать отставание, хотя и декларируется, но чаще остается пока, к сожалению, желаемым свойством средств защиты. На рис. 1 показана динамика выявленных уязвимостей за последние годы [3].

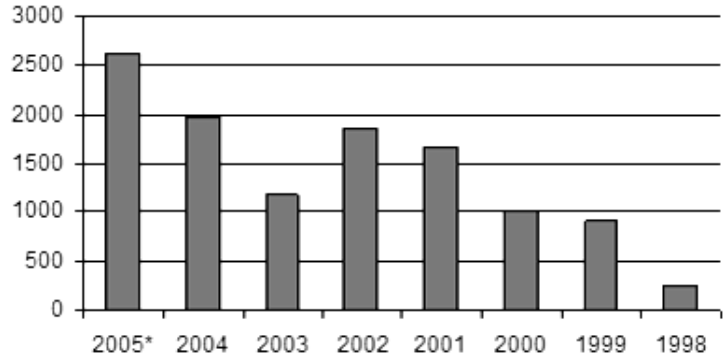

Рис. 1. Динамика роста обнаруженных уязвимостей (2005* — за 7 месяцев).

Насколько же реально защищены информационные системы? На рис. 2 представлены результаты оценки на одной из моделей эксплуатационной безопасности информационных систем [4], иллюстрирующие приведённое выше утверждение о различиях жизненных циклов. Методически модель очень прозрачна (в ней соотносятся интенсивности обнаружения и устранения уязвимостей), но вполне правдоподобна, и поэтому хорошо иллюстрирует качественную оценку уровня защищенности реальных систем, особенно если принять во внимание фактические данные с рис. 1.

На графике показана зависимость вероятности того, что система не имеет уязвимостей, от среднего времени устранения одной уязвимости (недель/ед.) для разных λ — интенсивностей обнаружения уязвимостей (единиц/год). Предполагается вполне адекватный для качественной оценки экспоненциальный закон распределения вероятностей времени в этих процессах. Как видим, только

при очень оптимистических параметрах, далёких от действительности, вероятность того, что в системе нет уязвимостей, превышает 0.5, в реальных же случаях она значительна ниже. И если уязвимостью ещё не воспользовались злоумышленники или не возникла системная коллизия, это не значит, что система защищена от них.

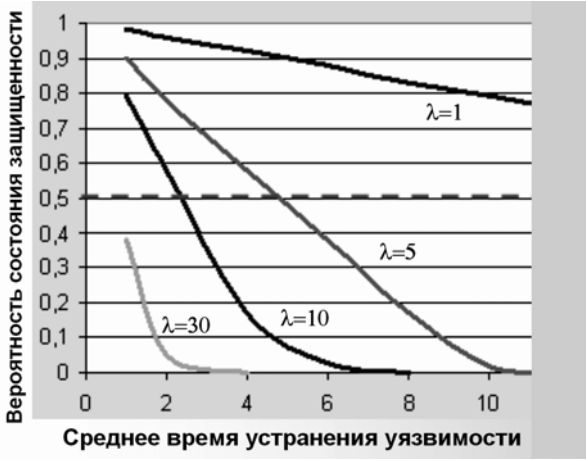

Рис. 2. Оценка эксплуатационной безопасности информационных систем.

Вернемся к аналогии «брони» и «снаряда». На верхней диаграмме рис. 3 их противостояние представлено в виде двух регулярно пересекающихся графиков функций F, понимаемых как некие условные противостоящие «силы», ступенчато возрастающие во времени t. Усреднив их, получим линейную зависимость примерного равновесие между ними в динамическом смысле, в чём, собственно говоря, и проявляется традиционная оппозиция.

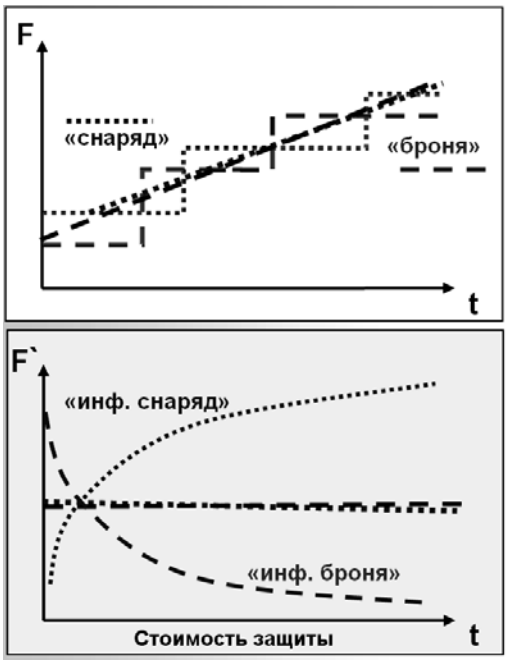

Рис. 3. Модель оппозиции «брони и снаряда», традиционной и информационной.

Иная картина, как показывает практика, наблюдается в противостоянии информационных «брони» и «снаряда». На нижней диаграмме рис. 3 изображены графики тех же функций в относительном измерении — можно считать их

Труды СПИИРАН. 2008. Вып. 6. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 6. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

производными от функции F. Для определенности примем для неё, упрощая, но качественно не искажая ситуацию, пропорциональную зависимость от t в виде $F \approx t^{\beta}$, где значения параметра $\beta > 1$ и $\beta < 1$ соответствуют «информационному снаряду» и «информационной броне», а $\beta \cong 1$ — традиционной оппозиции. Тогда её представят две горизонтальные почти совпадающие линии, а расходящиеся кривые покажут наглядный вид «расширяющейся пропасти» между угрозами ИТ-безопасности и средствами защиты. (Обратим внимание: по оси абсцисс можно измерять пропорционально времени также стоимость защиты, что потребуется для изложения в следующем разделе.)

Справедливости ради, надо отметить, что не во всех классах средств защиты информации «снаряд» побеждает «броню». Криптографические средства демонстрируют, скорее, традиционную динамику, что вполне объясняется тем, что жизненные циклы инструментария обеих сторон сопоставимы и технологически, и во времени. В какой-то мере динамическое равновесие наблюдается и между некоторыми классами вирусных угроз и средств антивирусной защиты, хотя и с отставанием последних по фазе в силу их практической реактивности. Правда, здесь иногда возникает крамольный вопрос: нет ли у производителей антивирусных средств заинтересованности в спросе на их продукцию?

Как же обеспечить динамическое равновесие между «броней» и «снарядом» в информационной сфере? Прежде всего необходимо разделить факторы объективные (технический прогресс, психологические ограничения человека и т.п.) и субъективные, преходящие. Для противодействия последним, думается, более подходящим инструментом является не техническая, а институциональная политика.

Один из объективных, как нам представляется, факторов был указан выше: существенная разница жизненных циклов средств нападения и защиты и, как следствие, преобладающая интенсивность деструктивных процессов. Требуется сбалансировать интенсивность появления новых уязвимостей и угроз и интенсивность их устранения.

Самый простой путь, как это ни парадоксально выглядит по отношению к исходному утверждению, состоит в увеличении эксплуатационной составляющей жизненного цикла продуктов и систем. Тогда количество потенциальных уязвимостей и угроз будет неизбежно асимптотически убывать, и рано или поздно интенсивности процессов сравняются. Возможен ли такой ход развития в принципе, ведь он фактически означает замедление технического прогресса? Тем более такой вариант сомнителен в условиях господства экономики рыночного типа, когда без ускоренного обновления продукции (т.е. создания новых уязвимостей), сокращения производственных издержек, в том числе на реинжиниринг (сохранение прежних уязвимостей), экономический успех проблематичен. Впрочем, в некоторых специальных, внеэкономических приложениях и этот, «консервативный», путь может быть приемлемым.

Ещё один путь возникает исходя из старого лозунга: нападение лучший способ обороны. В самом деле, если интегрировать средства защиты и нападения, не уравняется ли в едином технологическом комплексе масштаб процессов противоборствующих сторон? Наверное, это реально, но всё же такой путь будет находиться в русле существующей технологической парадигмы развития ИКТ, которая сформировалась задолго до того, как проявились современные проблемы защиты информации, и сводящейся к «навешиванию» на незащищенное функциональное ядро системы аппаратно-программных средств защиты. Но, как и в первом случае, не являясь универсальным, такой подход

Труды СПИИРАН. 2008. Вып. 6. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 6. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

тем не менее может оказаться полезным, и, кроме того, в его рамках могут возникнуть новые методы и технологии противоборства.

И всё же, видимо, радикальный путь состоит в переходе на принципиально новые платформы и протоколы, для которых «броня» станет имманентной составляющей. Конечно же, уязвимости найдутся всегда, хотя бы из-за неизбежных ошибок в ПО или присутствия «инсайдеров», но уровень противоборства перейдет на качественно иной технологический и профессиональный уровень, не доступный для дилетантов, подобно тому как это происходит в относительно благополучной области криптозащиты и криптоанализа.

3. Экономика и информационная безопасность

Тема эта обширна и многопланова, серьёзная её разработка только начинается, и мы остановимся здесь лишь на отдельных ее аспектах, в которых проявляется противоречивость проблем информационной безопасности.

Сразу же отметим, что редукция оценки информационной безопасности объектов экономики исключительно к экономическим категориям, а такой соблазн имеет место, вообще говоря, неправомерна, хотя и может быть приемлемой при внутрикорпоративном анализе. В самом деле, ущерб от успешной атаки на информационную систему банковской или иной бизнес-структуры, не говоря уже о системах управления экологически опасных производств, может выйти далеко за рамки финансовых или деловых интересов этих объектов, произвести инфраструктурный эффект. Кстати, в этом обстоятельстве также видится своего рода противоречивость: отсутствие четкой грани между корыстными, террористическими или иными, например политическими, целями атак на информационные системы.

Основной же парадокс порождает сам факт формирования индустрии средств обеспечения информационной безопасности. Дело не только в том, что, как было отмечено выше, производители, исходя из объективных требований рыночной эффективности, тиражируют отстающие от динамики угроз продукты. Важнее другое: подчиняясь опять-таки рыночным критериям, отрасль нуждается в постоянно расширяющемся спросе на свою продукцию, а это значит, что «расширяющаяся пропасть» лишь способствует её экономическому процветанию. Впрочем, этот парадокс не оригинален. Яркая аналогия — фармацевтический бизнес, который болезненно прореагирует на улучшение здоровья потенциальных потребителей. Спрос может и будет успешно формироваться независимо от объективных условий. Вспоминается очень эффективно проведенная маркетинговая кампания по так называемой «проблеме-2000», а также некоторые исследования по статистике и экспертной оценке информационных угроз, порою похожие на плохо скрытые рекламные акции определенных производителей определенных продуктов или компрометацию конкурентов.

Наиболее заметные случаи нарушения информационной безопасности имеют корыстные, т.е. экономические мотивы. И если бы не отмеченные выше инфраструктурные проявления, то можно было бы и не драматизировать нынешнюю ситуацию, рассматривая её как переходный процесс, — бесконечно «пропасть» расширяться не будет. Даже при сохранении тенденции она должна стабилизироваться, как обычно приходят к динамическому равновесию популяции «хищников» и «жертв», «паразитов» и «хозяев» в хорошо известных моделях экологической динамики [5]. Тогда, может быть, нужно смириться с неизбежными потерями от нарушений безопасности информационных активов и

ставить задачу оценки приемлемого уровня ущерба? То есть издержки от нарушений безопасности должны будут планироваться, учитываться и оптимизироваться наряду с другими видами издержек.

Результаты исследований свидетельствуют, что «российские компании с неохотой вкладывают средства в информационную безопасность» [3] (рис. 4*)*.

Рис. 4. Распределение расходов на защиту информации в российских компаниях.

Так может быть, с учетом вышесказанного, они, действуя интуитивно или будучи ограничены в ресурсах, правы? Что же касается межкорпоративной конкурентной борьбы в информационной сфере, то, хотя в основе её лежат экономические мотивы, технологически и организационно она едва ли существенно отличается, например, от межгосударственного информационного противоборства.

Обратимся ещё к одной неоднозначной проблеме экономики информационной безопасности — оценке экономической эффективности затрат на защиту информации, ставшей за последние годы весьма актуальной. Действительно, затраты растут, но «пропасть» расширяется, и такое положение не может не беспокоить руководителей бизнеса.

В настоящее время не выработано единого понимания этой проблемы, имеют место различные подходы к ее решению, преимущественно ориентированные на внутрикорпоративное понимание политики безопасности, поскольку методические рекомендации универсального характера в чистом виде не дают удовлетворительного решения. Полезно вспомнить, что на заре компьютеризации управления производством складывалась аналогичная ситуация, когда подходы и методики, в целом оправдавшие себя до этого в других отраслях, давали порой абсурдные результаты для новой отрасли — автоматизированной обработки данных. Тем не менее экономическое мышление, несмотря на существование интересных и перспективных исследований, в целом остаётся пока в традиционном русле.

Обратимся к рис. 5. На верхней диаграмме приведена интерпретированная для нашего случая идеальная, но вполне приемлемая и практически работающая модель, позволяющая оптимизировать соотношение качества и цены в самых разнообразных применениях. В ней соотносятся две противоположно направленные функции стоимости (защиты и ущерба от её нарушения) и, естественно, определяется оптимальный по критерию минимума полной стоимости уровень защищенности.

Труды СПИИРАН. 2008. Вып. 6. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 6. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

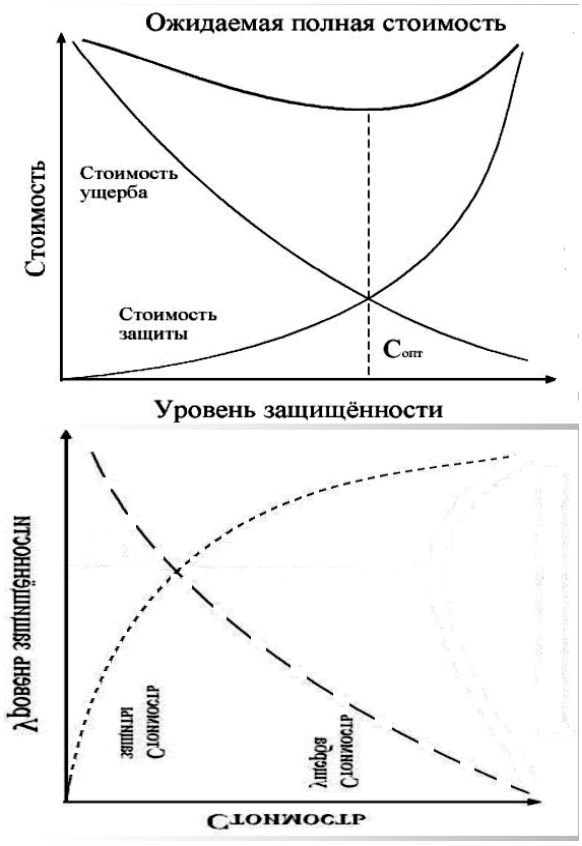

Рис. 5. Идеальная модель оценки оптимальной защиты.

На нижней диаграмме рис. 5 изображены те же зависимости, но с поворотом координатной плоскости, что хорошо видно по сохраненным для наглядности надписям в зеркальном виде. А теперь вернёмся назад и сопоставим полученные графики с нижней диаграммой на рис. 3, иллюстрирующей «расширяющуюся пропасть». Как видим, на рис. 5 «пропасть» тоже расширяется, но с точностью до наоборот по сравнению с реальностью: кривая ущерба, которая должна быть пропорциональна относительной «силе информационного снаряда» падает в отличие от кривой на рис. 3, а уровень защищённости, т.е. относительная «сила брони», наоборот растёт.

Это еще одно противоречие — теории и практики. При оценке экономической эффективности систем обеспечения информационной безопасности исходят из правильной в общетехническом смысле посылки (качество имеет прямую зависимость от затрат на него), но исходя из ложного в данном случае утверждения, что уровень защищенности (тоже качество в определенном смысле) должен возрастать по мере роста стоимости системы защиты. Не хотелось бы компрометировать конструктивные работы в данной области, но надо признать, что к настоящему моменту ещё не сложились общепринятые и вполне адекватные реальному положению вещей подходы к оценке экономической эффективности систем защиты информации.

Еще один болезненный аспект, также относящийся к экономике информационной безопасности, но не только. Речь пойдет об оценке и соответственно управлении информационными рисками, без чего никакой экономический анализ в сфере информационной безопасности невозможен. И вполне закономерно, что уже заявило о себе новое направление в страховой деятельности —

Труды СПИИРАН. 2008. Вып. 6. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 6. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

страхование информационных рисков. Впрочем, его предметность довольно зыбка, поскольку дискуссионным остаётся вопрос не только, как их оценивать, но и что оценивать, так как единого понимания смысла этого термина, к сожалению, пока нет.

Тенденция в развитии инфокоммуникационных систем направлена на структурное усложнение, динамику и распределённость ресурсов. Они всё более выполняют интегрирующие, инфраструктурные функции в обеспечении основных видов жизнедеятельности людей, поэтому обратим внимание на особенности анализа рисков именно в сложных информационных системах. В том числе можно ещё особо выделить критически важные информационные объекты, распределенные системы инфраструктурного назначения, в которых адекватная оценка рисков, идентификация критических состояний имеют значение, далеко выходящее за пределы самих объектов. О них можно говорить ещё как о неравновесных системах или системах с сильной положительной обратной связью, а системы с подобными свойствами склонны к нелинейному поведению. Не случайно работы в области моделей нелинейной динамики привлекают всё большее внимание исследователей в приложении к сложным объектам различной природы — на то есть достаточно оснований и теоретического, и фактологического характера. И в частности, в них отмечается особая роль степенных функций как в уравнениях динамики, так и в распределении вероятностей характеристик таких систем.

В то же время прикладные модели анализа и управления рисками явно или неявно линейные, а экспертные системы используют зачастую псевдовероятностные оценки, предполагающие, опять-таки явным или неявным образом «хороший» нормальный или экспоненциальный закон распределения. В оправдание надо сказать, что существующие экспертные системы в большинстве своём являются товарными продуктами, поэтому развиваются они, подчиняясь в основном конъюнктурному спросу, по экстенсивному пути, что не стимулирует методическое совершенствование, обновление парадигмы.

Итак, можно утверждать, что усложнение информационных систем, увеличение значимости активов приводят к нелинейному росту потенциального ущерба. Покажем на несложном примере модель этого механизма, более подробно представленного в [6].

На рис. 6, во-первых, показано соотношение между экспоненциальным и степенным законами распределения; их близость при достаточно большом значении параметра степенного распределения нарастает по мере его увеличения. Функции плотности распределения вероятностей и интегральную для экспоненциального и степенного законов запишем соответственно как $f_{\exp}(x) = \lambda e^{-\lambda(x-1)}$ и $f_p(x) = \alpha x^{-(\alpha+1)}$; $F_{\exp}(x) = 1 - e^{-\lambda(x-1)}$ и $F_p(x) = 1 - x^{-\alpha}$. Распределения сопоставлены по равенству математического ожидания. Это не наилучшее, хотя и близкое к нему, как показано в [6], приближение, но визуально графики функций (тонкие линии) практически совпадают уже при умеренном значении параметра степенного распределения, $\alpha = 9$, и соответствующего параметра экспоненциального распределения $\lambda = 8$. Поэтому выбор закона распределения даже при несколько меньших параметрах мало существенен.

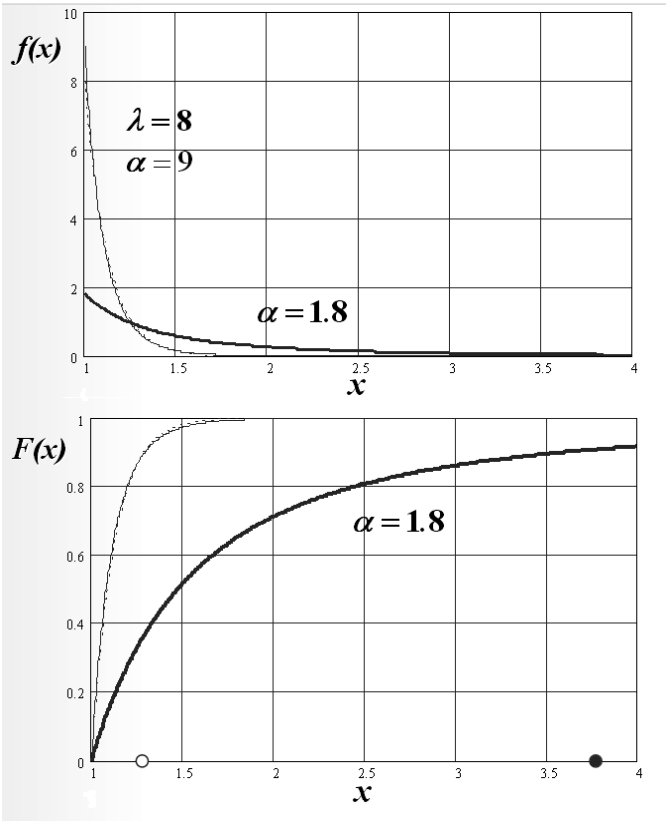

Рис. 6. Функции распределения вероятностей меры риска.

Действительно, экспоненциальный закон во многих случаях удовлетворительно описывает распределение временных характеристик, и это не только эмпирический факт. Но технически идентичный отказ в обслуживании информационной системы или время её восстановления, например, локального банка, местной администрации, опасного производства, транспортного узла и т.д., приведет к совершенно разному, порой несопоставимому ущербу, то есть цена времени будет в каждом случае разная. Экспоненциальный закон становится во всех отношениях неудовлетворительным, шкала меры риска (x) должна быть преобразована, причем нелинейно, и естественно в качестве нелинейности использовать также степенную функцию.

Для приведения шкалы к равномерному виду остаётся пересчитать параметр α. Тогда, несложные расчеты показывают, и это хорошо заметно на диаграммах (жирные линии), что при возрастании значимости активов (будем оценивать её математическим ожиданием) в 2 раза, параметр $\alpha = 1.8$, медиана распределения меры риска увеличивается в 5.4 раза, а 0.9-квантиль — почти на порядок, более чем в 9 раз (на нижней диаграмме соответствующие квантили отмечены светлой и тёмной точками). Но при $\alpha \le 2$ дисперсия $D_p(x) \to \infty$ и система может квалифицироваться уже как катастрофоопасная. Это наглядный пример того, насколько чувствительной оказывается мера риска, если не упрощать её до линейности.

4. Некоторые актуальные факты

Факты, отмеченные ниже, известны и очевидны, однако заметного движения по пути разрешения этих противоречий не наблюдается.

Труды СПИИРАН. 2008. Вып. 6. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 6. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Противоречивы методы и средства системной защиты. Возник совершенно определённый методический и технологический разрыв между механизмами и программно-техническими средствами защиты, функционирующими в реальном масштабе времени в режиме мониторинга, с одной стороны, и возможностями и инструментами комплексной оценки ИБ, её «медленной» составляющей (аудит, экспертиза безопасности), — с другой. Тоже своего рода «расширяющаяся пропасть». В первом случае разрабатываются все более тонкие средства, хотя и реализующие преимущественно «реактивный» подход — защиту от того, что уже случилось; во втором — чаще всего эвристические модели, экспертное оценивание, ориентация на конъюнктурные требования вводимых нормативов, использование которых на практике остаётся проблематичным. Между этими направлениями, в той или иной мере, но необходима интеграция.

Противоречиво техническое нормотворчество. Несколько всем известных примеров. ФЗ «О техническом регулировании» предполагал принятие технических регламентов — регламенты практически отсутствуют, а прежние нормативы в целом устарели и не обязательны к применению. ГОСТ Р ИСО/МЭК 15408-2002 «Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» — требования новых стандартов становятся, и это закономерно, все менее детализированными, в то же время разработка регламентов, руководящих документов для их применения наталкивается на серьезные трудности, калькированный перевод с английского разрушает привычный понятийный аппарат, известны удивительные ошибки перевода.

Понятийный аппарат и терминология семантически размываются и американизируются, теряется однозначность и устоявшиеся понятия, возникают логические неполнота и противоречия. Корпоративный подход к обеспечению информационной безопасности, который к тому же особо подвержен иноязычному влиянию, еще больше способствует размыванию понятий в этой сфере. В результате вместо некоторой междисциплинарной смысловой противоречивости и неоднозначности в недавнем прошлом возникло новое явление: многие понятия, легко и повсеместно теперь употребляемые, виртуализируются, едва ли не теряя смысл. Следование в русле чужого понятийного аппарата, каким бы универсальным и интернациональным он не казался, по сути, есть акт разоружения в информационном противоборстве.

Противоречива ситуация с подготовкой кадров: специальностей много, а специалистов не хватает. Структура специальностей, содержание образования не могут сформироваться, сохраняется дублирование, при нехватке специалистов многие выпускники идут работать в другие области ИКТ.

Перечислим для конкретности специальности группы 090100 «Информационная безопасность» [7]:

- Криптография (090101);
- Компьютерная безопасность (090102);
- Организация и технология защиты информации (090103);
- Комплексная защита объектов информатизации (090104);
- Комплексное обеспечение информационной безопасности АС (090105);
- Информационная безопасность телекоммуникационных систем (090106);
- Противодействие техническим средствам разведки (090107).

Если первая и последняя позиции в этом списке, очевидно самодостаточны и самостоятельны, выделение специальности 090106 также, наверное, оправданно в силу специфики коммуникационных процессов, то остальные явным образом, больше или меньше, но существенно пересекаются. Не будем здесь предлагать и обсуждать альтернативы, но согласиться со сложившейся сейчас номенклатурой специальностей трудно.

В то же время не заметно успехов в просвещении гуманитариев — сужать понятие «информационная безопасность» до технической проблематики в образовании в настоящее время уже недопустимо. Любому современному человеку, особенно будущим педагогам, крайне необходимы знания хотя бы в области информационно-психологической защиты от агрессивных и деструктивных воздействий на его сознание. Знание основных технических вопросов безопасности в условиях сплошной компьютеризации и «интернетизации» также не будет вредным, а оно сейчас у гуманитариев, как показывает опыт, не простирается далее элементарной осведомленности о компьютерных вирусах и «спаме» и, может быть, еще каких-нибудь туманных сведений об ЭЦП.

Отдельный вопрос — подготовка и воспитание специалистов в области информационного права. Хотя среди юристов существует мнение, что достаточно переформулировать или свести вопросы, связанные с информационно-правовыми отношениями, к терминам и процедурам традиционного материального права и проблемы не будет, в общем случае такое вряд ли возможно без ущерба для существа дела — информация это «материя» особая и попытка редукции проблемы здесь неправомерна. Поэтому специалисты нужны, но задача их подготовки оказалась непростой из-за своей противоречивости: будущим ИТ-инженерам просто не хватает времени для получения достаточного, чтобы считаться квалифицированным правоведом, юридического базиса, а студенты-юристы, видимо по складу ума, не воспринимают необходимый инженерный минимум.

5. Заключение

Последний частный пример вернул нас к тому глубокому и закономерному противоречию, к которому пришли мы в начале изложения: к неразрывности и одновременно противостоянию техносферы и человека. Претендовать на решение столь глобальных проблем в короткой статье было бы, конечно, самонадеянно, но уход от них, предпочтение им лишь злободневных конъюнктурных задач представляется малоперспективным — практика ИБ тому подтверждение.

Хотелось бы обратить ещё раз внимание на то, что многочисленные лежащие на поверхности явлений проблемы, которые, как мы все видим, появляются быстрее, чем находят свое разрешение, имеют фундаментальные причины. Без их понимания и осознания «информационный снаряд» по-прежнему будет преобладать над «информационной бронёй», а «пропасть» между ними останется столь же широкой.

Литература

1. *Антиномов Д.* IT-безопасность: никто не готов к новым угрозам. [Электронный ресурс] / Д. Антиномов; CNews / ООО «МЕДИАЛЕНД.РУ» М., 1995–2008. 15 с. 01.02.2006 // <http://www.cnews.ru/reviews/index.shtml?2006/02/01/195291>

(по состоянию на 05.02.2008).
2. *Юсупов Р. М., Заболотский В. П.,* Научно-методические основы информатизации. СПб.: Наука, 2000. 455 с.
3. *Щеглов А. Ю.* Вопросы защиты информации. Без комментариев. [Электронный ресурс] / А. Ю. Щеглов; ЗАО «НПП «Информационные технологии в бизнесе». СПб., 2001-2007. 5 с. 06.12.2006 // <http://articles.security-bridge.com/articles/15/11864> (по состоянию на 05.02.2008).
4. *Щеглов А. Ю.* Оценка эксплуатационной безопасности системных средств. Анализ защищённости современных универсальных ОС. [Электронный ресурс] / А. Ю. Щеглов; ЗАО «НПП «Информационные технологии в бизнесе». СПб., 2001-2007. 8 с. 13.11.2006 // <http://articles.security-bridge.com/articles/15/11841> (по состоянию на 05.02.2008).
5. *Вольтерра В.* Математическая теория борьбы за существование. М.: Наука, 1976. 285 с.
6. *Шишкин В. М.* Степенное распределение и управление рисками критических систем // Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук: Т.31. М.: КомКнига, 2007. С. 39–59.
7. Общероссийский классификатор специальностей по образованию. ОК 009-2003. Издание официальное. / Минобразования России. Госстандарт России. М.: ИПК Издательство стандартов, 2003. [Электронный ресурс] // <http://www.ed.gov.ru/prof-edu/sred/rub/okso.doc> (по состоянию на 05.02.2008).