ФИЛОСОФИЯ ЗАЩИТЫ

ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
хозяйствующих субъектов, работающих в условиях рыночной экономики

Совершенствуя существующую систему экономической безопасности хозяйствующего субъекта, его руководитель принимает во внимание совокупность факторов риска, их взаимодействие и взаимное влияние друг на друга. В первую очередь в расчет принимаются три их основные составляющие: вероятность реализации фактора риска (возникновения инцидента), ущерб от его реализации (потенциальные потери ресурсов, потребительских свойств, деловой репутации фирмы) и величину ресурсных затрат ХС на снижение негативных последствий для защищаемого объекта (например, компенсации потерь) или ликвидацию риска для последнего как такового (уклонение от рисковой операции).

Существует множество подходов к выбору наиболее подходящих методов обеспечения экономической безопасности ХС. Они нашли широкое отражение в различных научных публикациях ряда современных авторов, проводящих исследования, результаты которых находят отражение в публикациях по профильной тематике[1].

Для понимания сущности технологии оценки рисков остановимся на наиболее простой методике, принимающей в расчет малое количество исследуемых параметров, освещенных авторами Минзовым А. С., Кольером С. М., упомянутым выше в ссылке 1.

Упрощенная методика (учитывающая только три вышеуказанных показателя) позволяет на практике принять оптимальное управленческое решение, касающееся выбора приоритетной политики безопасности в отношении защищаемого объекта, функционирующего по заданному алгоритму, в заданном месте и в определенное время. В рассматриваемой ме-

МИХАИЛ ВЛАСЕНКО,
доцент кафедры «Анализ рисков и экономическая безопасность»
Финансового университета при Правительстве РФ, кандидат экономических наук

тодике будем использовать следующие обозначения:
P – вероятность реализации реально существующего фактора риска (опасности, угрозы) на защищаемый объект;
U – ущерб от реализации угрозы (величина потенциальных потерь);
R – риск – мера, определяющая степень опасного воздействия отдельной угрозы на защищаемый объект (ресурс, процесс, рабочее место, человека, изменяющего его свойства, параметры);
Z – затраты на минимизацию ущерба от воздействия опасности[2].

Полученные результаты могут быть представлены в процентном выражении, в долях единицы или классифицироваться по некоторой шкале в виде значений терм-переменных, например, «высокая», «средняя», «низкая», опасность, потери.

Графическая интерпретация результата анализа факторов риска экономической деятельности хозяйствующего субъекта ХС по двум показателям (вероятность/ущерб) и трем качественным уровням опасности (высокая/средняя/низкая) измерения каждого фактора риска представлены на рис. 1.

Проведя оценку системы экономической деятельности предприятия с точки зрения отдельных рисков для ее подсистем и элементов, получим результаты, представленные в виде системной области, разбитой на девять частей, которые отличаются по двум параметрам – вероятности возникновения инцидента и ущерба от его реализации. Эти два параметра позволяют нам классифицировать инциденты (факторы риска) по трем уровням опасности для защищаемой системы – низкому, среднему, высокому.

Как видно из данного рисунка, все поле представляет собой девять частей, для каждой из которых имеется свой уровень вероятности реализации фактора риска и ущерба объекту (потери потребительских свойств, ТМЦ) от него.

Проведя анализ и оценку специфики и особенностей каждого из девяти секторов, представленных на рис. 1, определимся с логикой выбора стратегии защиты.

В результате анализа установлено, что область 9 имеет самый высокий уровень показателей как по оси X (ущерб), так и по оси Y (вероятность происшествия). Потери от реализации угроз высокой степени вероятности, наносящих максимальный ущерб, будут оказывать наибольшее влияние на деятельность ХС, поэтому данная область является наиболее важной (первоочередной) для воздействия на факторы риска, входящие в нее, системы экономической безопасности. Похожими характеристиками будут обладать области 6 и 8. В их случае один из показателей X или Y будет на отметке среднего значения, а второй – на отметке высокого значения. Эти области имеют, так же как и область 9, довольно высокий уровень риска.

Как видно из рисунка, область 1 имеет самые низкие показатели по двум осям: этот сектор является наименее рисковым по сравнению с другими областями, что сводит задачу защиты ресурсов выделенной области к минимуму. В некоторых случаях в отношении факторов риска данной области из-за его незначительности и приемлемости для объекта защитные меры обычно не предпринимаются вообще. Такой вариант может иметь место в случае, когда

ВЛАСЕНКО Михаил Николаевич,
специалист в области безопасности бизнеса более чем с 20-летним стажем работы. Ранее находился на государственной службе. Стоял у истоков охранного бизнеса, руководил охранно-сыскным предприятием, службами безопасности инвестиционной компании, крупной торговой сети и управляющей компанией машиностроительного холдинга.
В настоящее время – доцент кафедры «Анализ рисков и экономическая безопасность» Финансового университета при Правительстве Российской Федерации, профессор РАЕ, действующий эксперт Международной контртеррористической тренинговой ассоциации (МКТА), независимый консультант по экономической безопасности, кандидат экономических наук.
Разработчик множества эффективных методик защиты экономических интересов объектов, функционирующих в условиях рынка, автор ряда учебных курсов по безопасности бизнеса, автор более 50 работ по профильной тематике.
г. Москва, 57643@rambler.ru

Рис.1. Результаты анализа и оценки факторов риска экономической деятельности ХС

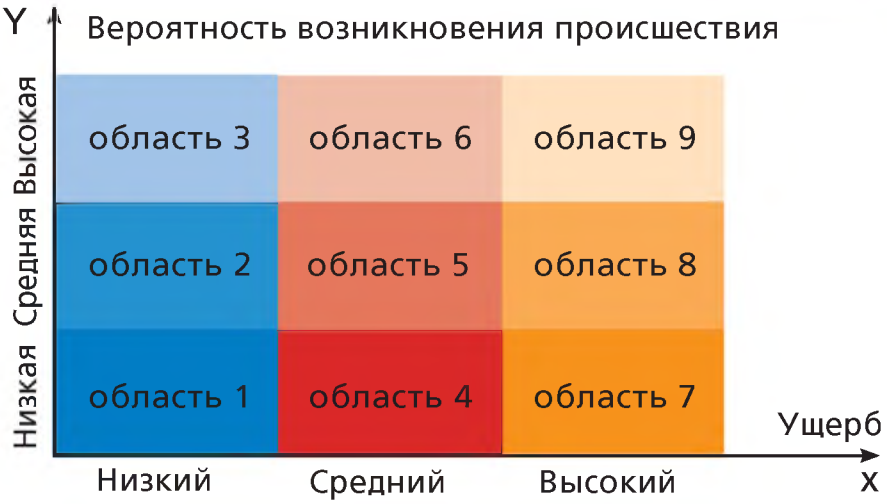
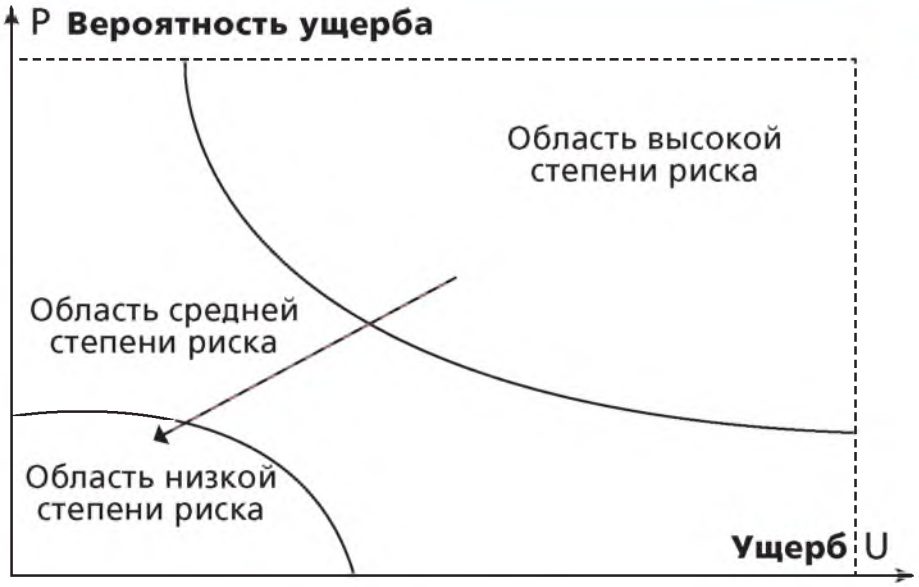


Рис. 2. Разделение рисков в двухфакторной модели анализа

Рис. 3. Графическая интерпретация превентивной политики безопасности



затраты на компенсацию потерь будут меньше, чем затраты на реализацию защитных мер, и это приемлемо спецификой объекта (потери не критичного для ХС ресурса, который легко поддается замене, например: сырье, обычный инструмент, рядовой сотрудник).

Области 2 и 4 также имеют схожие параметры с областью 1, их защита вполне может строиться на приемах минимальной (разумной) достаточности, в том числе и полное игнорирование рисков, считая их приемлемыми для объекта.

Затруднения могут возникнуть с областями 3, 5, 7, которые имеют в сумме серединные значения, что не позволяет однозначно определить политику защиты объекта. При принятии решений по обеспечению безопасности следует руководствоваться выделенным бюджетом на всю систему защиты предприятия в целом, а также перспективами развития защищаемого ресурса в будущем, его важности для системы экономической деятельности и предприятия в целом.

С учетом выше представленных рассуждений все защищаемые ресурсы организации могут быть разделены на три характерные области в зависимости от уровня возможного риска и степени его опасности для объекта защиты (рис. 2).

Проанализировав и оценив подобным образом систему экономической деятельности организации, ее основные ресурсы, подлежащие защите, мы можем ранжировать риски и предложить руководителю такие механизмы обеспечения безопасности, которые будут обеспечивать защиту ресурсов в зависимости от их значимости для деятельности ХС в рамках принятой политики безопасности.

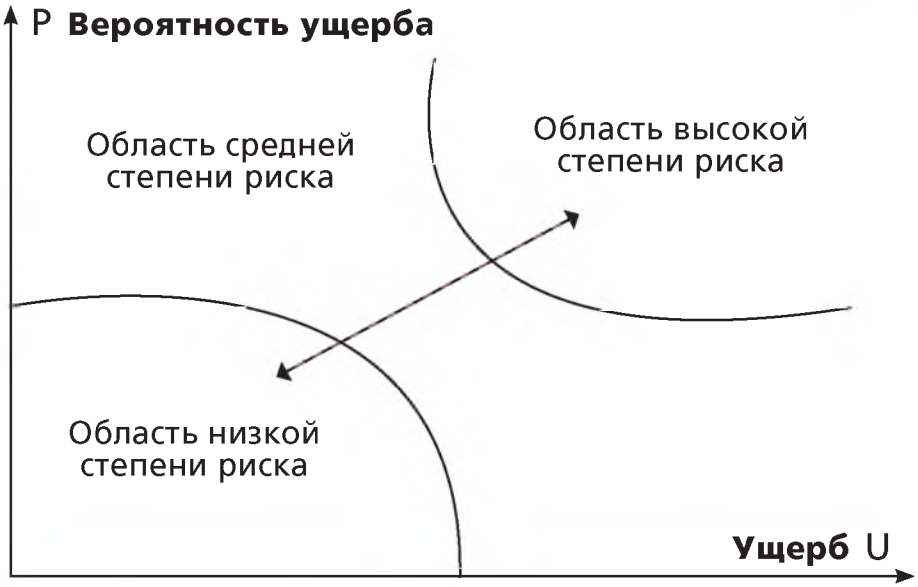
Для всех случаев сопоставления рисков смежных областей <P, U> более предпочтительными для минимизации являются те из них, которые будут соответствовать областям с более высоким значением рисков и/или ущерба.

С учетом вышеизложенного руководитель хозяйствующего субъекта может принять оптимальное решение о применении тех или иных механизмов защиты, учитывая еще один важный фактор: наличие ресурсных возможностей ХС, которые могут быть задействованы для обеспечения его экономической безопасности, а также ограничений и приоритетов, о которых разговор пойдет ниже. Данное решение может лечь в основу политики безопасности, которая, как было указано в одной из предыдущих публикаций, может носить как компенсационный, так и предупредительный характер или сочетать их в отношении одного и того же объекта.

Рассмотренная методика выбора системы защиты в части обоснования затрат на систему экономической безопасности показывает, что не представляется возможным четко провести грань между рисками, потери от которых необходимо предупреждать, и теми, потери от которых необходимо компенсировать руководитель стоит перед дилеммой: когда применить компенсационную, а когда превентивную технологию защиты.

В настоящее время, на практике, для обеспечения экономической безопасно-

Рис. 4. Графическая интерпретация активной политики безопасности



сти ХС, функционирующих в условиях современного рынка, применяются следующие основные политики безопасности:

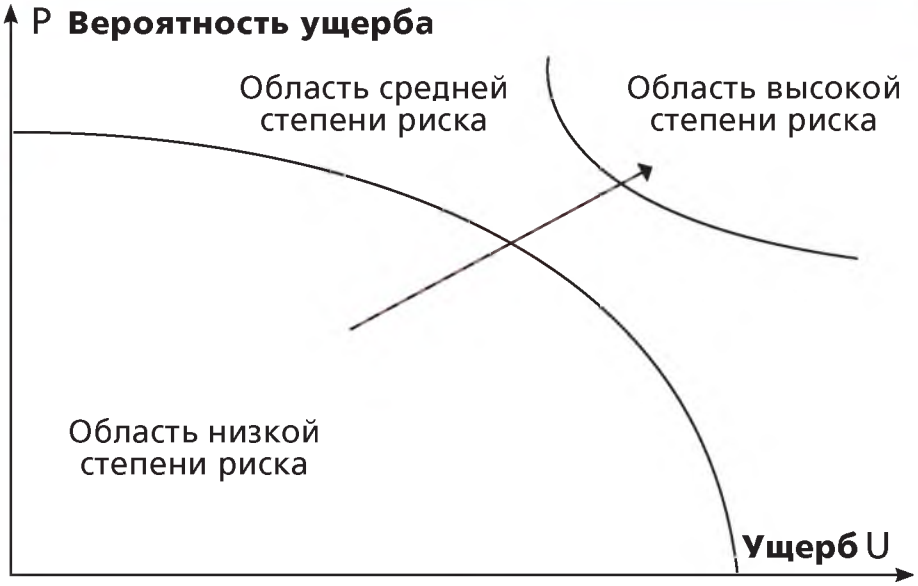
А) Превентивная политика безопасности (предупредительная) – ориентирована на предупреждение и максимальную защиту как от наиболее вероятных рисков, наносящих максимальный ущерб, так и от рисков средней вероятности, наносящих большой ущерб, а также рисков большой вероятности, наносящих средний ущерб. При этом маловероятные риски, ущерб от которых незначительный (стоимость защиты превышает потенциальные потери), принимаются как допустимые. К тому же, система безопасности предусматривает создание резерва ресурсов, которые могут быть задействованы для компенсации потерь, в случае реализации рисков последней группы. Затраты на систему безопасности в данном случае – максимальные. Стрелкой на рисунке показан акцент смещения внимания руководителя при выборе областей защиты (рис. 3).

Б) Активная политика безопасности (предупредительно-компенсационная) – ориентирована на предупреждение и максимальную защиту только от наиболее вероятных рисков, наносящих максимальный ущерб. Что касается рисков средней вероятности, наносящих большой ущерб, а также рисков большой вероятности, наносящих средний ущерб, в системе безопасности предусматривается резерв ресурсов, который задействуется для компенсации потерь в случае реализации рисков в указанных группах. При этом маловероятные риски, ущерб от которых незначительный, обычно игнорируются. Превентивные затраты на систему принимаются руководителем как допустимые безопасности, в данном случае – средние.

Стрелкой на рисунке показан акцент смещения областей защиты (рис. 4).

В) Реактивная политика безопасности (компенсационная) – традиционно не ориентирована на существенное предупреждение ущерба. В системе безопасности, построенной по данному принципу, предусматривается резерв ресурсов, который задействуется для компенсации потерь в случае реализации каких-либо рисков, вне зависимости от их групповой принадлежности. Стрелкой на рисунке показан акцент смещения областей защиты (рис. 5).

Рис. 5. Графическая интерпретация реактивной политики безопасности



Предупредительные затраты на систему безопасности в данном случае – минимальны.

Таким образом, мы видим три основополагающих подхода к обеспечению экономической безопасности субъектов хозяйственной деятельности. При этом необходимо помнить, что сами по себе (в одиночку) описанные подходы практически не применяются. В любом случае имеет место их комбинация со смещением управляющего акцента в ту или иную сторону. Притом такие смещения осуществляются динамично, постоянно изменяясь во времени, адаптируясь под особенности внутренней и внешней среды ХС.

Как указано выше, система безопасности не является статической. Политики безопасности могут меняться в зависимости от рыночной ситуации,

Рис. 6. Зависимость вероятности нанесения ущерба системе информационной безопасности от величины затрат на создание и поддержание защиты

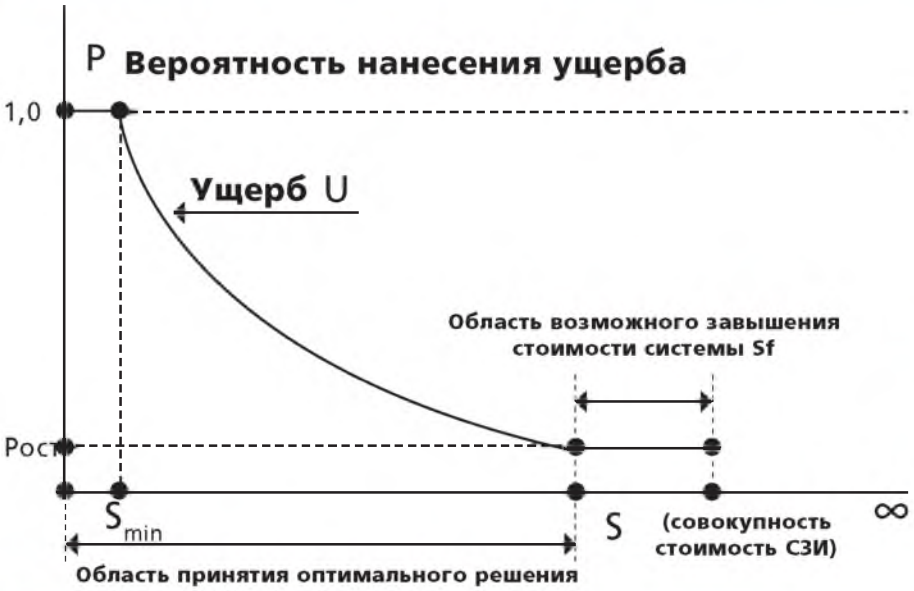
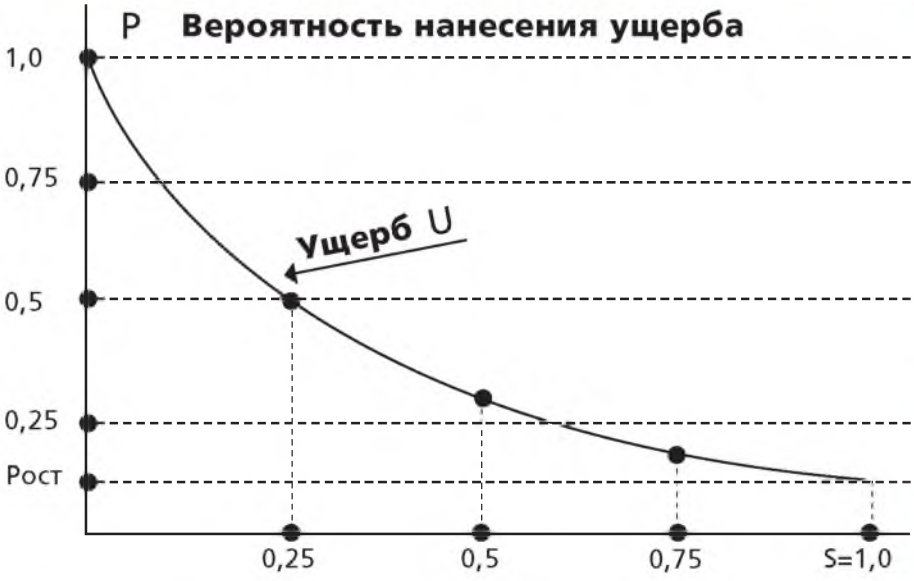


Рис. 7. Снижение величины ущерба от вложений средств в СЗИ



(доля средств от оптимальной совокупной стоимости СЗИ)

приоритетных для ХС целей и задач в настоящее время.

Для простоты понимания основ оптимизации затрат на систему безопасности ХС рассмотрим пример защиты его информационной системы.

Зависимость вероятности нанесения ущерба информационной системе P предприятия от величины затрат S на создание и поддержание системы защиты находятся во взаимосвязи и могут быть представлены графически (рис. 6).

При этом на участке S_{min} – S наблюдается снижение возможных потерь предприятия по причине нарушения системы информационной безопасности при вложении средств в систему ее защиты не до нулевого уровня, а до величины Рост, вызванной следующими основными факторами:

- скрытыми недостатками системы защиты;
- возможными несанкционированными действиями персонала, в том числе и злоумышленников, предусмотреть которые в процессе проектирования, создания и эксплуатации системы безопасности сложно;
- появлением новых технологий, нарушающих работу СЗИ и неучтенных в существующей системе безопасности при ее создании;
- технологическими сбоями в работе системы по причинам, не зависящим от действий обслуживающего персонала;
- форс-мажорными обстоятельствами.

Необходимо помнить, что оптимальная величина вложений в СЗИ лежит в области принятия решений $S_{опт} \in [0; S]$ и зависит от политики предприятия в отношении размера вложений в безопасность, уровня его организационной зрелости и других обстоятельств, о которых говорилось выше, определяющего особенности управления предприятием и приемлемые технологии принятия руководителем управленческого решения.

В то же время часто при принятии неоптимального решения (с точки зрения затрат) имеет место фактическое завышение стоимости СЗИ на величину S_f. Данное обстоятельство вызвано следующими основными факторами:

- создание избыточной защиты по требованию нормативных актов (законов, указов, распоряжений, инструкций, ГОСТов[3], СНиПов[4] и т. д.);
- создание системы безопасности для защиты государственной тайны;
- создание избыточной защиты по требованию деловых партнеров;
- создание избыточной защиты по требованию вышестоящей организации;
- создание избыточной защиты в связи с отсутствием опыта в профильной сфере, что приводит к ошибкам в расчетах, переоценке угроз и т. д.;
- принятие руководителем решения о приобретении более дорогой системы в связи с использованием недостоверной информации о более дешевых системах (технико-эксплуатационных показателях, сложности обслуживания, наработки на отказ и т. д.);
- при выполнении имиджевых требований;

Таблица 1. Результаты оценки рисков ХС

№ п/п	Наименование рисков	Вероятность	Ущерб, млн. руб.	Затраты на снижение риска до допустимого уровня, млн руб.
1	R1	0,1	0,5	0,2
2	R2	0,01	0,2	0,1
3	R3	0,2	1,2	0,2
4	R4	0,4	4,0	0,5
5	R5	0,02	1,0	0,2
6	R6	0,3	2,0	0,1
7	R7	0,2	1,5	0,5
8	R8	0,3	1,8	0,3

- при отсутствии технологических (несовместимость старых и новых решений), организационных, временных, пространственных, природно-климатических и других возможностей применить более дешевые решения;
- принятие потребителем условий поставщика услуг (систем) безопасности, проводящего агрессивную маркетинговую политику по распространению систем защиты;
- в случае принятия решения под воздействием коррупционной составляющей, например, принуждение со стороны вневедомственной охраны МВД к переходу жителей города, установивших аналоговую систему охраны квартир, на цифровую систему охраны объектов.

Особое внимание лицу, принимающему решение, необходимо обратить на участок от 0 до S_{min}, характеризующий состояние СЗИ (системы безопасности), при котором минимальные вложения в систему уже сделаны, но потрачены они на подготовительные мероприятия. При этом система безопасности остается нефункциональной, риски не снижаются. Только при достижении величины вложений S_{min} дальнейшее финансирование системы безопасности будет способствовать плавному снижению вероятности реализации рисковой ситуации до уровня Рост.

В случае ограниченного финансирования системы защиты, отсутствия возможности выделения средств размером S_{min} – S разумнее всего отказаться от реализации разработанной технологии защиты и поискать другие, более приемлемые и дешевые решения.

Под оптимизацией в области безопасности понимается процесс определения такого состояния исследуемой системы, при котором обеспечивается достижение экстремального (минимального или максимального) значения одним или несколькими (что лучше) показателями ее функционирования (функции цели).

Многочисленные исследования профильных специалистов показали, что при рациональном использовании ресурсов, задействованных в обеспечении безопасности, грамотном выборе мер защиты и их сочетания эффект может значительно превосходить величину средств, вложенных в защиту. Это вызвано значительным взаимным положительным влиянием мер защиты, которое, как правило, больше, чем их взаимное негативное воздействие (рис. 7).

В тех случаях, когда доминирующим выступает требование обеспечения абсолютной безопасности информации, когда Рост. должно стремиться к 0 (например, защита государственной тайны), концепция экономически оптимальной системы ЗИ неприменима.

Более высокий уровень безопасности достигается за счет увеличения затрат на систему безопасности (защиты информации).

Как показывает практика, величина ущерба от реализации угроз, вероятность их возникновения и стоимость защитных мер не связаны между собой. Часто угрозы, имеющие низкую вероятность реализации, могут нанести максимальный ущерб, вплоть до фатального, когда объект не может восстановить свой первоначальный потенциал и наоборот.

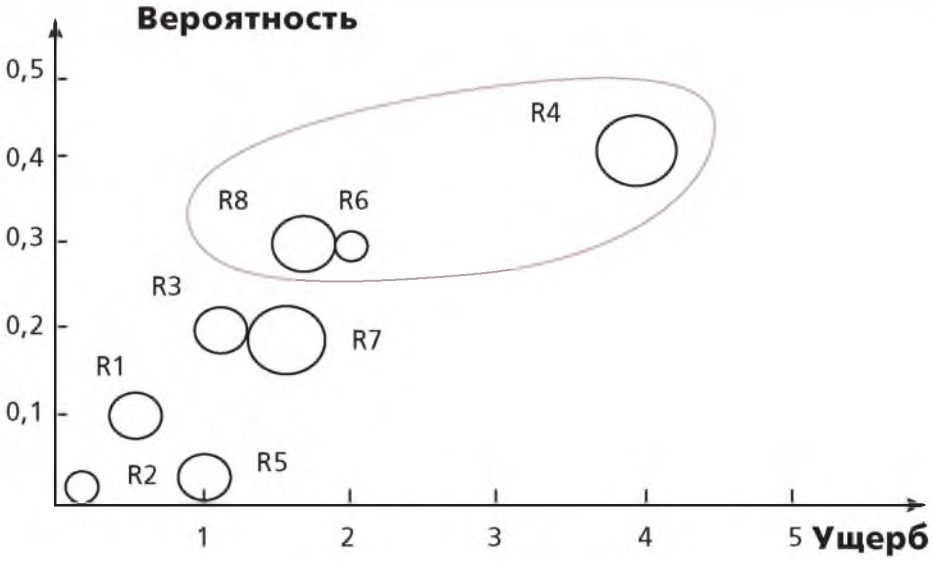
С учетом указанных обстоятельств руководитель принимает решение на внедрение тех или иных мер безопасности, выбирая приоритетную политику безопасности, учитывающую все ранее перечисленные факторы в совокупности. На практике это может быть проиллюстрировано решением простенькой задачи.

Руководитель предприятия, создавая систему обеспечения безопасности, должен принять решение относительно выбора основных рисков в деятельности хозяйствующего субъекта, в отношении которых необходимо принять первоочередные защитные меры.

В таб. № 1 представлены результаты оценки рисков ХС по различным направлениям его экономической деятельности: вероятности их возникновения и оценка возможного ущерба. Кроме этого в таблице приведена оценка средств на снижение риска до допустимого уровня. Допустимая величина затрат на снижение рисков (выделена руководителем предприятия из бюджета) составляет, например, 0,9 млн руб.

Какие риски необходимо учитывать при заданном уровне

Рис. 8. Распределение рисков в системе координат



Целесообразно затребовать выделение дополнительного бюджета, который может быть зарезервирован и далее расходован для компенсации возможных потерь

допустимой величины затрат на обеспечение экономической безопасности ХС, при условии, что предотвращенный ущерб должен быть max. Решение обоснуем графически максимальным.

Решение: Нарисуем график в координатах (вероятность–ущерб). На графике (рис. 8) обозначим риски в форме окружностей, диаметр которых пропорционален затратам на снижение риска до допустимых уровней. Шкала для измерения диаметра окружностей та же, что и для определения величины ущерба. Более значимые риски расположим в правом верхнем углу рисунка (с высокой вероятностью и большим возможным ущербом). Незначительные риски расположены в левом нижнем углу. При выборе рисков, в отношении которых будут предприняты защитные меры, в первую очередь внимание уделяется более значимым рискам с малыми затратами на их снижение до допустимого уровня.

Вывод: В первую очередь необходимо при обеспечении экономической безопасности, используя комплексный подход, уделить внимание рискам R4, R6 и R8. Суммарные затраты на их снижение до допустимых значений составят:

$$Z_{\Sigma} = Z_{R4} + Z_{R6} + Z_{R8} = 0{,}5 + 0{,}1 + 0{,}3 = 0{,}9 \text{ млн руб.}$$

В данном случае мы применили предупредительную политику безопасности. Пологике, у нас остались достаточно опасные для объекта защиты риски: R3 и R7, а также незначительные (приемлемые риски): R1, R2, R5.

Как поступить в данном случае? Ресурсов для компенсации возможных потерь – нет!

На месте руководителя можно затребовать выделение дополнительного бюджета на защиту, который может быть зарезервирован и далее расходован для компенсации возможных потерь по рискам R1, R2, R3, R5, R7. Но для этого потребуется значительная сумма, сопоставимая с первоначальным бюджетом. На этот шаг руководитель, вероятнее всего, не пойдет!

Есть еще выход: передать риск третьей стороне, например страховой компании. Риски R1, R2, R3, R5, R7 нет смысла страховать все стразу. У руководителя вызывают наибольшую обеспокоенность риски R3 и R7. Вероятность их возникновения P=0,2. По расценкам страховых компаний, действующих в настоящее время, их страховое вознаграждение может равняться 10–20 % от размера страховой выплаты в случае наступления страхового случая.

Ущерб от реализации рисков R3 и R7 составит 2,7 млн руб. по условиям задачи. Исходя из этого размер страхового вознаграждения должен составить 0,54 млн руб. Согласно условиям задачи, превентивная защита от данных рисков обойдется для бюджета предприятия в 0,7 млн руб., что существенно ниже 0,9 млн руб., потраченных в первом случае средств. На первый взгляд проблема решена, экономия – налицо!

Как видно из расчета, сумма размером 0,54 млн руб. превышает половину первоначально выделенных на безопасность бюджетных средств. Руководитель и в данном случае не пойдет на данный шаг! Что делать, как защитить объект? К каким мерам безопасности прибегнуть?

Особенности и практические аспекты выбора нами приоритетных политик безопасности, в условиях ограниченности финансовых и других ресурсов, будут рассмотрены нами ниже в последующей публикации. ●

1 Минзов А.С., Кольер С.М. «Методика обоснования затрат на обеспечение системы информационной безопасности хозяйствующего субъекта».\\ М. «Вестник Академии экономической безопасности МВД России». 3'2010 (http://www.econsafety.ru).
Власенко М.Н., Журко Т.В. Оценка эффективности обеспечения системы безопасности деятельности хозяйствующих субъектов. «Аудит и финансовый анализ». № 5, 2008.
Власенко М.Н. «Методология обеспечения экономически эффективного и безопасного функционирования хозяйствующих субъектов в условиях регионального рынка: системный подход». \\ М. «Национальные интересы, приоритеты и безопасность». 5 (146)-2012, стр. 40-47.
Шедько Ю.Н. Программно-целевой метод как инструмент повышения эффективности территориальных социоэкономических систем // Региональная экономика: теория и практика. 2010. № 44. С. 24-30.
Ильин В.В., Шедько Ю.Н Подходы к оценке социально-экономической эффективности развития регионов России // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2012. № 11-12. С. 14-15.
2 Как показывает практика, точность определения значения P зависит от интервала рассматриваемого периода времени Δt, который рассчитывается статистическими методами. Чем больше величина интервала Δt, тем более точные данные мы получим.
3 ГОСТ – государственный стандарт.
4 СНиП – Строительные нормы и правила.
5 http://www.ami-tass.ru/strahovanie/strakhovye-tarify.html и http://www.i-g.ru/insurance/responsibility/