ЭКОНОМИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ, 2008, том 44, № 2, с. 100–107

МАТЕМАТИЧЕСКИЙ АНАЛИЗ ЭКОНОМИЧЕСКИХ МОДЕЛЕЙ

ПРИМЕНЕНИЕ МЕТОДОВ ОПТИМИЗАЦИИ ПРИ АНАЛИЗЕ И УПРАВЛЕНИИ ИНФОРМАЦИОННЫМИ РИСКАМИ

© 2008 г. В. В. Немиткина

(Москва)

Рассматривается математическая модель зависимости уровня информационного риска от объема финансирования мероприятий информационной безопасности. На основе построенной модели формулируется задача оптимизации распределения денежных средств между отдельными задачами защиты информации с целью снижения общего уровня риска. Предлагается способ нахождения экономически обоснованного объема финансирования, необходимого для обеспечения информационной безопасности.

ВВЕДЕНИЕ

В последнее время быстрое развитие технологий передачи и обработки информации сделало ее одним из ценнейших ресурсов. На сегодняшний день информация приобретает уникальную ценность и является одним из критически важных ресурсов (это новые идеи, производственные, коммерческие секреты и т.д.). Поэтому совершенно очевидно, что вопросы обеспечения безопасности информации являются ключевыми проблемами бизнеса (Хрусталев, 2001).

Перед современным бизнесом остро встает задача обеспечения надежной защиты своих информационных ресурсов. Однако, как и любая защита, защита информации является делом крайне дорогостоящим, и далеко не всегда руководители предприятий осознают, что такие вложения могут быть выгодными, позволяя существенно снизить потери, связанные с информационными рисками. Большинство публикаций, посвященных вопросам информационной безопасности, изобилуют всевозможными техническими подробностями, при этом упуская из виду проблему экономической целесообразности тех или иных решений. А ведь именно вопрос экономической эффективности является ключевым при принятии решения о выделении денежных средств на реализацию программ и мероприятий по обеспечению информационной безопасности. На сегодняшний день наиболее распространенный способ решения данного вопроса – применение систем анализа рисков, позволяющих оценить риски в информационной системе и выбрать оптимальный по эффективности вариант контрмер.

В настоящее время существует целый ряд программных продуктов, ориентированных на оценку информационных рисков организаций (Петренко, Симонов, 2005). Однако подавляющее большинство таких продуктов рассматривают только риски, связанные с компьютерной подсистемой информационной инфраструктуры компании, оставляя в стороне бумажный документооборот, проблему защиты информации при телефонных и личных переговорах, а также другие процессы в организации, в ходе которых происходит передача, обработка или хранение информации. Кроме того, такие программные продукты в своей работе используют лишь общие рекомендации по защите компьютерных сетей и часто не учитывают конкретных особенностей информационной инфраструктуры фирмы.

В последнее время руководители высшего звена начинают уделять больше внимания вопросам обеспечения информационной безопасности на предприятии, осознавая важность данной проблемы. Однако далеко не всегда они могут обоснованно оценить уровень денежных средств, необходимый для решения задач информационной безопасности. Не менее важным является распределение данных средств между отдельными задачами обеспечения защиты информации. Эта проблема, как правило, решается исключительно на основе интуитивных предположений руководителей подразделений без опоры на формальное обоснование экономической целесообразности данного решения.

Таким образом, имеет большое научно-практическое значение построение методики расчета уровня информационного риска в зависимости от общего объема и распределения денежных средств, выделяемых на обеспечение информационной безопасности в организации. Несмотря

на большое разнообразие методик анализа и управления информационными рисками, можно выделить общую для них последовательность этапов:

– инвентаризация и классификация информационных ресурсов компании;

– определение перечня угроз, актуальных для исследуемой информационной системы;

– оценка вероятности реализации угроз и уровня риска для отдельных информационных ресурсов;

– построение интегральной оценки уровня риска для информационной системы в целом;

– разработка рекомендаций по управлению информационными рисками.

В предлагаемой методике будет сохранена общая последовательность этапов, однако ряд стандартных решений претерпит некоторые изменения, которые в дальнейшем позволят математически строго сформулировать задачу оптимизации расходов на информационную безопасность.

1. ИНВЕНТАРИЗАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Для решения задач безопасности независимо от области, в которой они возникают, в первую очередь нужно определить перечень защищаемых объектов. В данном случае при анализе информационных рисков необходимо создать максимально полный список информационных ресурсов, подлежащих защите. Следует помнить о том многообразии форм, в которых может существовать информация. Большинство существующих методик рассматривает лишь информацию, хранение и обработка которой осуществляется с помощью средств вычислительной техники. Однако данный подход крайне узок и не учитывает риски, связанные с информацией, представленной в других формах.

В данной статье под информацией будем понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Федеральный закон № 24-ФЗ, 1995). Информационным объектом будем называть некоторый объем информации, объединенной по времени, месту и форме ее представления. Такое определение позволяет исследовать все многообразие информации, циркулирующей на фирме (электронные и бумажные документы; служебная переписка; устные переговоры и совещания, на которых обсуждается информация, касающаяся деятельности компании, и т.п.), и может содержать сведения, критичные для деятельности организации.

2. ОПРЕДЕЛЕНИЕ УГРОЗ

С точки зрения безопасности выделяют три основных свойства информации (Девянин, 2005; Information Technology, 1991).

1. Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

2. Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

3. Конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.

В соответствии с этими свойствами под безопасностью информации понимается защищенность информации от нарушений конфиденциальности (нежелательного разглашения информации), целостности (искажения информации), доступности (утраты или снижения степени доступности информации). Таким образом, будем выделять три основные угрозы безопасности информации: угроза конфиденциальности, угроза целостности и угроза доступности информации.

В рамках данной статьи остановимся на этом списке угроз, однако при проведении полномасштабного исследования приведенная классификация может быть расширена и уточнена. Так, например, угроза конфиденциальности может быть разделена на ряд подпунктов: угроза конфиденциальности информации со стороны внешнего нарушителя (предполагает проникновение стороннего человека с целью хищения информации) или со стороны внутреннего нарушителя (разглашение конфиденциальной информации сотрудником организации) и т.п. Перечень угроз

будет зависеть от того, какая именно информация требует защиты, от модели нарушителя, а также глубины проводимого анализа. Кроме того, следует отметить, что угрозы должны выбираться таким образом, чтобы они были независимы друг от друга, что значительно упростит дальнейшие вычисления.

После этого делается возможным проведение классификации информационных объектов для объединения их в блоки с целью снижения трудоемкости дальнейших вычислений. Так, в один блок можно поместить документы, имеющие сходство по виду носителя, структуре, технологии обработки, тематике, типу сведений и т.п. Важным параметром при классификации информационных объектов будут требования к их защищенности от всех выделенных типов угроз. Например, бухгалтерская информация, хранящаяся на бумажных носителях и в памяти ЭВМ, будет относиться к двум разным информационным блокам, так как вероятность реализации угроз для них будет разной. Следует помнить, что такое разбиение информации на блоки не является окончательным и может быть пересмотрено в дальнейшем.

После того как определены все рассматриваемые информационные объекты (блоки) и создан полный перечень угроз, можно переходить к оценке информационных рисков.

3. ОПРЕДЕЛЕНИЕ РИСКОВ

В общем случае риск определяется как “сочетание вероятности нанесения ущерба и тяжести этого ущерба” (ГОСТ Р 51898-2002, 2002; Jack, 2006). Однако такой подход является достаточно общим и не отражает особенностей рассматриваемой предметной области. Также информационный риск можно определить как ожидаемые потери или возможный результат реализации угрозы при существовании уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы (Петренко, Симонов, 2005).

В рамках данной статьи под информационным риском будем понимать математическое ожидание финансовых потерь при реализации некоторой угрозы (группы угроз) для рассматриваемого информационного объекта (набора объектов) (Хрусталев, 2005). Это позволит дать количественную оценку риска, что крайне важно для дальнейшей аналитической обработки результатов.

Пусть денежные потери от реализации угрозы для некоторого информационного объекта описываются случайной величиной ξ, которая имеет дискретное распределение и принимает значения 0 и A с вероятностями $1-p$ и p, соответственно (где A – величина денежных потерь организации при реализации рассматриваемой угрозы для информационного объекта; p – вероятность реализации рассматриваемой угрозы для информационного объекта).

Величина A определяется методом экспертных оценок и должна максимально полно включать в себя все денежные убытки, возникающие при реализации угрозы (финансовые потери, связанные с восстановлением информационного ресурса и информационной инфраструктуры или с нарушением деятельности организации; ущерб репутации организации; ущерб от разглашения конфиденциальной информации и персональных данных и т.д.).

В большинстве существующих методик вероятность p реализации угрозы рассматривается как статическая величина, определяемая экспертом (группой экспертов). Однако такой подход существенно ограничивает возможность использования данной оценки для анализа. Величина p зависит от значительного числа факторов (особенностей функционирования организации, уровня квалификации сотрудников, отвечающих за обеспечение режима информационной безопасности, объема финансирования мероприятий по защите информации и т.п.). Как правило, эти факторы являются либо неизменными, либо носят исключительно технический характер.

Особое место занимает размер денежных средств, выделяемых на информационную безопасность, и их распределение между отдельными задачами. Именно этот вопрос зачастую является слабым звеном во взаимодействии подразделений, занимающихся вопросами информационной безопасности, и руководства компании. В большинстве случаев начальники подразделений безопасности не могут обосновать с экономической точки зрения необходимость выделения конкретных сумм на вопросы обеспечения безопасности и наглядно представить эффект, который будет получен от вложения данных денежных средств в защиту информации.

Практика показывает, что существует явная зависимость вероятности реализации угрозы от объема денежных средств, выделяемых на мероприятия по защите рассматриваемого информационного ресурса от некоторой угрозы. Таким образом, представим p в виде $p=f(x)$, где x – объем денежных средств, выделенных на реализацию мероприятий по обеспечению защиты информационного ресурса от некоторой угрозы; $f(x)$ – функция, описывающая вероятности реализации

угрозы для некоторого информационного ресурса в зависимости от объема средств, вкладываемых в мероприятие по ее предотвращению. Для этой функции должно выполняться неравенство $0 \le f(x) \le 1$. Таким образом, в соответствии с ранее введенным определением значение риска для некоторого ресурса будет иметь вид $P(x) = M\xi = Af(x)$.

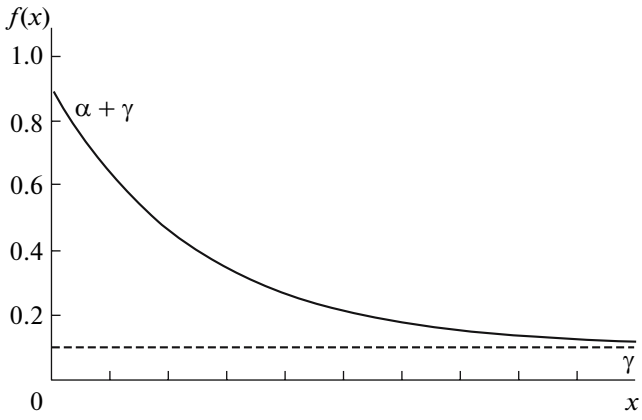

Рис. 1.

По мнению экспертов (Петренко, Симонов, 2005; Баутов, 2002; Бурдин, Кононов, 2002), в большинстве случаев с увеличением объема ассигнований вероятность реализации угрозы снижается по экспоненциальному закону (рис. 1), т.е. $f(x)$ имеет вид $f(x) = \alpha e^{-\beta x} + \gamma$, где α, β, γ – некоторые параметры, характеризующие зависимость вероятности реализации угрозы для некоторого информационного ресурса от объема средств, вкладываемых в мероприятие по ее предотвращению.

Параметр γ показывает минимальную вероятность реализации угрозы, к которой стремится $f(x)$ при увеличении объема выделяемых денежных средств. Параметр β характеризует скорость снижения вероятности реализации угрозы при увеличении ассигнований на мероприятия по ее пресечению и определяет эффективность вложения денежных средств. Параметр α – масштабирующий и выбирается так, чтобы значение функции $f(0) = \alpha + \gamma$ соответствовало вероятности реализации угрозы в случае, если средства на защиту не выделяются.

При этом должны выполняться условия: $\alpha, \beta, \gamma \ge 0$, $\alpha + \gamma \le 1$. Значения параметров α, β, γ могут выбираться из заранее созданной базы данных, основанной на результатах статистических наблюдений, или определяются путем экспертных оценок. Данный этап является наиболее трудоемким в рассматриваемой методике и требует привлечения высококвалифицированных специалистов.

В отдельных случаях могут иметь место некоторые другие виды зависимостей, однако в рамках данной статьи они не будут рассматриваться отдельно, так как все дальнейшие операции в этих случаях будут проводиться схожим образом.

Приведенную выше методику оценки рисков следует применить к каждой паре "информационный блок – угроза", которые были построены на этапах инвентаризации и определения угроз. Результаты удобно представить в виде табл. 1, где A_{ij} – величина денежных потерь организации при реализации угрозы j для информационного блока i; $f_{ij}(x)$ – функция, описывающая вероятность реализации угрозы j для информационного блока i в зависимости от объема средств, вкладываемых в мероприятие по ее предотвращению; x_{ij} – объем денежных средств, выделенных на реализацию мероприятий по обеспечению защиты информационного блока i от некоторой угрозы j. Далее в соответствии с этими данными рассчитаем значение риска для каждой пары "информационный блок – угроза" (табл. 2).

Оценив уровень риска для каждой пары "информационный блок – угроза", перейдем к определению интегрального уровня риска для информационной системы в целом. Рассмотрим случайную величину ξ, описывающую суммарный размер денежных потерь организации от реализации различных информационных угроз. Так как в соответствии с методикой информационные блоки не пересекаются друг с другом, то при одновременной реализации нескольких угроз для некоторого набора информационных блоков общий объем убытков будет равен сумме потерь от

Таблица 1

Информационные блоки	Угроза 1	…	Угроза n
Информация 1	$A_{11}, f_{11}(x), x_{11}$	…	$A_{1n}, f_{1n}(x), x_{1n}$
…	…	…	…
Информация m	$A_{m1}, f_{m1}(x), x_{m1}$	…	$A_{mn}, f_{mn}(x), x_{mn}$

Таблица 2

Информационные блоки	Угроза 1	…	Угроза n
Информация 1	$M\xi_{11}$	…	$M\xi_{1n}$
…	…	…	…
Информация m	$M\xi_{m1}$	…	$M\xi_{mn}$

реализации отдельных угроз для конкретных информационных блоков (Дубров, Лагоша, Хрусталев, Барановская, 2001). То есть величина ξ равна сумме случайных величин ξ_{ij}, каждая из которых описывает потери от реализации конкретной угрозы для определенного информационного блока: $\xi = \sum_{i,j} \xi_{ij}$.

В этом случае математическое ожидание случайной величины ξ будет равно сумме математических ожиданий ξ_{ij}: $M\xi = \sum_{i,j} M\xi_{ij}$. Таким образом, получаем денежное выражение значения риска для организации в целом. В дальнейшем данное значение может быть использовано в качестве критерия при принятии решений о выделении финансирования на обеспечение информационной безопасности, при планировании возможных расходов, а также при рассмотрении вопросов страхования от информационных рисков (Лавринов, Хрусталев, 2005).

Кроме того, на основании данных, представленных в табл. 2, можно выявить наиболее опасные участки информационной инфраструктуры предприятия, т.е. информационные блоки и угрозы, для которых значение риска будет превышать некий заранее определенный допустимый уровень. Обладая такими данными, можно предельно четко сформулировать наиболее важные направления реорганизации системы информационной безопасности с тем, чтобы снизить уровень риска до приемлемого значения.

4. РЕШЕНИЕ ЗАДАЧИ ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ, ВЫДЕЛЯЕМЫХ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Следующим этапом является решение задачи оптимизации, целью которой будет нахождение эффективного распределения денежных средств, выделенных на информационную безопасность. Задача оптимизации имеет вид: найти такое распределение денежных средств, выделенных на информационную безопасность, при котором значение информационного риска для организации в целом будет минимально.

В качестве целевой функции выберем функцию, описывающую значение информационного риска для организации в целом

$$\sum_{i,j} A_{ij} f_{ij}(x_{ij}) \longrightarrow \min.$$

Рассмотрим ограничения на значения аргументов данной функции, которые необходимо учесть при решении задачи: значения аргументов x_{ij} должны быть неотрицательными, а их сумма не должна превосходить общего объема денежных средств D, выделенных на информационную безопасность:

$$x_{ij} \geq 0, \quad \sum_{i,j} x_{ij} \leq D.$$

Таким образом, задача оптимизации примет вид:

$$\sum_{i,j} A_{ij} f_{ij}(x_{ij}) \longrightarrow \min,$$

$$\begin{cases} \sum_{i,j} x_{i,} \leq D, \\ x_{ij} \geq 0. \end{cases}$$

Задача относится к классу задач нелинейного программирования с линейными ограничениями, для решения которых разработан целый ряд различных методов. В данном случае необходимо использовать методы условной оптимизации (например, метод Зойтендейка, метод условного градиента Франка–Вульфа и др. (Андронов, 2001; Смородинский, Батин, 2003; Химмельблау, 1975)). Решение данной задачи позволит эффективно распределить средства между отдельными направлениями и добиться минимально возможного уровня риска при данном объеме финансирования.

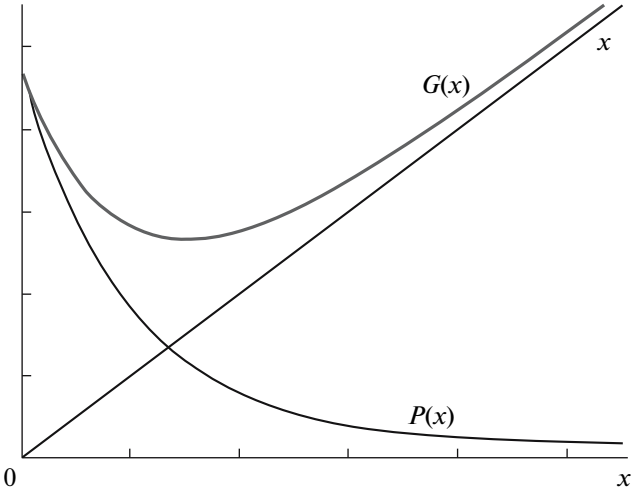

Рис. 2.

В некоторых организациях могут существовать требования по уровню безопасности для отдельных информационных объектов. Как правило, такие требования задают максимально приемлемую вероятность реализации определенной угрозы для некоторого перечня информационных объектов. Подобные ограничения также могут быть учтены при решении задачи оптимизации. В этом случае необходимо добавить дополнительные условия, которые будут задавать ограничения сверху на функции вероятности реализации угроз $f_{ij}(x)$, соответствующие парам "угроза – информационный блок": $f_{ii}(x_{ii}) < b_{ii}$, где b_{ii} – максимально допустимый уровень вероятности реализации угрозы j для информационного блока i.

На первый взгляд, решение такой задачи существенно усложняется, так как дополнительно введенные ограничения являются нелинейными. Однако ввиду того, что все рассматриваемые функции $f_{ij}(x)$ монотонно невозрастающие, такие условия могут быть легко приведены к линейному виду $x_{ij} \geq f_{ij}^{-1}(b_{ij})$, где f_{ij}^{-1} – функция обратная к f_{ij}. В этом случае при решении задачи оптимизации $f_{ij}^{-1}(b_{ij})$ будет являться фиксированным числом. Тогда задача оптимизации будет иметь вид:

$$\sum_{i,j} A_{ij} f_{ij}(x_{ij}) \longrightarrow \min,$$

$$\begin{cases} \sum_{i,j} x_{ij} \leq D, \\ x_{ij} \geq f_{ij}^{-1}(b_{ij}), \\ x_{ij} \geq 0. \end{cases}$$

Таким образом, задача возвращается в класс задач нелинейного программирования с линейными ограничениями, а значит, к ней могут быть применены ранее указанные методы. Однако следует помнить, что решение данной задачи может существенно отличаться от решения, найденного в условиях отсутствия дополнительных ограничений.

5. РЕШЕНИЕ ЗАДАЧИ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОГО ОБЪЕМА ДЕНЕЖНЫХ СРЕДСТВ, ВЫДЕЛЯЕМЫХ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Еще одной задачей, которая становится доступной для решения с использованием построенной модели, является задача нахождения экономически обоснованного объема денежных средств, необходимого для обеспечения информационной безопасности. Очевидно, что общие затраты на информационную безопасность будут складываться из непосредственных расходов (x) на проведение мероприятий по защите информации x, а также значений информационного риска $P(x)$, которые показывают размер денежных средств, для компенсации возможного ущерба. Таким образом, в общем виде функция общих затрат будет иметь вид $G(x) = P(x) + x$ (рис. 2).

Следовательно, для нахождения экономически оправданного уровня финансирования нужно решить задачу оптимизации, где функция общих затрат $G(x)$ будет критерием оптимизации, а условие неотрицательности переменных x_{ij} – единственным ограничением:

$$\sum_{i,j}(A_{ij}f_{ij}(x_{ij}) + x_{ij}) \longrightarrow \min,$$

$$x_{ij} \geq 0.$$

Данная задача так же, как и предыдущая, относится к классу задач нелинейного программирования, и к ней можно применить аналогичные методы.

Решение данной задачи позволит определить оптимальный объем финансирования, выделяемого на информационную безопасность. Полученные результаты могут подтвердить обоснованность текущего уровня финансирования информационной безопасности или предоставить рекомендации по его корректировке. Если полученное значение оказывается меньше общего объема денежных средств, выделенных на защиту информации, может быть рассмотрен вопрос о снижении уровня финансирования отдельных статей бюджета на информационную безопасность. Если результат вычислений превосходит текущий уровень затрат, необходимо поставить вопрос об увеличении объема средств, выделяемых на информационную безопасность, что позволит существенно снизить уровень риска, а значит, и расходы, связанные с негативными последствиями реализации угроз.

ЗАКЛЮЧЕНИЕ

Построенная математическая модель оценки информационного риска наглядно демонстрирует зависимость уровня риска от объема денежных средств, выделяемых на информационную безопасность. Модель позволяет по-новому подойти к ряду задач анализа и управления информационными рисками. Методика, построенная на основе данной модели, позволяет:

– проводить оценку текущего уровня информационного риска;

– находить оптимальное распределение денежных средств, выделенных на обеспечение информационной безопасности между отдельными задачами;

– определять экономически обоснованный уровень финансирования, выделяемого на защиту информации.

Отметим, что создание подобной модели для конкретной организации является достаточно трудоемким делом и требует привлечения высококвалифицированных специалистов. Кроме того, ввиду изменений, вносимых в политику безопасности, внедрения новых механизмов защиты, а также трансформации угроз информационным ресурсам, модель может потребовать пересмотра. Однако своевременное внесение в нее соответствующих незначительных корректировок позволит поддерживать ее в актуальном состоянии в течение достаточно продолжительного времени.

СПИСОК ЛИТЕРАТУРЫ

Андронов С.А. (2001): Методы оптимального проектирования. СПб.: СПбГУАП.

Баутов А.Н. (2002): Экономический взгляд на проблемы информационной безопасности // *Открытые системы*. № 2.

Бурдин О.А., Кононов А.А. (2002): Комплексная экспертная система управления информационной безопасностью “АванГард” // *Информационное общество*. Вып. 3.

Девянин П.Н. (2005): Модели безопасности компьютерных систем. М.: Издательский центр “Академия”.

Дубров А.М., Лагоша Б.А., Хрусталев Е.Ю., Барановская Т.П. (2001): Моделирование рисковых ситуаций в экономике и бизнесе. М.: Фин. и стат.

Лавринов Г.А., Хрусталев Е.Ю. (2005): Управление рисками при проектировании и производстве продукции военного назначения. М.: ЦЭМИ РАН.

Петренко С.А., Симонов С.В. (2005): Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс.

Смородинский С.С., Батин Н.В. (2003): Оптимизация решений на основе методов и моделей математического программирования. Минск: БГУИР.

Химмельблау Д. (1975): Прикладное нелинейное программирование. М.: Мир.

Хрусталев Е.Ю. (2001): Планирование информационной безопасности предприятия. II Всероссийский симпозиум "Стратегическое планирование и развитие предприятий". М.: ЦЭМИ РАН.

Хрусталев Е.Ю. (2005): Метод оценки рисков при создании наукоемкой продукции // *Финансовый бизнес*. № 4.

Федеральный закон "Об информации, информатизации и защите информации" от 20.02.1995 г. № 24-ФЗ с изменениями от 10.01.2003 г.

ГОСТ Р 51898-2002 "Аспекты безопасности. Правила включения в стандарты" от 05.06.2002 г.

Jack A.J. (2006): An Introduction to Factor Analysis of Information Risk (FAIR): A Framework for Understanding, Analyzing, and Measuring Information Risk // *Norwich University Journal of Information Assurance*. Issue 2. Vol. 1.

Information Technology (1991): Information Technology Security Evaluation Criteria (ITSEC). Luxembourg, Brussels: Office for Official Publications of the European Communities.

Поступила в редакцию
05.07.2007 г.

Application of the Optimization Methods for the Analysis and Control of the Information Risks

V. V. Nemitkina

The article describes the mathematical model of correlation between the information risk and the amount of financing the information security measures. A model is the basis for optimization the task of allocation of the finance between the separate measures of protecting the information to lower the general risk. The author proposes a model of optimal economic amount of financing to provide information security.