# Управление рисками и безопасностью

## Оценка защищенности критически важных объектов на основе построения моделей событий рисков

А. А. Кононов, А. П. Котельников, К. В. Черныш

**Аннотация.** В статье представлена формальная модель и алгоритмы решения задач оценки рисков нарушения безопасности больших распределенных систем и критически важных объектов, что позволяет повысить эффективность решения задач управления их безопасностью. В основе предлагаемого подхода лежит метод построения моделей событий рисков нарушения безопасности и оценки рискообразующих потенциалов угроз, порождающих события рисков.

**Ключевые слова:** *информационная безопасность, оценка рисков, управление безопасностью, критически важные объекты.*

### Введение

Настоящая работа в значительной степени является результатом обобщения и продолжения исследований, которые нашли свое отражение в публикациях [1, 2, 3, 4, 5].

Информационные технологии все шире внедряются в процессы управления и функционирования всех сфер экономики, производства, обеспечения безопасности и функционирования государства и социальных институтов и образуют информационную инфраструктуру жизнедеятельности современного общества. Эта инфраструктура все в большей степени принимает на себя выполнение жизненно важных функций в обеспечении существования и деятельности организаций и предприятий, включая те, деятельность которых играет критически важную роль в обеспечении нормальных условий жизни, производственной и деловой активности, а также обеспечения национальных интересов и безопасности.

В складывающихся условиях именно через информационную инфраструктуру появляется возможность наиболее эффективным образом решать вопросы управления безопасностью критически важных объектов.

В статье представлена формальная модель и алгоритмы решения задач оценки рисков нарушения безопасности больших распределенных систем и критически важных объектов. В основе предлагаемого подхода лежит метод построения моделей событий рисков нарушения безопасности и оценки рискообразующих потенциалов угроз, порождающих события рисков.

Есть немало исследований по проблемам управления рисками КВО [6, 7, 8, 9]. Ценность предложенного подхода состоит в том, что до последнего времени именно такой универсальный подход, для автоматизации вычислений оценки и агрегации оценок рисков различной природы для больших социально-экономических систем, отсутствовал, в то время как проблемы контроля безопасности в боль-

ших системах с разнородными рисками возрастают, в т. ч. из-за увеличения взаимозависимости структурных составляющих и из-за цены возможных ущербов при утрате контроля за безопасностью каких-либо составляющих.

## 1. Построение структурной модели для управления рисками

В управлении безопасностью больших организационно-экономических и организационно-технических систем ключевую роль играет управление рисками. Основной особенностью оценки рисков опасностей существующих для критически важных объектов (КВО) является невозможность, в большинстве случаев, использовать аппарат теории вероятностей для их оценки, поскольку, зачастую, невозможно набрать хоть какой-то статистический материал, по событиям, которые во многом определяются уникальными особенностями объектов, их взаимосвязей и возможных ситуаций. Таким образом, нужны более универсальные, чем вероятностные и статистические подходы, например, методы отслеживания причинно-следственных связей возникновения событий рисков.

Каждый отдельно взятый риск есть результат некоторого возможного события нарушения безопасности КВО, **события риска**, наносящего ущерб КВО, среде, в которой этот КВО функционирует, всем тем, кто зависит от безопасности КВО.

В большинстве случаев невозможно определить точное значение ущерба, который может быть нанесен в результате того или иного события риска. Это сложно сделать и потому, что число потенциальных событий рисков чрезвычайно велико, и потому, что во многих случаях ущерб не сводится лишь к материальному ущербу, который может быть выражен в денежном выражении, но требует учета нематериальной составляющей ущерба. Не менее сложно определить точное значение вероятности события риска. Поэтому можно говорить только об оценках этих величин. Для фиксирования оценки этих величин по отдельным возможным событиям рисков предлагается использовать ранговые шкалы.

Ранговая шкала величины ущерба должна позволять оценивать как материальный, так и нематериальный ущерб. Очевидно, что необходимую универсальность, которая позволит удовлетворить указанное требование, шкале можно придать, если откладывать на ней не просто оценки ущерба, а оценки опасности (нежелательности) событий рисков. 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 оценки опасности этих событий рисков. Очевидно, что в предлагаемом методе кардинального ранжирования по величине опасности риска закладывается определенный верификационный механизм корректности оценок, поскольку указание степени риска для каждого вновь определяемого события риска требует фактически подтверждения целой системы аксиом о том, что каждое событие риска, находящееся по шкале ниже определяемого, менее опасно (нежелательно), а каждое находящееся выше — более опасно (нежелательно) определяемого. В случае если эти условия ранжирования для вновь вносимого в БД события не выполняется, требуется пересмотр всех тех оценок, для которых это требование не выполняется.

Ранговая шкала вероятности событий риска верифицируется таким же путем.

Еще одним способом повысить доверие к получаемым результатам может стать привлечение нескольких экспертов и предоставление им очной или заочной (посредством электронных коммуникаций), возможности знакомиться с результатами оценки опасностей и вероятностей событий рисков, которые сделали другие эксперты и приходить к некоторому консолидированному мнению (метод дельфийских групп).

**Определение.** Величиной риска будем считать результат произведения оценки опасности (нежелательности) события риска на оценку вероятности этого события.

Все события рисков могут быть представлены, как результат реализации некоторого множества угроз, связанных с недостаточным уровнем безопасности КВО. Каждую из угроз в свою очередь всегда можно ассоциировать с каким-либо компонентом КВО. Таким образом, для принятия решений по повышению безопасности необходимо выделить все компоненты, с которыми могут быть ассоциированы те или иные угрозы, реализация которых может привести к возникновению того или иного события риска и рассчитать «вклад» каждого из компонентов в формирование этого риска. Сразу следует указать и на еще одну особенность предлагаемого подхода. Это включение в понятие «угроза» и понятия «уязвимости». То есть все возможные уязвимости также включаются в модели угроз. Но вероятность присутствия уязвимостей бывает, как правило, 100-процентной в отличие от угроз, вероятность реализации, которых во многом зависит от источников угроз и моделей нарушителя. Поскольку любая угроза реализуется, из-за наличия той или иной уязвимости, то, как правило, модели событий рисков, в предлагаемом методе, включают, как минимум две угрозы, одна из которых отражает уязвимость объекта, а вторая активность нарушителя.

Представим формальную схему решения указанной задачи.

Пусть некоторый критический объект представлен в виде системы его частей **S**, т. е. система может быть представлена в виде некоторого множества, составляющих ее компонент $\mathbf{O}_{i^s}$, где $i^s \in \mathbf{I}^{\mathbf{S}}$, $\mathbf{I}^{\mathbf{S}}$ — множество индексов всех компонент **S**:

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

Компоненты, с которыми невозможно связать какие-либо угрозы безопасности системе **S**, в модель могут 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:

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

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 $\left\{\mathbf{O}_{i^S}\right\}$ 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. То есть для любого объекта $\mathbf{O}^j_{i^s}$ при $j < J$ будет существовать множество $\mathbf{O}^j_{i^s} \supset \left\{\mathbf{O}^{j+1}_{i^o}\right\}$, $i^o \in \mathbf{I}^{\mathbf{O}^j_{i^s}}$, где $\mathbf{I}^{\mathbf{O}^j_{i^s}}$ — множество индексов компонентов ($j$ + 1)-го уровня иерархии, входящих в состав компонента $\mathbf{O}^j_{i^s}$.

Назовем *объектами* компоненты низшего уровня иерархии и положим, что они могут быть объединены в *подсистемы*. Для каждой подсистемы в свою очередь может быть определено такое множество угроз, которое будет включать только те угрозы, которые не могут быть отнесены к отдельным объектам и, потому формально могут идентифицироваться только на более высоком иерархическом уровне. В этом случае, в рамках предлагаемой формальной схемы, сама подсистема должна быть идентифицирована в качестве объекта множества $\mathbf{O}_{i^s}$, к которому и будут отнесены указанные угрозы. 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. Если для ЛС может быть определено, некоторое множество угроз, которое не может быть отнесено ни к одной из входящих в нее компонент в отдельности от других, то в этом случае сама ЛС должна быть идентифицирована в качестве объекта множества $\mathbf{O}_{i^s}$ и по нему должны быть идентифицированы указанные угрозы. 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 объекта множества $\mathbf{O}_{i^s}$.

## 2. Построение моделей угроз, моделей событий рисков и расчет рискообразующих потенциалов

Все множество угроз $\mathbf{Y}^{\mathbf{S}}$, связанных с системой **S** и со всеми ее компонентами может быть представлено как

$$\mathbf{Y}^{\mathbf{S}} = \{\mathbf{Y}^{\mathbf{O}_{i^s}}\}, \quad (3)$$

где, $\mathbf{Y}^{\mathbf{O}_{i^s}}$ — множество угроз по каждому объекту $\mathbf{O}_{i^s}$. Таким образом, множество $\mathbf{Y}^{\mathbf{S}}$ представляет собой не что иное, как модель угроз для системы **S**.

Будем отличать множество $\mathbf{Y}^{\mathbf{S}}$ от множества $\mathbf{Y}^{\mathbf{KS}}$, которое представляет собой каталог всех угроз системы **S**, и отличается от множества $\mathbf{Y}^{\mathbf{S}}$ тем, что любая угроза в множестве $\mathbf{Y}^{\mathbf{KS}}$ не связана с конкретным объектом системы **S**, и множество $\mathbf{Y}^{\mathbf{S}}$ может быть получено из $\mathbf{Y}^{\mathbf{KS}}$ 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 $\mathbf{Y}^{r_{iR}} \in \mathbf{Y}^{\mathbf{S}}$.

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

$$w_{iR} = c_{iR} \times p_{iR} \tag{4}$$

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

$$p_{iR} = \prod_{x}^{X^{r_{iR}}} p_x^{r_{iR}}, \tag{5}$$

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

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 $\mathbf{Y}^{r_{iR}}$, то можно говорить о том, что это множество угроз в рамках системы **S** обладает совокупным рискообразующим потенциалом $w_{iR}$. Рискообразующий потенциал каждой из угроз, входящих в множество $\mathbf{Y}^{r_{iR}}$, предлагается рассчитывать по формуле:

$$q_{iR} = \frac{w_{iR}}{X^{r_{iR}}}. \tag{6}$$

Эта формула справедлива постольку, поскольку отражает следующую логику: если бы хотя бы одна из угроз не была реализована, то рассматриваемое событие риска $r_{iR}$ не произошло бы в том виде, в котором мы его оцениваем. А именно: либо не было никакого события риска, либо это было событие с совершенно иными показателями цены риска, вероятности этого события и, как следствие, величины риска по этому событию. Поэтому будет справедливым предположить, что «вклад» каждой угрозы, из множества тех угроз, которые приводят к рассматриваемому событию риска, характеризуемый ее рискообразующим потенциалом по данному событию, 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 нельзя исключить, что 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 оценки опасности угроз, 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* $q^{i^{YS}}$ — определяется максимальным значением ее рискообразующего потенциала по всем моделям рисков множества $\mathbf{R}^{i^y}$:

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

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

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

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

Если компонент $\mathbf{O}_i$ $j$-го иерархического уровня включает в себя множество компонентов $j + 1$ уровня

иерархии $\mathbf{O}_i^j \supset \left\{\mathbf{O}_{i^z}^{j+1} \middle| i^z \in \mathbf{I}^Z\right\}$, $\mathbf{I}^Z$ — количество объектов на j+1 уровне, входящих в качестве компонентов объекта $\mathbf{O}_i$ то его рискообразующий потенциал $q^{\mathbf{o}_i^j}$ рассчитывается как сумма рискообразующего потенциала угроз для этого компонента и сумма рискообразующих потенциалов компонентов, входящих в его состав:

$$q^{\mathbf{o}_i^j} = \sum_{i^O}^{\mathbf{I^O}} q_i^{S}{}_{\mathbf{o}} + \sum_{i^z}^{\mathbf{I}^Z} q_{i^z}^{\mathbf{o}_i^{j+1}}, \qquad (9)$$

где $q_{i^z}^{\mathbf{o}_i^{j+1}}$ — рискообразующий потенциал компонента $O_{i^z}^{j+1} \subset \mathbf{O}_i^j$.

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

## 3. Моделирование возможностей снижения рисков

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.

Для того чтобы оценить рископонижающий потенциал меры защиты, нужно построить модели ожидаемых воздействий этой меры на модели событий риска. Основными характеристиками таких моделей являются новые 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 $y_x^{i^R} \in \mathbf{Y}^{r_{i^R}}, x \in \mathbf{X}^{r_{i^R}}$ ($\mathbf{X}^{r_{i^R}}$ — множество индексов угроз, входящих в $\mathbf{Y}^{r_{i^R}}$) может быть определено множество мер защиты $\mathbf{M}^{r_{i^R}}$.

При реализации меры защиты

$$m_{i_m} \in \mathbf{M}^{i_z}, i_m \in \mathbf{I}^M$$

($\mathbf{I}^M$ — множество индексов мер, парирующих угрозу $y_x^{i^R}$), 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 угрозе $y_x^{i^R}$ события риска $r_{i^R}$. Если при применении меры защиты понижается величина риска по этому событию, то тогда в соответствии с (6) понижаются и рискообразующие потенциалы всех угроз, реализация которых приводит к событию риска.

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

Тогда применение комплекса мер $\mathbf{K}_{i^K}^S$ 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 компонентов разного уровня иерархии будут 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 $\mathbf{K}_{i^K}^S$ носят сугубо предварительный промежуточный характер по трем причинам.

Во-первых, после принятия любого комплекса мер $\mathbf{K}_{i^K}^S$ может измениться вся система объектов, поскольку принятие мер может повлечь за собой внедрение в систему определенных средств защиты, каждое из которых 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.

В-третьих, при расчете величины системного рискообразующего потенциала каждой отдельной угрозы (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 $\mathbf{K}_{i^K}^S$, 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 $\mathbf{K}_{i^K}^S$. То есть по каждой угрозе должно быть показано, что не существует события риска, в котором ее значимость может превысить текущий уровень ее системного рискообразующего потенциала с учетом того, что в системе будут реализованы меры, предусмотренные комплексом $\mathbf{K}_{i^K}^S$.

Таким образом, для того чтобы оценить риски, которые будут существовать в системе после принятия комплекса $\mathbf{K}_{i^K}^S$, следует вновь выполнить всю систему процедур, предусмотренную при расчете (1)–(9).

## Заключение

Введение показателей рискообразующего и рископонижающего потенциалов, измеряемых величиной риска, связанного с конкретными угрозами и компонентами оцениваемой системы, открывает новые возможности в управлении рисками, поскольку позволяет отслеживать взаимосвязи между отдельными угрозами, уязвимостями по отдельным компонентам системы и рисками, связанными с системой в конкретной ее конфигурации и в конкретной среде функционирования.

Если строго придерживаться следующего правила: при оценке таких параметров событий рисков, как цена риска и вероятность события риска, определять их как показатели, относимые к одному году, и цену риска указывать в конкретных денежных единицах — то показатель рискообразующего потенциала (опасности нарушения безопасности КВО) будет отражать ожидаемые среднегодовые потери для КВО в оцениваемой конфигурации в конкретных условиях ее функционирования по каждому ее компоненту, по каждой структурной составляющей и по системе КВО в целом, а показатель рископонижающего потенциала мер будет отражать соответственно возможности снижения этих потерь при принятии оцениваемых мер.

Описанные в статье методы решения задач управления рисками могут применяться во многих сферах деятельности. На сегодняшний день есть опыт их использования в управлении информационной безопасностью электронных платежных технологий в региональных расчетных системах Банка России (программные комплексы «АванГард» и «РискАналитик») [10]; в системе управления безопасностью в аэропорту «Шереметьево» (программный комплекс «РискДетектор») [11]; в системе безопасности ОАО «Российские железные дороги» (программный комплекс оценки уровня безопасности «РискМенеджер») [12]; в системе мониторинга безопасности критически важных объектов транспортной инфраструктуры и перевозки опасных грузов Ространснадзора (программно-аппаратный комплекс мониторинга и контроля рисков чрезвычайных ситуаций на транспорте «РискТрансНадзор») [13].

## Литература

1. *Гордеев Ю. А.*, *Кононов А. А.*, *Бурдин О. А.* Система моделей и аксиоматика оценки рискообразующих потенциалов компьютеризированных организационных систем // Информационные технологии в проектировании и производстве // Науч.-техн. журн. / ФГУП «ВИМИ», 2002. № 3. С. 46–48.
2. *Кононов А. А.*, *Сичкарук А. В.*, *Черныш К. В.* Задачи управления киберрисками и кибербезопасностью критических инфраструктур национального масштаба //

Проблемы управления рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 31 М.: Издательство ЛКИ, 2007, с. 95–98.
3. *Пучков В. А.*, *Черешкин Д. С.*, *Черныш К. В.*, *Кононов А. А.* Использование категорирования в обеспечении безопасности критических инфраструктур национального масштаба // Управление рисками и безопасностью: Труды Института системного анализа Российской академии наук. Т. 41. М.: Ленанд/URSS, 2009, с. 6–13.
4. *Кононов А. А.*, *Стиславский А. Б.*, *Цыгичко В. Н.*, *Черешкин Д. С.* Автоматизированный комплекс средств обеспечения антитеррористической безопасности на примере транспортного комплекса // Труды СПИИРАН. 2009. Вып. 10. СПб.: Наука, 2009, с. 47–62.
5. *Кононов А. А.*, *Черныш К. В.*, *Гуревич Д. С.*, *Поликарпов А. К.* Оценка рисков в иерархических структурах критически важных объектов // Управление рисками и безопасностью / Под ред. Д. С. Черешкина. Труды Института системного анализа Российской академии наук. Т. 52. М.: Ленанд/URSS, 2010, с. 5–15.
6. *Акимов В. А.*, *Лесных В. В.*, *Радаев Н. Н.* Основы анализа и управления риском в природной и техногенной сферах. М.: Деловой экспресс, 2004. 352 с.
7. *Акимов В. А.*, *Лапин В. Л.*, *Попов В. М.*, *Пучков В. А.*, *Томаков В. И.*, *Фалеев М. И.* Надежность технических систем и техногенный риск. М.: Деловой экспресс, 2002. 368 с.
8. Риски в природе, техносфере, обществе и экономике / В. А. Акимов, В. В. Лесных, Н. Н. Радаев; МЧС России. М.: Деловой экспресс, 2004. 352 с.
9. Стратегические риски России: оценка и прогноз / МЧС России; под общ. ред. Ю. Л. Воробьева; М.: Деловой экспресс, 2005. 392 с.
10. *Владимирова Т. Н.* Опыт работы по внедрению системы мониторинга информационной безопасности платежной системы Банка России // Информационный бюллетень Главного управления безопасности и защиты информации Центрального банка Российской Федерации. 2005. № 1. С. 47–56.
11. *Стиславский А. Б.* Управление рисками нарушения безопасности инфраструктуры транспортного комплекса [Электронный ресурс] // Библиотека авторефератов и тем диссертаций: [сайт]. [2010]. URL http:// http://dibase.ru/article/09032010_stislavskiyab/7 (дата обращения: 24.09.2012).
12. УСП Компьюлинк завершил ряд проектов в ОАО «РЖД» комплекса [Электронный ресурс] // Электронный центр малого бизнеса: [сайт]. [2006]. URL http://www.tradecenter.ru/NewsAM/NewsAMShow.asp?ID=296606 (дата обращения: 24.09.2012).
13. *Пукемов К.* Угрозы портам и вокзалам будут отслеживать из космоса [Электронный ресурс] // Известия: [сайт]. [2012]. URL http://izvestia.ru/news/531120 (дата обращения: 24.09.2012).

**Кононов Александр Анатольевич**. С. н. с. ИСА РАН. К. т. н. Окончил Московский институт управления им. С. Орджоникидзе в 1982 г. Количество печатных работ: более 100 (в т. ч. 1 монография). Область научных интересов: математическое моделирование, управление безопасностью, информационная безопасность. E-mail: kaa@isa.ru

**Котельников Алексей Павлович**. Заведующий кафедрой Белгородского университета кооперации, экономики и права. К. т. н., доцент. Окончил Харьковский политехнический институт в 1976 г. Количество печатных работ: 48. Область научных интересов: математическое моделирование. E-mail: apk1703@gmail.com

**Черныш Константин Васильевич**. Заместитель директора ИСА РАН. К. т. н. Окончил МВТУ им. Баумана в 1973 г. и МГУ в 1989 г. Количество печатных работ: 22. Область научных интересов: математическое моделирование, управление безопасностью. E-mail: chern@isa.ru