Степенное распределение и управление рисками критических систем

В. М. Шишкин

1. О критичности и риске — вместо введения

Прежде, чем перейти к изложению основного содержания статьи, хотелось бы остановиться на ключевых словах, содержащихся в её названии — критичности и риске, смысл которых в настоящее время оказался несколько размытым.

Сфера информационной безопасности в последние годы стала ареной активного словотворчества, не всегда оправданного, поскольку введение новых терминов и понятий совсем не обязательно приводит к уточнению сущности представляемых объектов и явлений. Происходит это на фоне настойчивого внедрения калькированной англоязычной терминологии, основанной на иной лингвистической и понятийной традиции. В узко технических применениях опасность заметного искажения существа обозначаемых объектов при этом вряд ли будет иметь место, но в более широком контексте информационной безопасности это не так. Принимая во внимание междисциплинарный и даже публичный характер современных её представлений, и помня старую истину: «правильно назвать — значит, правильно понять», следует признать опасность неадекватного, а возможно и злонамеренного словоупотребления, навязывания ложных смыслов в столь ответственной сфере деятельности.

Мы исходим из того, что оправданием для введения новых терминов или их интерпретаций является обозначение принципиально новых явлений или объектов. И, хотя информационную безопасность, как предметную область, можно отнести к новейшим направлениям теории и практической деятельности, тем не менее, нет оснований полагать, что понятийная основа ее должна выходить за пределы достаточно богатой научно-технической традиции.

Характерный пример семантической нечеткости как раз и представляет рассматриваемая группа однокоренных терминов, а именно: «критический», «критичный», «критичность», сравнение употребления которых в разных текстах исключает однозначное понимание. Одной из причин этого, видимо, является «некритическое» отношение к англоязычным терминам «critical» и «criticality», которые далеко не всегда допускают буквальный перевод.

В то же время в физике, равно как и в математике, понятие критичности используются давно, и смысл производных терминов вполне прозрачен, несмотря на разнообразие применений (критическая масса, критический объем, критическая температура, критическая точка, критическое значение, критические явления и многое другое). Сравнивая такого рода определения, использующие термин «критический», не трудно обнаружить в них семантический инвариант, указывающий на возможность при малых изменениях некоторых, опять таки критических, параметров к качественному изменению объекта.

При ясном понимании, что стоит за понятием «критический» в традиционных научных дисциплинах, уже не может вызывать сомнений производное понятие «критичность», как обозначение или характеристика критического, в указанном смысле, состояния того или иного объекта. Именно такое понимание рассматриваемых терминов в иных предметных областях, включая информационную безопасность, кибербезопасность следует признать правомерным.

Критический элемент или критическая система в теории надёжности, отказ которых приводит к отказу системы, в состав которых они входят, т. е. происходит её переход в иное качество, также понятны и не противоречат физическим или математическим интерпретациям. Но «критически важный элемент критической инфраструктуры» звучит уже несколько странно и избыточно (примеров подобного рода можно привести немало, поэтому, не имея намерения вступать с ними в полемику, ссылки на источники делать не будем).

Разные подсистемы или системы играют при функционировании объекта далеко не одинаковую роль, отказы различных компонентов могут приводить к разным последствиям, и переходов от одного состояния к другому может быть не один, а больше. Поэтому возникает проблема ранжирования уровня критичности, а значит и определения ее меры. Однако и в таком контексте рассматриваемое понятие не выходит за традиционные представления, поскольку остается неизменной его суть — возможность изменения состояния. Но когда критичность, качественное понятие, называют, например, мерой важности, присваиваемой некоторому объекту, возникает явная логическая ошибка — с таким же успехом важность можно назвать мерой критичности.

Критичность нередко связывают с неустойчивостью, как в математическом, так и в широком смысле этого слова, с чем также можно согласиться, поскольку потеря устойчивости предполагает качественный переход. И достаточно общее определение критического состояния, как «состояния крайней неустойчивости, достигаемого открытой неравновесной системой в ходе предшествующего периода эволюционного развития»; и даже громоздкое определение критических систем, как «сложных компьютеризированных технических/оргтехнических систем, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, разрушению системы финансового обращения, дезорганизации систем энергетического и коммуникационно-транспортного обеспечения государства, глобальным экономическим и техногенным катастрофам, утрате обороноспособности государства», в целом не вызывают возражений.

Аналогичная ситуация по разным причинам сложилась с термином «риск», смысл которого до сих пор в технических приложениях однозначно не определился, а за их пределами имеет узко специфический, как например, в страховой деятельности, интуитивный или вовсе бытовой характер. Пример исчерпывающего сущностного анализа этого термина, основанного на выделении семантического инварианта, можно найти в [1]. В результате соответствующее понятие приводится к бесспорным категориям «неопределенности», «возможности», оценочности суждения о неблагоприятном исходе или развитии процесса, что позволяет, не теряя общности, корректно использовать его в разнообразных приложениях. При этом, учитывая, что в указанном понимании риск является качественной характеристикой, возникает свобода выбора и преобразования его меры, без необходимости исключительно вероятностной её интерпретации или, тем более, эквиваленции риска и вероятности, что часто, и не всегда обоснованно, делается.

В отличие от широкого контекста информационной безопасности, где в силу её междисциплинарности трудно рассчитывать на унификацию понятий, употребление рассмотренных терминов в системе представлений кибербезопасности может быть упорядочено и ограничено в смысловом отношении, что исключит некорректность и произвол в их использовании.

И пусть они остаются семантически не вполне чёткими, важно отделить сущность от меры, чтобы за терминами стояло нечто объективное, а значит — измеримое, т. е. их мера.

Для дальнейшего изложения определим риск, киберриск, в том числе, как возможность нанесения ущерба объекту, киберсистеме, а в качестве его меры примем некоторое множество величин, способных характеризовать, хотя бы арифметически, потенциальный ущерб, понимаемый в произвольном смысле. В таком случае можно говорить и о распределении вероятностей этой меры риска.

Что касается критичности, то с учётом вышеизложенного, будем её рассматривать, как состояние объекта около перехода в новое качество, представляющее риск для объекта. Тогда определение меры критичности сводится к задаче параметризации критических состояний, решение которой, конечно, не однозначно, так как выбор параметров, их содержательная интерпретация в значительной степени зависит от конкретных обстоятельств. Возможный подход к параметризации будет показан в разделе 3.

2. Почему степенное распределение

Тенденция в развитии киберсистем направлена на их структурное и функциональное усложнение, распределённость ресурсов. Поведение сетевых структур, состоящих из очень большого числа компонентов, определяется огромным числом взаимодействий, при этом обратные связи и недетерменированное поведение некоторых компонентов системы приводит к возникновению нелинейных эффектов.

В самом деле: сообщения на транспортном уровне управляются с использованием обратной связи в зависимости от качества передачи; размер серии пакетов зависит от динамически настраиваемых параметров TCP; эти параметры в свою очередь зависят от случайных задержек, вариация которых возникают из-за прохождения пакетов через буфер маршрутизатора и в результате изменения маршрутов передачи; процессы, возникающие при виртуальном соединении, имеют разные временные масштабы; отказ одних компонентов может порождать отказ других, переходя в лавинообразные отказы. Феноменология этих явлений достаточно хорошо известна.

В то же время киберсистемы становятся всё более человеко-машинными, но уже не в традиционном смысле этого слова, предполагающем участие в процессе функционирования профессионального человекаоператора, возмущающие возможности которого ограничены и прогнозируемы. Человек из средства поддержки процесса во многих случаях становится целью функционирования, и проявления человеческого фактора поэтому всё более разнообразятся. Операторами выступают и рядовые потребители информационных услуг, но также и квалифицированные злоумышленники, инициирующие или использующие естественные возмущения в системе. Специфическую функциональную категорию возмущающих систему факторов представляют и так называемые «инсайдеры».

О системах такого рода можно говорить как о неравновесных, системах с сильной положительной обратной связью. В их функционировании обнаруживаются свойства нелинейной динамики и, соответственно, склонность при некоторых условиях к катастрофическому поведению. Последнее обстоятельство важно в нашем случае, так как имеет непосредственное отношение к критическим состояниям.

Уже достаточно давно была показана необходимость использования моделей нелинейной динамики в анализе сложных систем [2], выдвигались аргументы в пользу нелинейного мышления по всему спектру научных изысканий, широкого применения нелинейной методологии, признавалась высокая эвристическая значимость моделей и понятий, разработанных в ней [3]. Идеи, высказанные в работах разных авторов, активно развивались в дальнейшем [4], и к настоящему времени накопилась обширная литература по данной тематике. Немалое внимание при этом уделялось и проблеме управления рисками, поскольку нелинейная парадигма существенно изменяла традиционные представления в этой области [5, 6].

Однако надо признать, что убедительные и даже красивые выводы, содержащиеся в этих и других работах, носят, скорее, глобальный во всех отношениях характер. Впрочем, скептиками это отмечалось и раньше: признавая достоинства нелинейного подхода, высказывались сомнения в его практичности. Так, например, довольно старую идею о полезности для наблюдения и исследования феноменов нелинейности «линейных очков» напомнил в 1997 г. известный физик П. Грассберг на первой конференции Немецкого общества сложных систем и нелинейной динамики (Deutsche Geseltschaft fuer Komplexe Systeme und Nichtlineare Dynamik) [7]. Тем не менее, выскажем убеждение, что потенциальная практичность методов нелинейной динамики для изучения поведения усложняющихся киберсистем высока. Может быть, прежде всего, она состоит в том, что стимулирует поиски конструктивных применений фундаментальных закономерностей, присущих сложным динамическим структурам. Мотивом для проведения данного исследования как раз и послужило намерение обнаружить факты, позволяющие на уровне методов и механизмов, применить представления теории нелинейных динамических систем в анализе критичности и управлении киберрисками.

Принципиальную значимость в моделях нелинейной динамики имеют степенные функции. Это достаточно убедительно было показано в работах ряда авторов, причём, что важно, исходя из разных позиций. Они представлялись и как статистические образы катастрофического поведения [8]; и как свойственные системам развивающегося типа [9]; и присущие системам с положительной обратной связью на основе анализа кинетических уравнений больцмановского типа — «в системах, где нет степенного распределения, нет и обратной связи» [10]. Статистические исследования самых разнообразных явлений на эмпирическом уровне давно обнаруживали такую же зависимость (законы Парето, Лотки, Ципфа и др.). Есть и более общие исследования, не получившие, правда, заметного развития, так называемых устойчивых законов, которые во многих случаях лучше приспособлены для описания эмпирических закономерностей [11]. Нельзя сказать, что внимание к степенным функциям связано исключительно с новыми исследованиями нелинейных динамических систем или с эмпирическими закономерностями, они восходят ещё к К. Вейерштрассу [9].

В итоге надо признать, что для рассматриваемого класса систем имеются основания считать степенные функции наиболее адекватными как для описания динамических свойств, так и в функциях распределения вероятностей меры риска.

Обычно экспоненциальные и степенные функции, в том числе и распределения вероятностей, противопоставляются, справедливо подчёркиваются их существенные различия. Тем не менее, в определённом диапазоне параметров они сближаются и, если не асимптотически, то можно сказать, «плавно» переходят друг в друга.

Рассмотрим функции, плотность и интегральную, экспоненциального и степенного распределения вероятностей без потери общности, соответственно, в виде (1) и (2):

$$f_{\exp}(x) = \lambda e^{-\lambda(x-1)},\ F_{\exp}(x) = 1 - e^{-\lambda(x-1)},\ x \geq 1, \lambda > 0; \tag{1}$$

$$f_p(x) = \alpha x^{-(\alpha+1)}, \quad F_p(x) = 1 - x^{-\alpha}, \quad x \geq 1,\ \alpha > 0. \tag{2}$$

Сопоставим их, сначала визуально, для больших значений параметра α, во всяком случае, достаточно удалённых от 1.. Для удобства сравнивать будем распределения с равными математическими ожиданиями. Это не наилучшее, но, как будет показано ниже, близкое к нему, причём мажорирующее, приближение. Тогда между параметрами распределений в виде (1) и (2), матожидания которых,

$$m_{\exp}(\lambda)=\frac{\lambda+1}{\lambda},\ m_{\mathrm{p}}(\alpha)=\frac{\alpha}{\alpha-1},\ \alpha>1, \tag{3}$$

устанавливается простое соотношение:

$$\alpha=\lambda+1. \tag{4}$$

На рисунке 1 для сравнения представлены две пары графиков функций плотности для экспоненциального (сплошные линии) и степенного (штриховые) распределений в равномерной (левая диаграмма) и двойной логарифмической шкалах (правая).

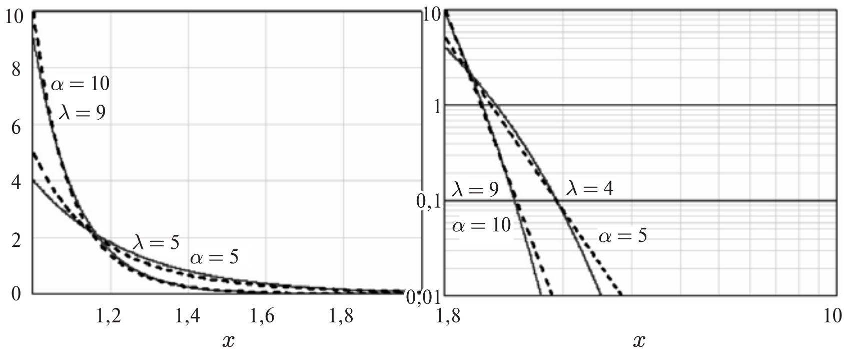

Рис. 1. Сравнительный вид экспоненциального и степенного законов распределения

Как видим, в каждой паре кривые на диаграммах мало различимы, и, по мере роста параметров, в равномерной шкале практически совпадают. Справедливости ради, надо отметить, что в логарифмической шкале при выборе подходящего масштаба отличия станут всё же заметны, особенно на хвостах, поскольку для степенного распределения траектория будет линейной.

Более точно определим приближение (2) к (1) (или наоборот) в среднеквадратическом смысле, минимизируя критерий (5).

$$s(\lambda,\alpha)=\sqrt{\int\limits_1^\infty(\lambda e^{-\lambda(x-1)}-\alpha x^{-(\alpha+1)})^2\,dx}\;. \tag{5}$$

Эта зависимость непрерывна на всём множестве допустимых значений параметров, и, как можно показать, имеет единственный минимум, для определённости пусть это будет $s_{\min}(\lambda)$, для любого фиксированного λ, который в общем виде находится как решение уравнения:

$$\frac{d}{d\alpha}s(\lambda,\alpha)=0\;. \tag{6}$$

Интегрирование выражений (5) и (6) приводит к бесконечным суммам, поэтому в удобном для анализа виде зависимости s от параметров и параметров друг от друга выразить не представляется возможным. Тем не менее, для каждого λ находится такое единственное значение $\alpha^o>1$, что $s(\lambda,\alpha^o)=s_{\min}(\lambda)$, при котором приближение (2) к (1) в смысле (5) будет наилучшим. При этом $\lim\limits_{\lambda\to\infty}s_{\min}(\lambda)=0$, а упрощённое приближение с соотношением параметров (4), т. е. $\alpha^*=\lambda+1$, монотонно стремится сверху к наилучшему. Однако, хотя и $\lim\limits_{\lambda\to\infty}s(\lambda,\alpha^*)=0$, но относительная разница между ними, $\delta_s(\lambda)=[s(\lambda,\alpha^*)-s_{\min}(\lambda)]/s_{\min}(\lambda)$, никогда не становится нулевой, и можно предположить, что $\lim\limits_{\lambda\to\infty}[s(\lambda,\alpha^*)-s_{\min}(\lambda)]=s_{\min}(\lambda)$, во всяком случае, численно $\lim\limits_{\lambda\to\infty}\delta_s(\lambda)\approx 1$. Похожее явление наблюдается и для параметров, между которыми всегда соблюдается отношение $\alpha^*>\alpha^o>\lambda$, но их относительные разницы $\delta_\lambda=(\alpha^o-\lambda)/\lambda$ и $\delta_\alpha=(\alpha^*-\alpha^o)/\alpha^o$, всё же демонстрируют стремление к 0.

Проиллюстрируем данные утверждения. На рисунке 2, для большей наглядности в логарифмической шкале, показана зависимость (5) для разных значений λ и кривая $s(\alpha-1,\alpha)$ (штриховая линия), где на всех графиках отчетливо видны минимумы функции $s(\lambda,\alpha)$ и мажорирование их критерием (5) для упрощённого приближения $s(\lambda,\alpha^*)$.

На рисунке 3 видно его стремление к наилучшему, $s_{\min}(\lambda)$ (верхняя линия на верхней диаграмме), и последнего к 0 (нижняя линия). Правда, на нижней диаграмме можно убедиться в относительной безуспешности стремления $s(\lambda,\alpha^*)$ к $s_{\min}(\lambda)$.

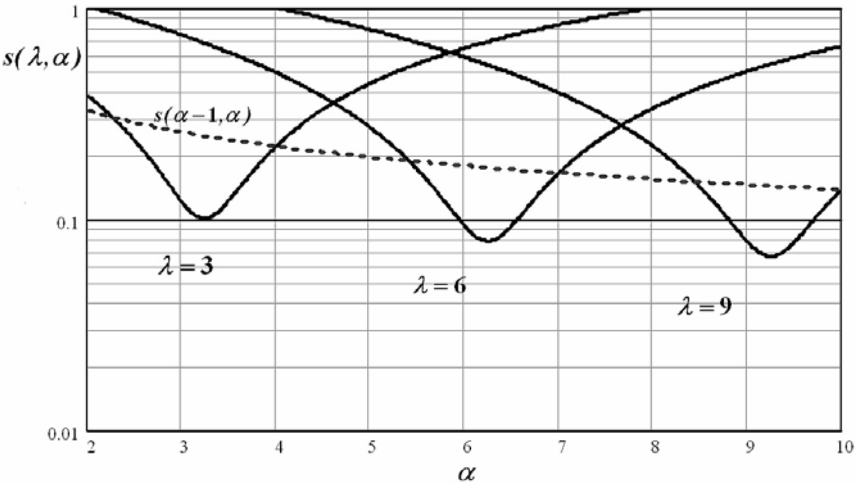

Рис. 2. Вид критерия приближения для различных значений λ

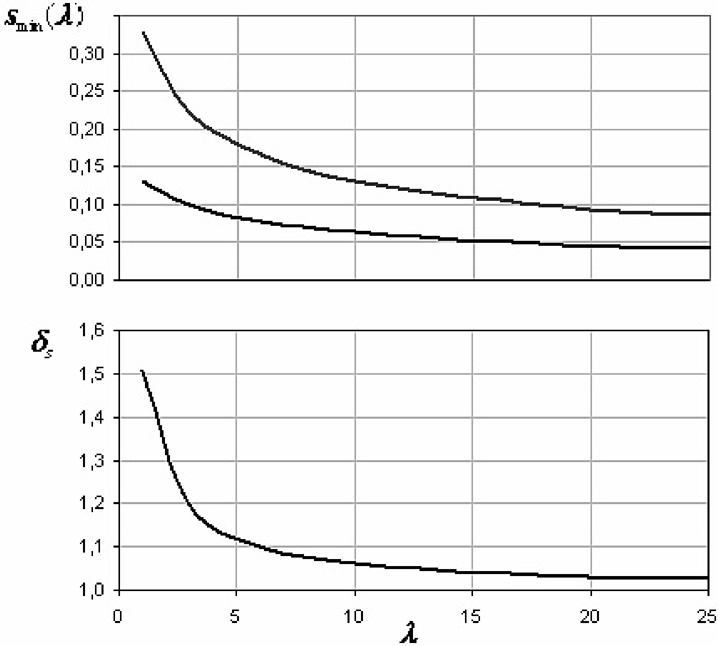

Рис. 3. Зависимость критерия приближения от параметра λ и оценка качества упрощенного приближения

Сходимость оценок упрощенного приближения к наилучшему, как видим, не быстрая, имеет свои особенности, и поэтому им следует пользоваться с осторожностью, но приближение последнего к экспоненциальному происходит значительно лучше и уже в области умеренных значений $\lambda = 4 \div 5$ становится вполне приемлемым.

Наконец, на рисунке 4 показана динамика изменения параметров приближающего степенного распределения. На верхней диаграмме хорошо заметно отношение $\alpha^* > \alpha^o > \lambda$ с сохранением абсолютной разницы между ними и стремлением к 0 относительных оценок δ_α и δ_λ (нижняя диаграмма).

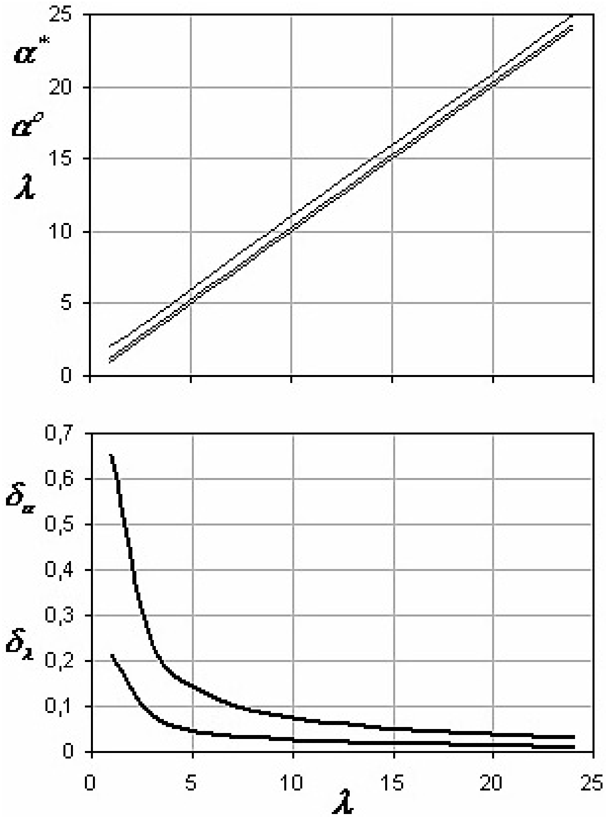

Рис. 4. Динамика изменения параметров приближающего степенного распределения

Наилучшее приближение является более «жёстким», так как по мере уменьшения параметра α свойства степенного распределения ухудшаются, поэтому для пессимистических оценочных расчётов вместо значения α^o можно использовать даже α^*, зная, что состояние оцениваемого объекта, по крайне мере, не лучше оценки.

Таким образом, имеется возможность с оцениваемой погрешностью, уменьшающейся по мере роста параметра λ или α, легко отобразить экспоненциальное распределение в степенное или наоборот. С другой стороны, учитывая, что λ и его обратная величина во многих приложениях экспоненциального распределения имеют физический смысл, становится возможным содержательно интерпретировать безличный параметр α степенного распределения.

3. Параметризация критичности

Киберсистемы все более выполняют интегрирующие, инфраструктурные функции в обеспечении основных видов жизнедеятельности людей, объективно становясь, таким образом, критическими в статусном смысле. И по сути, и, например, соответственно определению, приведённому в разделе 1 данной статьи, взятому из проекта одного технического регламента. Но коль так, очевидно, возникает необходимость ранжировать уровень критичности, учитывая не только значимость, важность объекта, но имея для этого какую-то объективную основу.

В то же время, сложные киберсистемы, о чём говорилось выше, должны рассматриваться как нелинейные динамические системы, поведение которых предполагает возможность перехода в критическое состояние уже в физическом смысле, независимо от их назначения. Но и статусное понимание критичности неявным образом также свидетельствует о нелинейности, по крайней мере, в восприятии меры риска.

Часто для иллюстрации катастрофических нелинейных эффектов приводятся данные по результатам природных стихийных явлений, подчиняющихся степенному закону распределения. Но как распределены физические характеристики этих явлений? Скорее всего, иначе. В самом деле, экстремальное по своим параметрам землетрясение на необитаемом острове не сравнится по своим последствиям даже со значительно более слабым тектоническим проявлением в густонаселённом районе, а одинаковые физические воздействия в районах капитального сейсмостойкого строительства и ветхих построек также приведут к совершенно разному ущербу.

Что касается киберсистем, то чем в своей технической сущности отличаются идентичные отказы в обслуживании или время восстановления информационной системы, например, локального банка, местной администрации, транспортного узла, опасного производства, АЭС? Во всех случаях имеет место всего-навсего поток отказов и восстановлений, а вот цена, в широком смысле этого слова, цена времени при равенстве временных характеристик процессов у них может быть очень разной, даже несопоставимой, а то и практически бесконечной.

Для критически важных информационных объектов, распределенных систем инфраструктурного назначения адекватная оценка рисков, идентификация критических состояний имеют значение, далеко выходящее за их пределы. В такого рода структурно сложных объектах, как отмечалось, незначительный локальный сбой, первичный отказ может сыграть роль малого параметра и привести к непредсказуемому системному эффекту. Но в оценке результатов и в этом случае принципиально ничего не изменится — лишь проявится иной, независимый от субъективного восприятия, механизм нелинейности. Однако и здесь придётся, оценивая ущерб, учитывать ещё и значимость объекта, поскольку технический крах системы совсем не обязательно означает статусную катастрофу конкретного объекта, которая в то же время может произойти на другом объекте из-за незначительных технологических отказов.

Поэтому критичность следует понимать, с одной стороны, как объективное проявление в поведении систем различной физической природы, в том числе, киберсистем, а с другой — как субъективное в некотором смысле восприятие риска. Причём в последнем случае приходится различать критичность локальную, например, с позиции владельца активов, и глобальную, в инфраструктурном или статусном её понимании.

Таким образом, распределение физических характеристик деструктивных процессов, будучи безусловно первичным, всегда не совпадает с распределением меры риска, отображаясь в него явным или неявным образом путём нелинейного преобразования физической шкалы соответственно нелинейным процессам в самом объекте или (и) ситуативно определяемой ценности активов. Линейное масштабирование шкалы распределения физических характеристик если и имеет смысл, то лишь при отсутствии собственной нелинейности системы и незначительной дисперсии характеристик деструктивных процессов. Столь благоприятные условия, по всей видимости, в реальных киберсистемах обнаружить трудно.

Далее будет предложен подход, позволяющий выполнить такое преобразование, и, используя свойства степенного распределения, дать формальные основания для параметризации критических состояний.

В предыдущем разделе значительное внимание было уделено анализу соотношения экспоненциального и степенного законов распределения вероятностей. Действительно, экспоненциальный закон во многих случаях удовлетворительно описывает распределение временных характеристик разнообразных реальных случайных процессов, и это не только эмпирический факт, но следствие его предельности. Но он становится во всех отношениях неудовлетворительным, когда нас интересует не столько сам процесс, сколько результаты его воздействия на объект, когда имеют место обстоятельства, о которых говорилось выше.

В самом деле, рассмотрим некоторый поток событий риска [12], воздействующих на киберсистему. Скорее всего, в силу множественности и независимости его составляющих, это будет простейший поток с экспоненциальным распределением вероятностей времени между событиями. Однако, очевидно, что эти события по своим последствиям совсем не обязательно равнозначны, и тогда мера риска, выраженная, например, как время восстановления системы после реализации событий риска, уже ни коим образом не может оставаться распределённой по экспоненциальному закону. То есть первичная шкала x должна быть нелинейно преобразована в z, и естественно в качестве нелинейности использовать степенную функцию.

Будем определять это преобразование в достаточно общем виде (7) степенной функции z с двумя параметрами p и q:

$$z = px^q,\ \ p > 0,\ \ q > 0\ . \tag{7}$$

При $q = 1$ функция вырождается в линейное масштабирование. Мы же рассматриваем случай, когда шкала нелинейно усиливается, и $q > 1$, но допустимо и обратное соотношение $q < 1$, при котором происходит ослабление шкалы меры риска.

Тогда задача отображения первичного распределения в распределение меры риска состоит в нахождении параметра степенного распределения в новой шкале при сохранении вида (2) функции распределения:

$$\alpha_x x^{-(\alpha_x+1)} \to \alpha_z z^{-(\alpha_z+1)}, \qquad (8)$$

где α_x и α_z — параметры распределения (2), соответственно, в шкале x и z.

Решается она довольно просто, и параметры преобразования (7) для выполнения (8) определяются в следующем виде:

$$p = \left(\frac{\alpha_z}{\alpha_x}\right)^{\frac{1}{\alpha_z+1}}, \qquad q = \frac{\alpha_x+1}{\alpha_z+1}. \qquad (9)$$

Однако возникает практический вопрос, из каких соображений назначать параметр α_z? Если α_x является либо первичным, физически наблюдаемым, либо определяется как решение α^o уравнения (6) или α^* из соотношения (4) в приближении к экспоненциальному распределению, то для определения α_z необходимо найти некоторое правило, позволяющее его идентифицировать.

Поскольку интегральным показателем риска в некоторой шкале его меры можно считать математическое ожидание соответствующего распределения вероятностей, то довольно естественно, хотя и не обязательно, изменение меры оценивать отношением математических ожиданий исходного и преобразованного распределений. Тогда в нашем случае достаточно задать коэффициент k_z, выражающий, например, изменение относительной ценности активов, который согласно (3) выразится в следующем виде:

$$k_z = \frac{m_{\text{р}}(\alpha_z)}{m_{\text{р}}(\alpha_x)} = \frac{\alpha_z(\alpha_x-1)}{\alpha_x(\alpha_z-1)}, \qquad (10)$$

откуда легко находится искомый параметр

$$\alpha_z = \frac{k_z\alpha_x}{(k_z-1)\alpha_x+1}, \quad k_z > \frac{1}{m_{\text{р}}(\alpha_x)}. \qquad (11)$$

Назначение k_z, вообще говоря, произвольно и не связано с исходным распределением, но формально на него должно быть наложено ограничение, указанное в (11), которое, надо сказать, трудно нарушить. Кроме того, при этом будет выполнено условие $\alpha_z > 1$, необходимое для возможности выражения матожидания в форме (3). Для полноты анализа полезно добавить, что α_z как функция k_z при указанных условиях непрерывна и монотонно убывает, приближаясь к 1.

В результате, подставив α_z в форме (11) в выражения (9), можно получить параметры приводящего к отображению (8) преобразования (7), как функций независимых переменных — параметра α_x исходного или приближённого распределения и назначаемого коэффициента k_z.

Если в качестве исходного берётся экспоненциальное распределение в виде (1), и приближение к нему степенного распределения делается по упрощённому варианту (4), то (11) запишется в форме (12):

$$\alpha_z^* = \frac{k_z(\lambda+1)}{k_z(\lambda+1)-\lambda}. \quad (12)$$

Обратим внимание на то, что, поскольку для параметров приближения исходного распределения, как было показано выше (рисунок 4), всегда $\alpha_x^* > \alpha_x^o$, то и в преобразованной шкале для значений параметров α_z^* и α_z^o, как функций вида (11), соответственно, от α_z^* и α_x^o, сохранится такое же отношение $\alpha_z^* > \alpha_z^o$. То есть и после преобразования упрощённая оценка параметра останется более слабой, чем наилучшая.

Приведём наглядный пример нелинейного роста потенциального ущерба, и насколько чувствительна, оказывается, мера риска, если не упрощать её до линейности (рисунок 5, параметры обозначены без индексов).

Пусть исходный процесс представлен простейшим потоком событий с интенсивностью $\lambda = 8$. Согласно (4) приближаем экспоненциальное распределение степенным (на рисунке параметры без индексов) с $\alpha_x^* = 9$ (тонкие линии на диаграммах, где ещё раз можно убедиться, сколь они близки). Назначим $k_z = 2$ (возрастание ценности активов, значимости объекта, его структурное усложнение, повышение требований оперативности и т. д.). Применив выражения (11) или (12), получаем $\alpha_z^* = 1.8$ (на диаграммах соответствующие функции распределения изображены жирными линиями). В результате медиана распределения 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).

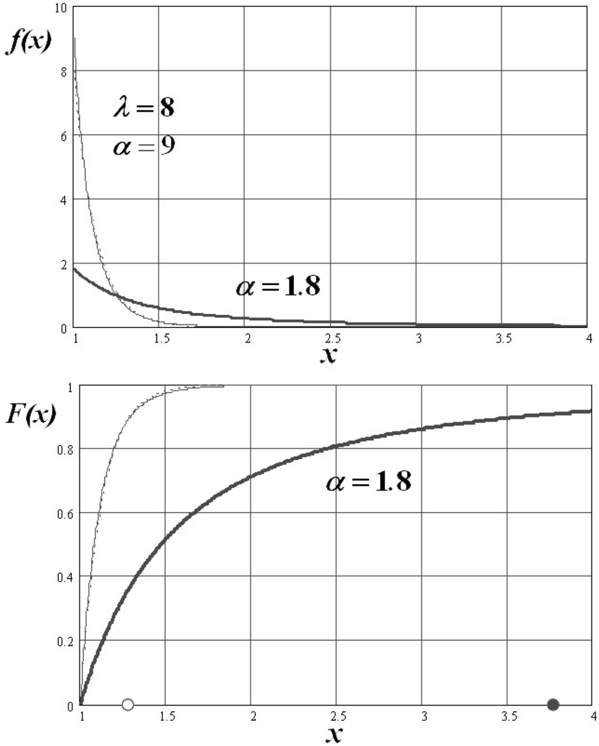

Рис. 5. Нелинейное преобразование меры риска

Добавим, что дисперсия, 2-ой центральный момент (о чём речь пойдёт ниже), при таком значении параметра бесконечна, и получается, что объект, в котором протекал вполне спокойный по техническим параметрам процесс, как только была учтена возникающая независимо от него нелинейность меры риска, оказывается едва ли не катастрофоопасным.

Какая же прагматика может быть извлечена из приведённого анализа? Возникает два класса задач или применений. К первому отнесём, задачи разнообразного оценивания объектов, отнесённых априори к критическим в некотором смысле этого слова. Разумеется, для того, чтобы определить параметр α_z и назначить k_z хотя бы в форме (10), недостаточно волевого решения, требуется расчёт, учитывающий разнообразие характеристик: здесь и характеристики надёжности, сложности, ценности и значимости самого объекта, и, конечно, характеристики процессов в оперативной среде. Однако для грубой оценки необходимых параметров преобразования достаточно и экспертного знания, особенно, если происходит относительное оценивание.

Пока речь не идёт о критических значениях оценки, но объективное ранжирование таких объектов уже может быть произведено, и, если уровень полученной оценки оказывается неудовлетворительным для данного объекта, то необходимы меры по управлению его критичностью. К ним можно отнести повышение надёжности, защищённости, а может быть, и снижение значимости объекта тем или иным образом, возможны и противоречивые пути уменьшения уровня критичности до приемлемого. Любые управляющие критичностью воздействия априори получат при этом оценку в той же шкале.

К этому же классу можно отнести задачи, возникающие при изменении обстоятельств и условий функционирования объекта, подобных названным в приведённом выше примере, что влечёт за собой необходимость преобразования шкалы меры риска и получения новых оценок.

Второй класс задач возникает для режима мониторинга. Отслеживая в реальном времени статистические характеристики контролируемых физических процессов и зная те же, что и в первом классе задач характеристики нелинейности, свойственные данному объекту, таким же образом, что и в первом случае, но уже на основе апостериорных данных, вычисляется текущее значение параметра α_z. При этом параметры внутренней системной нелинейности объекта можно определять также динамически. Назначение задач данного класса одно — прогноз возникновения критических состояний в контролируемой киберсистеме и выработка оперативных воздействий на неё с целью не допустить их развития.

Но, тем не менее, остаётся вопрос, как связать значение параметра с критическими состояниями, ведь критичность по сути своей дискретна. В этом и состоит преимущество степенной модели распределения вероятностей для меры риска, что она не только представляется наиболее адекватной, но и позволяет, в силу своих особенностей безотносительно к конкретным объектам определить критические состояния в них через критические значения параметра α_z.

Дело в том, что моменты степенного распределения (будем оперировать центральными моментами μ_i) обладают замечательным свойством. Не станем здесь приводить громоздкие, даже в общем виде, предельные выражения для них, достаточно будет частных, полезных в дальнейшем:

$$\mu_2 = \frac{\alpha}{(\alpha-2)(\alpha-1)^2},\ \alpha > 2;$$

$$\mu_3 = \frac{\alpha}{\alpha-3} - 3\frac{\alpha^2}{(\alpha-2)(\alpha-1)} + 2\left(\frac{\alpha}{\alpha-1}\right)^3,\ \alpha > 3; \tag{13}$$

$$\mu_4 = \frac{\alpha}{\alpha-4} - 4\frac{\alpha^2}{(\alpha-3)(\alpha-1)} + 6\frac{\alpha^3}{(\alpha-2)(\alpha-1)^2} - 3\left(\frac{\alpha}{\alpha-1}\right)^4,\ \alpha > 4.$$

Важен простой факт, который из них следует, а именно: при $\alpha \le i$ $\mu_i \to \infty$, что является безусловно качественным переходом для моделируемого таким распределением объекта или явления. То есть значения $\alpha = i$ можно считать критическими, независимо от моделируемой реальности, а состояния объекта в окрестности этих значений также следует считать критическим в некотором смысле. Практически применяются моменты с индексами $i = 2 \div 4$, и тогда с этими точками можно связать, соответственно, кризис рассеяния, асимметрии и эксцесса распределения, что уже допускает некоторую содержательную интерпретацию.

Интересно рассмотреть те же явления в пространстве нормированных центральных моментов, которые определяются следующим образом:

$$\beta_1 = \frac{\mu_3^{\ 2}}{\mu_2^{\ 3}},\ \ \beta_2 = \frac{\mu_4}{\mu_2^{\ 2}}. \tag{14}$$

Они обычно используются для качественной оценки статистического материала и аппроксимации эмпирическими или стандартными распределениями, образы которых в этом пространстве (точки, линии или области) позволяют просто и наглядно оценить предполагаемые свойства аппроксимируемого распределения по близости к известным [13]. Между прочим, заметим, что для степенного распределения

$$\lim_{\alpha\to\infty}\beta_1 = 4,\ \ \lim_{\alpha\to\infty}\beta_2 = 9, \tag{15}$$

т. е. они совпадают со своими значениями для точечного образа экспоненциального закона в этом пространстве. Тем самым косвенно подтверждается высказанный ранее тезис о «плавности» перехода экспоненциального и степенного распределений друг в друга.

Очевидно, что сначала при $\alpha = 4$ $\beta_2 \to \infty$, затем при $\alpha = 3$ уже $\beta_1 \to \infty$, а траектория степенного распределения терпит разрывы, что подтверждает сделанные выводы о критичности этих значений параметра. Но наиболее интересные явления происходят при $\alpha \le 2$, когда и нормирующий знаменатель, дисперсия, $\mu_2 \to \infty$, а в выражениях (13) возникает плохо разрешимая неопределённость. Наконец, математическое ожидание при $\alpha \le 1$, теряет конечное значение, что можно увидеть даже по выражению (3). Именно в этой области значений параметра с приближением к $\alpha \approx 1$ наблюдаются процессы, связанные с понятием самоорганизованной критичности [2], которому уделено большое внимание в работах, указанных в предыдущем разделе.

Однако в плоскости (β_1, β_2) обнаруживается ещё одна точка, которую трудно обнаружить другим способом, но и её можно отнести к критической. Оказывается, при $\alpha \approx 6.565$ траектория степенного распределения пересекает граничную линию между двумя существенно разными типами эмпирических распределений — «если кривые пересекаются, это что-то значит». Происходит переход от ограниченного распределения Джонсона типа S_B к неограниченному типа S_U, явный признак того, что в окрестности этого значения параметра хвост распределения начинает существенно удлиняться, во всяком случае, а, учитывая свойства степенного распределения, и утолщаться, направо в сторону более значимых событий риска.

На рисунке 6 показано, как это происходит. Затемнённая нижняя часть диаграммы соответствует области S_B, а светлая — S_U, граница между ними определяется параметрическими уравнениями (16), приведёнными в [13]:

$$\beta_1 = (\omega - 1)(\omega + 2)^2,\ \beta_2 = \omega^4 + 2\omega^3 + 3\omega^2 - 3\,. \tag{16}$$

Траектория степенного распределения для $\alpha > 4$ пересекает границу в точке с приблизительными координатами $\beta_1 \approx 12{,}52$ и $\beta_2 \approx 31{,}43$. Поскольку имеют место пределы (15) при монотонном убывании, то переход происходит именно в область S_U. Далее, подставив полученные значения в (14), из (13) находится искомое, легко запоминающееся $\alpha \approx 6.565$.

Итак, по крайней мере, четыре значения параметра, $\alpha = i$ при $i = 1 \div 4$, а ещё, надо полагать, и пятое, самое слабое, но, думается, важное

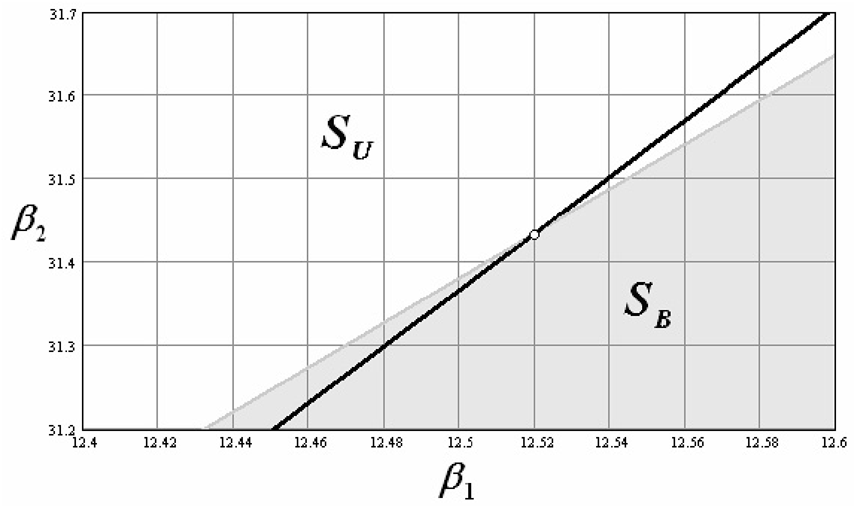

Рис. 6. «Пятая» критическая точка

для задач прогнозирования, есть основания считать критическими и связывать с ними критические состояния моделируемых объектов. В чём и как критичность выражается в содержательных терминах — другой вопрос, но объективно это так.

Как уже было сказано, наиболее сложные и интересные процессы происходят при $\alpha \le 2$ и особенно в окрестностях 1, в области «джокера» в терминах синергетики. Они требуют специального исследования в приложении к нашему подходу. К тому же это быстрые, с потерей устойчивости, многомерные, а значит плохо управляемые процессы, поэтому практическая задача по обеспечению кибербезопасности всегда состоит в том, чтобы не допустить повышения критичности до такого уровня, удержать процесс в области «русла». И в этом смысле приведённый анализ даёт инструмент для управления рисками критических систем.

4. Проблемы и перспективы

Индикация критических или предкритических состояний, которую позволяет обеспечить предложенный подход, надо признать, не достаточна для целенаправленного активного управления рисками, безопасностью киберсистем. Чтобы решать задачи такого рода, не обойтись без знания в содержательных терминах структуры факторов риска, оценок их значимости, действие которых в конечном итоге и отражается в индикаторах. Средства управления также надо содержательно определить и структурно увязать с факторами риска. Некоторые шаги в этом направлении сделаны [14].

Тогда, поскольку управление рисками должно осуществляться в области «русла», можно говорить об отыскании параметров порядка и управления ими с практической конкретностью. Пожалуй, в этом и состоит главная проблема реализации нашего подхода, как теоретическая, так и технологическая.

Требуют исследования вопросы динамики оценок. Как быстро развиваются критические состояния, каков горизонт прогноза в зависимости от текущего значения наблюдаемого параметра степенного распределения?

Особое внимание необходимо крайним критическим состояниям. Первое — самоорганизованная критичность. Хотя до этого состояния объект доводить нельзя, но что предшествует её развитию в предлагаемом статистическом образе? «Пятое» состояние интересно своей неясностью и возможностями для отдалённого прогноза.

Наконец, нельзя обойти проблему рассеяния оценок, которая нередко игнорируется из-за сложностей, при этом возникающих, но без её решения доверие к оценкам всегда будет под вопросом.

Представление разнообразных системных нелинейностей в сложных информационных структурах, отображаемых в преобразовании шкалы меры риска, в значительной степени независимо от задач собственно управления рисками, но даст более убедительную основу для такого преобразования.

В практическом отношении важно методически обеспечить содержательное шкалирование меры риска, её связь с техническими характеристиками, и тогда даже упрощённые, грубые оценки, которые можно сделать без решения названных проблем и сложного инструментирования, будут полезны для применения.

Литература

1. *Хованов Н. В.* Математические модели риска и неопределенности. СПб.: Издательство СПбГУ, 1998. 204 с.
2. Новое в синергетике: Взгляд в третье тысячелетие / Кибернетика: неограниченные возможности и возможные ограничения. Под ред. И. М. Макарова. М: Наука, 1996. 264 с.
3. *Mainzer K.* Thinking in Complexity / The Computational Dynamics of Matter, Mind, and Mankind. 3rd rev, andenlarget ed. Berlin: Springer, 1997. 456 p.

4. Новое в синергетике: Взгляд в третье тысячелетие / Информатика: неограниченные возможности и возможные ограничения. Под ред. Г. Г. Малинецкого, С. П. Курдюмова. М: Наука, 2002. 480 с.
5. *Владимиров В. А., Воробьёв Ю. Л., Малинецкий Г. Г., Подлазов А. В.* и др. Управление риском. Риск, устойчивое развитие, синергетика. М.: Наука, 2000. 432 с.
6. *Малинецкий Г. Г.* Сценарии, стратегические риски, информационные технологии // Информационные технологии и вычислительные системы. 2002, № 4. С. 83–108.
7. *Князева Е. Н.* Сложные системы и нелинейная динамика в природе и обществе [Электронный ресурс]. Режим доступа: http://www.synergetic.ru/society/index.php?article=kn3
8. *Кузнецов И. В., Малинецкий Г. Г., Подлазов А. В.* Научная основа междисциплинарного исследования бедствий, катастроф и кризисов. Препринт / ИПМ РАН. № 47. М., 2004. 11 с.
9. *Александров В. В.* Развивающиеся процессы и системы. Степенные законы // Информационные системы и технологии. 2007. № 1 (1). С. 58–83.
10. *Герман А. С.* Антиглобалистский манифест // Академия Тринитаризма, М., Эл № 77-6567, публ. 13857, 06.10.2006 / Под ред. Л. А. Шелепина [Электронный ресурс]. Режим доступа: http://www.trinitas.ru/rus/doc/0230/002a/02301006.htm
11. *Золотарев В. В.* Устойчивые законы и их применения. М.: Знание, 1984. 63 с.
12. *Черешкин Д. С., Кононов А. А.* Экспертная система комплексной оценки безопасности автоматизированных информационных систем // Проблемы управления и моделирования в сложных системах: Труды II Международной конференции / Под ред. В. П. Масленикова, Н. А. Кузнецова, В. А. Виттиха. Самара: СНЦ РАН, 2000. С. 363–365.
13. *Хан Г., Шапиро С.* Статистические модели в инженерных задачах / пер. с англ. Е. Г. Коваленко. Под ред. В. В. Налимова. М.: Мир, 1969. 396 с.
14. *Шишкин В. М.* Метамодель анализа, оценки и управления безопасностью информационных систем // Проблемы управления информационной безопасностью: Сборник трудов ИСА РАН / Под ред. Д. С. Черешкина. М.: Едиториал УРСС, 2002. С. 92–105.