Модели и методы управления киберрисками многофакторного ущерба

А. Б. Вольфтруб, А. К. Поликарпов

Проблема управления рисками информационной безопасности не нова. В современном мире информация является одной из важнейших основ любого бизнес-процесса. Теория защиты информации вводит понятия риска нарушения информационной безопасности и управления рисками, т. е. прогнозирования и оценки влияния того или иного риска на систему, а также определение мер, позволяющих минимизировать его.

Для автоматизации решения подобных задач разрабатываются различные программные комплексы. Математическая модель, описываемая в этой статье, реализована в системе автоматизации управления рисками «АванГард», разработанной в Институте системного анализа РАН [1–6]. Этот программный комплекс успешно используется различными предприятиями. Статья описывает один из методов используемых для оценки рисков, а также определяет направление дальнейших исследований в этой области.

Используемые термины и определения

Описываемые в статье методы применяются для управления рисками в компьютерных автоматизированных информационных системах, поэтому термины «система», «риск», «технология», «компонент», «объект» следует рассматривать в применении к данной области.

Преимущества компьютерных технологий очевидны. Вместе с тем нужно четко понимать, что их использование порождает и новые риски, которые необходимо знать и оценивать, добиваясь их снижения. Риски могут возникать в связи с тем, что технологии недостаточно надежны, уязвимы и/или применяются с нарушением правил (требований) их безопасного использования. Особенно важно учитывать эти риски при внедрении новых технологий в критические, т. е. жизненно важные для организации, а также для ее партнеров или клиентов системы и процессы.

Основной особенностью рисков, связанных с использованием компьютерных систем, является невозможность в большинстве случаев использовать аппарат теории вероятностей для их оценки, поскольку процессы,

обуславливающие их существование, как правило, не являются стохастическими. Оценить подобные риски и управлять ими можно только отслеживая причинно-следственные связи их возникновения.

Каждый отдельно взятый риск есть результат некоторого возможного события нарушения безопасности системы, ***события риска***, приводящего к определенному ущербу.

Для оценки значений ущерба, а также вероятности наступления события риска удобно использовать ранговые шкалы.

Использование ранговых шкал позволяет перейти от понятия материального ущерба к понятию оценки опасности (нежелательности) события риска. При этом те события рисков, для которых вся опасность сводится к материальному ущербу, могут использоваться для построения базовой шкалы в денежных единицах. В дальнейшем можно абстрагироваться от того, что в качестве исходной метрики при построении шкалы ранжирования использовались денежные величины, и проставленные оценки по событиям риска воспринимать исключительно как значения опасности этих событий рисков. Очевидно, что в предлагаемом методе ранжирования закладывается определенный верификационный механизм коррекции оценок, поскольку указание степени риска для каждого вновь определяемого события риска требует фактически подтверждения целой системы утверждений о том, что каждое событие риска, находящееся по шкале ниже определяемого, менее опасно, а каждое находящееся выше — более опасно, чем определяемое. В случае если это не так, требуется пересмотр всех тех оценок, для которых это требование не выполняется.

Ранговая шкала вероятности событий риска имеет аналогичную систему верификации.

Еще большую надежность методу придает возможность для экспертов знакомиться с результатами по оценке опасностей и вероятностей событий рисков, которые сделали другие эксперты, и приходить к некоторому консолидированному мнению (метод Делфи).

Величиной риска будем считать результат произведения оценки опасности события риска на оценку вероятности этого события.

Все события рисков могут быть представлены как результат реализации некоторого множества угроз, связанных с недостаточным уровнем безопасности используемых технологий. Каждую из угроз в свою очередь всегда можно ассоциировать с каким-либо компонентом. Таким образом, для принятия решений по повышению безопасности необходимо выделить все компоненты, с которыми могут быть ассоциированы те или иные рискообразующие угрозы, и рассчитать «вклад» каждого из компонентов в формировании этого риска.

Представим формальную схему решения указанной задачи. Пусть дана некоторая организационная система **S**, которая может быть представле-

на в виде некоторого множества составляющих ее компонент $\mathbf{O}_{i^s}$, где $i^s \in I^{\mathbf{S}}$, $I^{\mathbf{S}}$ — множество индексов всех компонентов **S**:

$$\mathbf{S} = \left\{ \mathbf{O}_{i^s} \right\}. \tag{1}$$

Компоненты, с которыми невозможно связать какие-либо угрозы безопасности системе **S**, нас не интересуют и могут в эту модель не включаться.

Как правило, любая система может быть структурирована таким образом, что в ней могут быть выделено несколько, скажем **J** уровней иерархии. Часть системы, относимую к *j*-му уровню иерархии, обозначим как $\mathbf{S}^j$, $j \in \mathbf{J}$. При этом уровень системы в целом будет соответствовать 1-му уровню иерархии. А низший уровень иерархии будет *j*-м. В этом случае система может быть представлена, в виде структурной модели:

$$\mathbf{S} = \left\{ \mathbf{O}^j_{i^s} \right\}, \tag{2}$$

где верхний индекс *j* указывает иерархический уровень, на котором находится компонент. В дальнейшем этот индекс используется в нотации только в тех случаях, когда иерархическое положение компонента имеет значение.

Помимо того, что отдельные компоненты, определенные на множестве $\left\{ \mathbf{O}^j_{i^s} \right\}$, могут принадлежать к разным иерархическим уровням, существует условие, что если компонент находится на более высоком уровне иерархии, он может включать себя компоненты более низкого иерархического уровня: $\mathbf{O}^j_{i^s} \supset \left\{ \mathbf{O}^{j+1}_{i^O} \right\}$, $i^o \in \mathbf{I}^{\mathbf{O}^j_{i^s}}$, где $\mathbf{I}^{\mathbf{O}^j_{i^s}}$ — множество индексов компонентов *j* + 1-го уровня иерахии, входящих в состав компонента $\mathbf{O}^j_{i^s}$.

Например, назовем объектами компоненты низшего уровня иерархии и предположим, что они могут быть объединены в подсистемы. Для подсистем, в свою очередь, могут быть определены свои множества угроз. Любая из угроз, входящих в любое из этих множеств, не может быть отнесена ни к одному из объектов, входящих в какую-либо подсистему, а лишь к подсистеме в целом. Подсистемы могут быть объединены в более крупные группы, например, по признаку их местоположения, в локальные среды (ЛС), и для ЛС, в свою очередь, могут существовать угрозы, которые невозможно отнести ни к одной из входящих в них подсистем или объектов. И так далее, до уровня системы в целом. Если для всей системы в целом

может быть определено, некоторое множество угроз, которое не может быть отнесено ни к одной из ее компонент в отдельности от других, то в этом случае сама система должна быть идентифицирована в качестве компонента множества $\mathbf{O}_{i^S}$. Все множество угроз $\mathbf{Y}^{\mathbf{S}}$, связанных с системой **S** и со всеми ее компонентами, может быть представлено как

$$\mathbf{Y}^{\mathbf{S}} = \{\mathbf{Y}^{\mathbf{O}_{i^S}}\}. \qquad (3)$$

Каждому объекту $\mathbf{O}_{i^S}$ сопоставляется некоторое множество угроз $\mathbf{Y}^{\mathbf{O}_{i^S}}$. Таким образом, множество $\mathbf{Y}^{\mathbf{S}}$ представляет собой ничто иное, как модель угроз для системы **S**.

Будем отличать множество $\mathbf{Y}^{\mathbf{S}}$ от множества $\mathbf{Y}^{K\mathbf{S}}$, которое представляет собой каталог всех угроз системы **S**, и отличается от множества $\mathbf{Y}^{\mathbf{S}}$ тем, что любая угроза в множестве $\mathbf{Y}^{K\mathbf{S}}$ не связана с конкретным объектом системы **S**, и множество $\mathbf{Y}^{\mathbf{S}}$ может быть получено из $\mathbf{Y}^{K\mathbf{S}}$ путем выполнения процедуры $\Pi^{\mathbf{Y}^{\mathbf{S}}}$ построения модели угроз системы на основе множества **S**: $\Pi^{\mathbf{Y}^{\mathbf{S}}}\left(\mathbf{S}, \mathbf{Y}^{\mathbf{KS}}\right) \to \mathbf{Y}^{\mathbf{S}}$.

Определим для системы **S** множество возможных событий риска $\mathbf{R}^{\mathbf{S}}$ нарушения ее безопасности. Если множество $\mathbf{Y}^{\mathbf{S}}$ определено достаточно полно, то любое событие $r_{i^R} \in \mathbf{R}^{\mathbf{S}}$ ($i^R \in \mathbf{I}^{\mathbf{R}}$, $\mathbf{I}^{\mathbf{R}}$ — множество индексов событий рисков, входящих в множество $\mathbf{R}^{\mathbf{S}}$) может быть представлено как результат реализации некоторого множества угроз $\mathbf{Y}^{r_{i^R}} \in \mathbf{Y}^{\mathbf{S}}$.

Каждое событие риска r_{i^R} имеет три основных количественных характеристики: c_{i^R} — цену риска — оценку ущерба, который может быть нанесен системе **S** событием риска r_{i^R}, p_{i^R} — вероятность события риска r_{i^R} и w_{i^R} — величину риска, рассчитываемую по формуле:

$$w_{i^R} = c_{i^R} \times p_{i^R}. \quad (4)$$

При этом важно отметить, что вероятность p_{i^R} события риска r_{i^R} может быть рассчитана как произведение вероятностей реализации каждой из угроз множества $\mathbf{Y}^{r_{i^R}}$:

$$p_{i^R} = \prod_{x=1}^{X^{r_{i^R}}} p_x^{r_{i^R}}, \quad (5)$$

где $X^{r_{i^R}}$ — количество угроз множества $\mathbf{Y}^{r_{i^R}}$.

Каждое из возможных событий риска, в силу самой возможности их реализации с указанными выше параметрами, привносит в систему потенциал риска и, таким образом, обладает тем, что далее предлагается называть ***рискообразующим потенциалом***. Поскольку событие риска есть результат одновременной реализации множества угроз $\mathbf{Y}^{r_{i^R}}$, то можно говорить о том, что это множество угроз в рамках системы **S** обладает совокупным рискообразующим потенциалом w_{i^R}. Рискообразующий потенциал каждой из угроз, входящих в множество $\mathbf{Y}^{r_{i^R}}$, предлагается рассчитывать по формуле:

$$q_{i^R} = \frac{w_{i^R}}{X^{r_{i^R}}}. \quad (6)$$

Эта формула справедлива постольку, поскольку отражает тот факт, что если бы хотя бы одна из угроз не была реализована, то событие риска r_{i^R} не произошло. То есть не было бы никакого события риска, либо это было бы совсем другое событие, с совершенно иными показателями цены риска, вероятности этого события и величины риска по этому событию. Поэтому естественно предположить, что «вклад» каждой угрозы из множества $\mathbf{Y}^{r_{i^R}}$, характеризуемый ее рискообразующим потенциалом по данному событию, одинаков и может быть рассчитан по формуле (6).

При построении моделей всех событий из множества $\mathbf{R}^{\mathbf{S}}$ любая из угроз y_{i^Y} ($i^Y \in \mathbf{I}^{\mathbf{Y}}$, $\mathbf{I}^{\mathbf{Y}}$ — множество индексов угроз, входящих в множество $\mathbf{Y}^{\mathbf{S}}$) из множества $\mathbf{Y}^{\mathbf{S}}$ могла войти в качестве рискообразующей в некоторое подмножество $\mathbf{R}^{i^y}$ множества моделей событий риска $\mathbf{R}^{\mathbf{S}}$. Соответственно, для нее может быть определено множество $\mathbf{Q}^{i^y}$ значений ее рискообразующего потенциала по каждому из событий рисков, в число рискообразующих угроз которых она входит.

В принципе, как правило, может быть построено неограниченно большое количество моделей событий риска, в которых каждая из угроз играет какую-то рискообразующую роль, но с точки зрения решения задачи управления рисками имеют значение только такие модели риска, которые помогают определить реальную значимость той или иной угрозы нарушения безопасности системы **S**. Очевидно, что реальная значимость угрозы y_{i^Y} – ее ***системный рискообразующий потенциал*** $q^{i^Y S}$ — определяется максимальным значением ее рискообразующего потенциала по всем моделям рисков множества $\mathbf{R}^{i^y}$:

$$q^{i^Y S} = \max \mathbf{Q}^{i^Y} . \tag{7}$$

Постольку поскольку каждая из угроз соотнесена с некоторым компонентом системы **S** и каждому из компонентов $\mathbf{O}_\text{i}$ соответствует множество угроз $\mathbf{Y}^{\mathbf{O}_i} = \left\{ y_{i\mathbf{O}}, i^{\mathbf{O}} \in \mathbf{I}^{\mathbf{O}} \right\}$, то для любого из объектов $\mathbf{O}_\text{i}$, который не включает в себя компонентов более низкого уровня иерархии, рискообразующий потенциал $q^{\mathbf{O}_i}$ рассчитывается по формуле:

$$q^{\mathbf{O}_i} = \sum_{}^{\mathbf{I}^{\mathbf{O}}} q_{i\mathbf{O}}^{S} , \tag{8}$$

где $q_{i\mathbf{O}}^{S}$ — системный рискообразующий потенциал угрозы $y_{i\mathbf{O}} \in \mathbf{Y}^{\mathbf{O}i}$.

Если компонент $\mathbf{O}_\text{i}$ j-го иерархического уровня включает в себя множество компонентов $j+1$ уровня иерархии $\mathbf{O}_i^j \supset \{\mathbf{O}_{iz}^{j+1}, z \in \mathbf{Z}^{\mathbf{O}_i^j}\}$, то его рискообразующий потенциал $q^{\mathbf{O}_i^j}$ рассчитывается как сумма рискооб-

разующего потенциала угроз для этого компонента и сумма рискообразующих потенциалов компонентов, входящих в его состав:

$$q^{\mathbf{O}_i^j} = \sum^{\mathbf{I}^{\mathbf{O}}} q_{i^{\mathbf{O}}}^{S} + \sum^{\mathbf{Z}^{\mathbf{O}_i^j}} q_z^{\mathbf{O}_i^{j-1}}, \qquad (9)$$

где $q_z^{\mathbf{O}_i^{j-1}}$ — рискообразующий потенциал компонента $\mathbf{O}_{iz}^{j+1} \subset \mathbf{O}_i^j$.

Таким образом, если учесть, что в предлагаемой системе понятий оценка риска по компоненте есть ни что иное, как ее рискообразующий потенциал, а в качестве компоненты может рассматриваться как любая часть (подсистема), так и система в целом, то формула (9) является общей формулой для расчета оценок риска для системы **S** и всех ее частей (подсистем).

Меры защиты, модель защиты, рископонижающий потенциал

Для каждой угрозы $Y_{i^y} \in \mathbf{Y}^{\mathbf{S}}$ (где $i^y \in \mathbf{I}^y$, $\mathbf{I}^y$ — множество индексов угроз, составляющих $\mathbf{Y}^{\mathbf{S}}$) может быть определено множество известных для этой угрозы мер противодействия (или мер защиты) $\mathbf{M}_{i^y}^{Y}$.

Множество всех известных мер защиты от каждой из угроз, входящих в множество $\mathbf{Y}^{\mathbf{S}}$, связанных с системой **S** и со всеми ее компонентами, может быть представлено как

$$\mathbf{M}^{\mathbf{S}} = \{\mathbf{M}_{i^y}^{Y}\}. \qquad (10)$$

Множество $\mathbf{M}^{\mathbf{S}}$ представляет собой модель защиты системы **S**.

Основной характеристикой меры защиты является ее способность снизить рискообразующий потенциал, существующий в системе **S.** Эту характеристику назовем ***рископонижающим потенциалом*** меры защиты.

Расчет рископонижающего потенциала меры защиты

Для того чтобы определить рископонижающий потенциал меры защиты, нужно построить ожидаемые модели воздействия этой меры на модели событий риска. Основными характеристиками таких моделей являются но-

вые прогнозируемые значения основных количественных характеристик события риска, происходящего в условиях, когда мера защиты применена.

Итак, событие риска $r_{i^R} \in \mathbf{R}^{\mathbf{S}}$ ($i^R \in \mathbf{I}^{\mathbf{R}}$, $\mathbf{I}^{\mathbf{R}}$ — множество индексов событий рисков, входящих в $\mathbf{R}^{\mathbf{S}}$) может быть представлено как результат реализации некоторого множества угроз $\mathbf{Y}^{r_{i^R}} \in \mathbf{Y}^{\mathbf{S}}$. Для каждой из угроз $y_{i^z}^{i^R} \in \mathbf{Y}^{r_{i^R}}, i^z \in \mathbf{I}^z$ ($\mathbf{I}^z$ — множество индексов угроз, входящих в $\mathbf{Y}^{r_{i^R}}$) может быть определено множество мер защиты $\mathbf{M}^{i_z}$.

При реализации меры защиты $m_{i_m} \in \mathbf{M}^{i_z}, i_m \in \mathbf{I}^{i_z}$ от угрозы $y_{i^z}^{i^R}$ значения цены риска, вероятности события риска и величины риска для события риска r_{i^R} могут измениться и принять соответственно значения $c_{i^R}^m$, $p_{i^R}^m$, $w_{i^R}^m$, где $w_{i^R}^m = c_{i^R}^m \times p_{i^R}^m$.

Величину $u^m = w_{i^k} - w_{i^k}^m$ назовем рископонижающим потенциалом меры m_{i_m} по событию риска r_{i^R}. Но если при применении меры защиты понижается величина риска по этому событию, то тогда в соответствии с выражением (6) понижаются и рискообразующие потенциалы всех угроз, реализация которых приводит к событию риска.

Предположим, что принимается некоторый комплекс мер $K_{i^K}^{\mathbf{S}}, i^K \in I^K$, где I^K — множество индексов возможных вариантов комплексов мер, $K_{i^K}^{\mathbf{S}} = \{M_{i^M}^{i^K}, i^M \in I^M\}$, I^M — множество индексов мер, входящих в комплекс $K_{i^K}^{\mathbf{S}}$.

Тогда применение комплекса мер $K_{i^K}^{\mathbf{S}}$ переводит множество событий рисков системы $\mathbf{R}^{\mathbf{S}}$ в новое состояние $\mathbf{R}^{\mathbf{S}^{K^i}}$. Что влечет за собой изменение уровней рискообразующих потенциалов по всем угрозам и объектам, рассчитываемым по формулам (7)–(9). Разница между старыми и новыми значениями рискообразующих потенциалов отдельных угроз и компонен-

тов разного уровня иерархии будет представлять собой величины рископонижающих потенциалов комплексов мер по соответствующей угрозе или компоненту.

Однако необходимо отметить, что указанные расчеты рископонижающих потенциалов и снижения уровней рисков по отдельным компонентам в результате реализации комплекса мер $K_{iK}^{\mathbf{S}}$ носят сугубо предварительный промежуточный характер по трем причинам.

Во-первых, после принятия любого комплекса мер $K_{iK}^{\mathbf{S}}$ может измениться вся система объектов, поскольку принятие мер, может повлечь за собой внедрение в систему определенных средств защиты, каждое из которых в принципе может обладать своим рискообразующим потенциалом, который тоже нужно оценить.

Во-вторых, принятие мер занимает определенный период времени, за этот период времени в системе могут произойти какие-то изменения в ее составе, кроме того, могут стать известны новые угрозы и построены модели новых событий рисков, которые могут произойти в случае реализации этих угроз.

В-третьих, при расчете величины системного рискообразующего потенциала каждой отдельной угрозы (формула (7)) было принято предположение, что невозможно рассмотреть все множество событий риска, к которым может привести реализация этой угрозы и рассматривались только, те события рисков, которые позволяли раскрыть максимальное значение значимости угрозы, предлагая игнорировать все те случаи, в которых реализация угрозы наносила меньший ущерб. Поэтому после того как были рассмотрены меры предусмотренные комплексом $K_{iK}^{\mathbf{S}}$ следует еще раз по каждой угрозе рассмотреть вариант ее реализации в таком событии риска, в котором ее значимость может быть повышена по отношению к той величине системного рискообразующего потенциала, что была по ней рассчитана по результатам применения комплекса мер $K_{iK}^{\mathbf{S}}$. То есть по каждой угрозе должно быть показано, что не существует события риска, в котором ее значимость может превысить ее текущий уровень ее системного рискообразующего потенциала с учетом того, что в системе будут реализованы меры предусмотренные комплексом $K_{iK}^{\mathbf{S}}$.

Таким образом, для того, чтобы оценить риски, которые будут существовать в системе мосле принятия комплекса $K_{iK}^{\mathbf{S}}$, следует вновь выполнить всю систему процедур предусмотренной при расчете формул (1)–(9).

Разделение показателя цены риска по составляющим ущерба

Каждое событие риска характеризуется его ценой. Оценивая величину риска, мы определяли ее как произведение цены риска на вероятность события риска

$$w_{iR} = c_{iR} \times p_{iR} .$$

Понятие цены риска c_{iR} весьма специфично и в большинстве случаев довольно неоднозначно. Наиболее часто под ценой риска понимают финансовые потери от наступления события риска. Однако действительные потери не всегда могут быть выражены финансовым эквивалентом. В некоторых случаях результатом наступления события риска является потеря репутации компании, потеря бизнес-партнера или упущенная возможность заключения выгодного контракта. Наконец, потери могут характеризоваться уменьшением производительности, сокращением рабочих мест, срывом сроков выполнения договоров и множеством других аспектов. Проанализировать все эти составляющие для представления их в виде финансового ущерба на этапе построения модели событий рисков для конкретной системы невозможно. Более того, в ряде случаев это даже нецелесообразно, поскольку иногда гораздо важнее оценить возможный ущерб по каждому показателю в отдельности, и в соответствии с этим подобрать наиболее оптимальный комплекс мер защиты.

Для учета различных ущербов построим в модели данных множество всех возможных составляющих ущерба. На этом этапе они не привязываются к конкретной анализируемой системе, а полученное множество представляет собой динамический каталог. Термин *динамический* в данном случае означает, что полученное множество может быть легко дополнено с учетом специфики конкретной анализируемой системы. Итак, получим множество возможных составляющих ущерба $C = \{c_i\}$, где $i \in I^C$ (I^C — множество индексов всех возможных составляющих ущерба).

На этапе анализа конкретной системы и построения для нее множества событий рисков R^S из множества C выбираем такое подмножество составляющих ущерба, которое имеет смысл для данной системы, и сопоставляем его с каждым событием риска, определенным для системы. При этом, если раньше для каждого события риска r_{iR} экспертами определялась общая цена риска, то сейчас цена определяется по каждому из множества выбранных для системы **S** составляющих ущерба. При необходимости на этом этапе имеющееся в модели множество C может быть расширено, исходя из специфики анализируемой системы. Следует отметить, что цены по каждой

составляющей ущерба определяются независимо друг от друга и в дальнейшем не суммируются, что избавляет нас от необходимости соотнесения всех оценок по некоторой общей шкале ранжирования. Кроме того, эти оценки могу выполняться независимо друг от друга различными экспертами.

Пусть $C^S = \{c_{i^S}\}$ — множество всех составляющих ущерба, определенных для системы **S**. Здесь $i^S \in I^S$ (I^S — множество индексов всех составляющих ущерба, определенных для системы **S**), при этом $C^S \subset C$.

Тогда для каждого события риска r_{i^R} наряду с вероятностью наступления события риска p_{i^R} определяется также множество $C^{i^R} = \{c^{i^R}_{i^S}\}$, где $i^S \in I^S$.

Величина риска рассчитывается для каждого ущерба в отдельности

$$w^{i^R}_{i^S} = c^{i^R}_{i^S} \times p_{i^R}. \quad (11)$$

Данная операция повторяется для всех $i^S \in I^S$. В результате для каждого события риска r_{i^R} получаем множество значений величины риска по каждому определенному в системе ущербу.

$$W^{i^R} = \{w^{i^R}_{i^S}\}. \quad (12)$$

Необходимо отметить, что оценить некоторые события риска по определенным составляющим ущерба довольно сложно, а влияние события риска на какой-либо ущерб может полностью отсутствовать. В этом случае значение цены риска по ущербу считается равным нулю. Тем самым обозначается, что данное событие риска не оказывает влияния на конкретную составляющую ущерба.

Справедливо лишь то, что для любого $\forall c_{i^S} \in C^S$ найдется хотя бы одно событие риска r_{i^R}, для которого $c^{i^R}_{i^S} \neq 0$.

Вводя понятие рискообразующего потенциала угрозы, мы определяли его как $q_{i^R} = \dfrac{w_{i^R}}{X^{r_{i^R}}}$, где $X^{r_{i^R}}$ — количество угроз множества $Y^{r_{i^R}}$, а $Y^{r_{i^R}}$, в свою очередь, множество угроз, одновременная реализация которых приводит к наступлению события риска r_{i^R}.

Рассчитывая значение величины риска по множеству составляющих ущерба, мы получаем множество рискообразующих потенциалов угрозы по каждому из ущербов

$$Q^{i^R} = \{q_{i^S}^{i^R}\}, \tag{13}$$

где

$$q_{i^S}^{i^R} = \frac{w_{i^S}^{i^R}}{X^{r_{i^R}}}. \tag{14}$$

Как уже отмечалось выше, при построении моделей всех событий рисков из множества $\mathbf{R^S}$ любая угроза y_{i^Y} ($i^Y \in \mathbf{I^Y}$, $\mathbf{I^Y}$ — множество индексов угроз системы) из множества $\mathbf{Y^S}$ может войти в качестве рискообразующей в некоторое подмножество $\mathbf{R}^{i^y}$ множества событий риска $\mathbf{R^S}$. Рискообразующий потенциал угрозы в этом случае представляет собой множество рискообразующих потенциалов по событиям риска Q^{i^y}.

Расчет величины риска для каждого определенного в системе ущерба приводит к тому, что для каждой угрозы мы получаем матрицу значений ее рискообразующих потенциалов

$$Q^{i^y} = \begin{Bmatrix} q_{1^S}^{1^R}, q_{2^S}^{1^R}, \mathsf{K}\, q_{n^S}^{1^R} \\ q_{1^S}^{2^R}, q_{2^S}^{2^R}, \mathsf{K}\, q_{n^S}^{2^R} \\ \mathsf{L}\ \mathsf{L}\ \mathsf{L}\ \mathsf{L}\ \mathsf{L}\ \mathsf{L} \\ q_{1^S}^{m^R}, q_{2^S}^{m^R}, \mathsf{K}\, q_{n^S}^{m^R} \end{Bmatrix}. \tag{15}$$

Здесь n — общее число составляющих ущерба, выбранных для системы **S**, а m — общее число событий риска, выделенных в системе **S**.

Системный рискообразующий потенциал угрозы $q^{i^Y System}$ представляет собой множество системных рискообразующих потенциалов данной угрозы по каждому фактору риска

$$Q^{i^Y System} = \{Q_{i^S}^{i^Y System}\}. \tag{16}$$

Последнее множество может быть получено нахождением максимума в каждом столбце матрицы (15)

$$Q_{i^S}^{i^Y System} = \max\{q_{i^S}^{1^R}, q_{i^S}^{2^R}, \mathsf{K}, q_{i^S}^{m^R}\}. \tag{17}$$

Расчет рископонижающего потенциала меры защиты по факторам ущерба

Применение в системе мер защиты воздействует на угрозы, меняя количественные характеристики событий рисков. Для каждой угрозы $y_{i^Z}^{i^R} \in Y^{r_{i^R}}$, где $i^Z \in I^Z$ (I^Z — множество индексов всех угроз входящих в $Y^{r_{i^R}}$) может быть определено множество мер защиты от угрозы $M^{i_Z} = \{m_{i_m}\}, i_m \in I^{i_z}$ (I^{i_z} — множество индексов всех мер защиты от угрозы $y_{i^Z}^{i^R}$). Реализация меры защиты $m_{i_m} \in M^{i_z}$ может изменить значения вероятности события риска r_{i^R}, а также его цены по факторам ущерба на $p_{i^R}^m$ и $C^{i^R m} = \{c_{i^S}^{i^R m}\}$ соответственно. С изменением количественных значений события риска изменится и множество значений величины риска по каждому из составляющих ущерба

$$W^{i^R m} = \{w_{i^S}^{i^R m}\}, \qquad \text{где} \qquad w_{i^S}^{i^R m} = c_{i^S}^{i^R m} \times p_{i^R}^m .$$

Вектор $U^m = \{u_{i^S}^m\}$, где $u_{i^S}^m = w_{i^S}^{i^R} - w_{i^S}^{i^R m}$, представляет собой множество значений рископонижающего потенциала меры m_{i_m} для каждой составляющей ущерба по событию риска r_{i^R}.

Величина рископонижающего потенциала меры m_{i_m} по угрозе $y_{i^Z}^{i^R}$ может быть получена путем расчета новых значений ее системного рискообразующего потенциала по формулам (14)–(17) с учетом изменившихся значений количественных характеристик события риска и последующим вычитанием их из первоначальных значений системного рископонижающего потенциала угрозы $y_{i^Z}^{i^R}$.

$$U_{i^Y}^m = \{(Q_{i^S}^{i^Y System} - Q_{i^S}^{i^Y System^m})\} \qquad (18)$$

Здесь $Q_{i^S}^{i^Y System}$ и $Q_{i^S}^{i^Y System^m}$ — значения системных рископонижающих потенциалов угрозы y_{i^Y} по ущербу с индексом i^S до и после применения в системе меры защиты m_{i_m} соответственно.

Каждая угроза соотносится с некоторым компонентом системы O_i. Следовательно, для этого компонента может быть подсчитан его рискообразующий потенциал. В случае если компонент O_i не включает в себя компоненты более низкого уровня иерархии, его рискообразующий потенциал будет равен

$$q_{O_i}^{i^S} = \sum^{I^O} q_i^{i^S}{}_O \ .$$

При наличии в составе компонента O_i компонентов более низкого уровня иерархии к полученному значению рискообразующего потенциала по ущербу с индексом i^S следует прибавить сумму рискообразующих потенциалов компонентов, входящих в состав компонента O_i по тому же ущербу.

$$q_{O_i}^{i^S} = \sum^{I^O} q_i^{i^S}{}_O + \sum^{Z^{O_i^j}} q_z^{O_i^{j-1}(i^S)} \ . \qquad (19)$$

Проведя расчеты для каждой из составляющих ущерба, получаем множество рискообразующих потенциалов объекта O_i по каждому из ущербов

$$Q_{O_i}^{i^S} = \{q_{O_i}^{i^S}\} \ .$$

После применения в системе меры защиты m_{i_m} и пересчета значений рискообразующего потенциала для объекта O_i по формуле (9) получаем

$$Q_{O_i}^{i^S m} = \{q_{O_i}^{i^S m}\} \ .$$

Отсюда рассчитываем значение рископонижающего потенциала по объекту

$$U_{O_i}^m = Q_{O_i}^{i^S} - Q_{O_i}^{i^S m} \ . \qquad (20)$$

Описанное разделение показателя цены события риска по составляющим ущерба очень важно, поскольку помогает более объективнее оценить влияние того или иного события риска на систему. Кроме того, данный подход позволяет определить систему приоритетов для ущербов и эффективно выбирать меры защиты для ущерба в каждом конкретном случае. Введение рискообразующего и рископонижающего потенциала объекта дает возможность рассчитать эффективность применения меры защиты к конкретному компоненту системы.

Данный подход хорош еще и тем, что определения значения цены риска по каждой составляющей ущерба могут выполняться независимо и даже в разное время, что никак не отразится на конечных оценках. Более того, если раньше выявление новых последствий в случае наступления конкретного события риска влекло за собой необходимость пересчета его количественных характеристик, то теперь они могут быть представлены в виде дополнительной составляющей и никак не затронут уже определенные характеристики остальных факторов.

Вместе с тем описанный подход не учитывает ситуации, когда, например, применение в системе меры защиты влияет на несколько событий риска одновременно. Помимо этого не оценивается результат применения в системе комплекса мер защиты, так как в этом случае влияния отдельных мер могут пересекаться, и суммирование рископонижающих потенциалов по каждой из применяемых мер невозможно.

Обозначенные вопросы обязательно будут рассматриваться в дальнейшем, поскольку являются весьма существенными для определения максимально эффективного комплекса мер защиты с учетом специфики задачи.

Литература

1. *Черешкин Д. С.*, *Кононов А. А.* Автоматизация построения моделей угроз и моделей защиты информационных систем с использованием комплексной экспертной системы «АванГард» // «Межрегиональная конференция безопасность регионов России ИБРР-99. СПб. 13–15 октября 1999 г.». Тезисы конференции. Ч. 1. 1999. С. 27.
2. *Кононов А. А.*, *Бурдин О. А.* Пример автоматизации аудита и управления информационной безопасностью компании // *Петренко С. А.*, *Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. С. 286–332.
3. *Кононов А. А.*, *Бурдин О. А.* Аксиоматика оценки рисков нарушения информационной безопасности компьютеризированных организационных систем // Проблемы информационной безопасности. Компьютерные системы. Санкт-Петербургский государственный технический университет. 2002. № 1. С. 27–30.
4. *Черешкин Д. С.*, *Кононов А. А.* Аксиоматика оценки рискообразующих потенциалов компьютеризации организационных систем // Информационная математика. 2003. № 1. С. 29–32.
5. *Черешкин Д. С.*, *Цыгичко В. Н.*, *Кононов А. А.* Задачи управления безопасностью региональной информационной инфраструктуры // Науч.-техн. информ. Сер. 1. 2003. № 8. С. 1–9.
6. *Бурдин О. А.*, *Кононов А. А.* Метод оценки рискообразующих потенциалов в компьютеризированных организационных системах // НТИ. Сер. 1. 2004. № 2. С. 19–21.