УДК 623.618

Анализ подходов к формализации показателя информационного превосходства на основе теории оценки и управления рисками

Михайлов Р. Л.

Актуальность. *В настоящее время в вооруженных силах развитых стран существует устойчивая тенденция к внедрению концепции управления боевыми действиями по сетецентрическому принципу. Неотъемлемым атрибутом данной концепции является информационное противоборство, то есть двусторонний конфликт в информационной сфере, ведение которого на тактическом и оперативном уровнях управления возлагаются на подсистемы радиомониторинга и радиоэлектронной борьбы. В то же время, в известных автору работах отсутствует формализованное описание показателя информационного превосходства – ключевого показателя эффективности ведения информационного противоборства, который бы связывал показатели эффективности каждой из указанных подсистем.* ***Целью работы*** *является анализ математических моделей теории оценки и управления рисками на предмет их использования в новой предметной области – в сфере информационного противоборства.* ***Используемые методы****. Решение задачи основано на использовании методов системного анализа, а также методов индукции и дедукции теории логики.* ***Результат.*** *На основе анализа более 50 источников выявлены особенности математической оценки и управления рисками в экономической сфере и в сфере безопасности информационных систем. Проанализированы математические модели, которые могут лечь в основу формализации показателя информационного превосходства, показаны пути их совершенствования в интересах адекватного отображения процесса информационного противоборства.* ***Новизна.*** *Элементом новизны работы является определение необходимости учета целенаправленных действий противостоящей стороны в ходе информационного противоборства на основе математического аппарата в области обеспечения безопасности информационных систем, а также учета игрового, по сути, характера его ведения и, соответственно, моделей оценки и управления рисками в экономических системах, которые позволяют оценить как возможный вследствие принятия управленческих решений доход, так и убыток в активах.* ***Практическая значимость.*** *Представленный анализ может быть использован специалистами для обоснования новых технологических решений в области информационного противоборства, а также военными специалистами – для обоснования новых форм и способов организации взаимодействия разнородных сил и средств при ведении вооруженной борьбы. Кроме того, данный анализ будет полезен научным работникам и соискателям, ведущим научные исследования в области координации в сложных многоуровневых системах управления.*

Ключевые слова: *оценка рисков, управление рисками, информационное противоборство, информационное превосходство, сетецентрический принцип управления.*

Актуальность

В настоящее время ключевая парадигма ведения вооруженного противоборства, действующая в вооруженных силах США и стран НАТО, а также внедряемая в РФ, базируется на концепции управления боевыми действиями по

Библиографическая ссылка на статью:
Михайлов Р. Л. Анализ подходов к формализации показателя информационного превосходства на основе теории оценки и управления рисками // Системы управления, связи и безопасности. 2017. № 3. С. 98-118. URL: http://sccs.intelgr.com/archive/2017-03/05-Mikhailov.pdf

Reference for citation:
Mikhailov R. L. Analysis of Approaches to the Formalization of the Indicator of Information Superiority Based on the Theory of Assessment and Risk Management. *Systems of Control, Communication and Security*, 2017, no. 3, pp. 98-118. Available at: http://sccs.intelgr.com/archive/2017-03/05-Mikhailov.pdf (in Russian).

сетецентрическому принципу. О сущности и содержании данной концепции написано достаточно подробно и много, из последних публикаций по этой тематике следует отметить работы [1-6]. Ключевыми и неразрывно связанными ее компонентами стали такие понятия, как «информационное противоборство», «информационное превосходство», «информационные операции», «действия в кибернетическом пространстве». Не пытаясь «привести к общему знаменателю» взгляды различных авторов, следует отметить, что все они сходятся в определении основной целью информационного противоборства достижение информационного превосходства над противостоящей стороной. Это связано с тем, что именно завоевание и удержание информационного превосходства в настоящее время становится обязательным этапом и необходимым условием начала и ведения современных военных действий. При этом под информационным превосходством понимается *возможность и способность осуществлять непрерывный сбор сведений, их обработку, распределение потока достоверной информации, а также способность не допустить выполнения аналогичных действий противником*. Проявляться информационное превосходство может в различных формах – от возможности и способности более качественно и быстро оценивать обстановку, принимать и доводить до подчиненных адекватные решения, до исключения (существенного затруднения) информационного обеспечения противника за счет проведения наступательных информационных операций [7].

В работе [8] указывается на два направления, в рамках которых может быть развернуто информационное противоборство: информационно-техническое и информационно-психологическое. Последнее из направлений применимо, в основном, на стратегическом уровне управления, в то время как на тактическом и оперативном уровнях под информационным противоборством в настоящее время понимаются отдельные вопросы организации радиомониторинга (РМ) и радиоэлектронной борьбы (РЭБ) [8], которые решают соответствующие подсистемы (РМ и РЭБ), представляющие собой совокупность средств РМ и РЭБ, размещенных на театре военных действий, и являющиеся обеспечивающими составными частями системы управлений войсками и оружием (СУВО). При этом имеет место необходимость координации данных подсистем применительно к решению задачи распределения объектов информационного пространства противостоящей стороны между средствами подсистемы РМ и средствами радиоэлектронного подавления (РЭП), входящими в состав подсистемы РЭБ, в интересах как обеспечения достижения данными подсистемами своих целей функционирования, так и цели СУВО (обеспечения информационного превосходства над противостоящей стороной) в целом.

Целью подсистемы РМ, в самом общем описании, является перехват сообщений, циркулирующих по каналам связи, в целях обеспечения военного руководства информацией о противостоящей стороне, в то время как подсистема РЭБ функционирует в целях срыва процесса управления противостоящей стороны путем подавления каналов связи ее СУВО. В интересах достижения своих целей каждая из этих подсистем заинтересована в воздействии на как можно большее количество объектов информационного пространства противостоящей

стороны, однако вследствие естественных причин один и тот же объект не может быть распределен одновременно средству РМ и средству РЭП. Вместе с тем, в известных автору работах отсутствует описание показателя информационного превосходства, учитывающего как эффективность координации данных подсистем при распределении объектов информационного пространства противостоящей стороны, так эффективности аналогичных процессов противостоящей стороны [9].

Сам процесс принятия решений в сложных организационно-технических системах представляет собой трудоемкую задачу, которую осложняют неполнота исходной информации, наличие множества показателей качества (критериев) оценки исходов альтернативных решений задачи, сокращение времени принятия решений и повышение требований к опыту и квалификации лиц, принимающих решения. Неполнота исходной информации связана с неопределенностью прогнозируемой ситуации, в рамках которой решение должно функционировать. В работе [10] И.Г. Черноруцкий выделяет два различных характера неопределенности:

- «природная» неопределенность, связанная с неопределенностью состояния внешней среды;
- неопределенность типа «активный партнер», отражающая поведение других субъектов по выбору решения.

«Природная» неопределенность, то есть отсутствие *целенаправленного* негативного внешнего воздействия на процесс функционирования системы исследуется при оценке и управления рисками в экономической деятельности организации. Особое место в подобных исследованиях занимают вопросы функционирования страховых организаций, в связи с чем существует отдельное направление математической теории – актуарная математика.

Учет неопределенность типа «активный партнер» приводит к постановке задачи принятия решений в условиях конфликта, и при анализе методов решения подобных задач активно используются элементы теории игр [11]. Наличие конфликта с другой системой в условиях неопределенности стратегии ее *целенаправленных* деструктивных воздействий является неотъемлемой чертой процесса оценки и управления рисками информационной безопасности организационно-технических систем (ОТС). Вместе с тем, стоит отметить тот факт, что в принципе невозможно «победить» нарушителя, и, соответственно, задачей управления рисками является снижение ущерба от него.

Кроме того, авторы работы [12] связывают факт риска с возможностью возникновения некоторых событий, которые нарушают текущее состояние системы или естественное (прогнозируемое) течение процесса ее функционирования. В связи с этим, проблема управления риском рассматривается в двух вариантах: при «естественном» ходе процессов и при их непрогнозируемом нарушении.

Таким образом, актуальность настоящей работы основывается, с одной стороны, на отсутствии в настоящее время формализованного описания показателя информационного противоборства, и, с другой стороны, на отсутствии в известных автору работах анализа возможности использования математическо-

го аппарата теории рисков для описания такого показателя. Искомые математические модели оценки показателя информационного противоборства должны включать элементы оценки риска в условиях наличия целенаправленного противодействия рассматриваемой системе и, кроме того, должны позволять оценивать как потенциальный ущерб от этого противодействия, так и возможное приращение целевого показателя информационного противоборства. В связи с этим необходимо провести анализ научно-методического аппарата оценки и управления рисками как в экономических системах, так и в системах информационной безопасности.

Анализ подходов к оценке и управлению рисками в экономических системах

Исследования по проблемам оценки и управления рисками экономической деятельности организации посвящены работы таких отечественные и зарубежные ученые как В.И. Авдийский, А.П. Альгин, Т. Бартон, В.И. Бархатов, Т. Бачкаи, В.Е. Беннинг, А.Н. Буренин, К. Гилкрист, М.В. Грачева, Грюнинг Х. Ван, В.П. Буянов, А.В. Воронцовский, В.Н. Вяткин, В.А. Гамза, П.А. Герасимов, П.Г. Грабовый, В.А. Горелик, В.М. Гранатуров, Ю.Ю. Екатеринославский, Б. Зимолон, В.В. Ильин, Р.М. Качалов, К.А. Кирсанов, Г.Б. Клейнер, В.Ю. Королев, А.А. Кудрявцев, М.Г. Лапуста, И.А. Лебедев, М.В. Лисанов, А.А. Лобанов, Маккарти Мэри Пэт, А. Маршалл, Б.А. Матвеев, Е.И. Мельникова, Д. Месена, Д. Мико, Дж. Милль, Л.А. Михайлов, Д.А. Никульшин, В. Окулов, С.Н. Петрова, А. Пигу, Б.Н. Порфирьев, Б.А. Райзберг, М.А. Рогов, В.И. Рябикин, В.Т. Севрук, Н.А. Сердюкова, Н.У. Сениор, В.С. Ступаков, Г.С. Токаренко, Р. Тримпоп, П. Уокер, Ф. Фабоцци, О.В. Хмыз, Н.В. Хохлов, С. Хьюс, К. Хэдхэд, Дж.Дж. Хэмптон, Г.В. Чернова, А.В. Чугунов, А.С. Шапкин, У. Шарп, Л.Г. Шаршукова, У. Шенкир, С.Я. Шоргин, Н.В. Шумихина и др. [13, 14].

Исторически первой была сформирована концепция минимизации риска, основанная на постулатах классической теории риска, родоначальниками которой являются Дж. Милль [15] и Н.У. Сениор, где категория «риск» интерпретируется исключительно с точки зрения возможности возникновения ущерба, потери или убытка. Развитие данной теории, сторонниками которой являются такие известные деятели экономической науки как Б.А. Райзберг [16], Н.В. Хохлов [17], М.В. Грачева [18], Г.В. Чернова, А.А. Кудрявцев [19] и многие другие, учитывающие сугубо негативные последствия проявления риска, сводит управление риском преимущественно к применению способов и методов, направленных на нейтрализацию потенциального ущерба или сведение уровня риска к минимально возможному значению. Иными словами, основное содержание концепции минимизации риска сконцентрировано на разработке и реализации методов управления, ориентированных на уменьшение риска до максимально возможного уровня, а в идеале – его полного или частичного избегания.

Вместе с тем, такие экономисты как А.П. Альгин [20], А.С. Шапкин [21], А.А. Воронцовский [22] и другие, являющиеся приверженцами неоклассиче-

ской теории риска, к основоположникам которой относят А. Маршалла и А. Пигу [23], считают категорию «риск» более сложным и емким понятием, подразумевающим не только потери, но и положительные последствия наступления непредвиденных событий. Впоследствии математический аппарат классического риск-менеджмента пополнился методами, основанными на сопоставимости оценки предельной полезности от управленческого решения в условиях риска и, собственно, меры риска за счет оценки и представления обоих этих показателей в общих единицах измерения [23].

В работе Б.Н. Порфирьева [24] впервые указано на невозможность достижения нулевого уровня риска, то есть полного его отсутствия, при этом выделено свойство приемлемости, что явилось основой образования концепции приемлемого риска. Данная концепция, получившая широкое распространение в зарубежной и отечественной практической деятельности, в настоящее время лежит в основе практически всех программ управления экономическими рисками. В.С. Ступаков и Г.С. Токаренко в своих работах отмечают, что ее целью является определение оптимального компромисса между такими противоречивыми точками зрения на риск, как «риск – благородное дело» и в тоже время «риск нужно сводить к минимуму» [25]. Основная идея данной концепции состоит в восприятии риска как управляемого процесса, в признании невозможности полностью избавиться от риска экономических потерь и в возможности его снижения до определенного, допустимого, приемлемого уровня, когда риск перестает быть угрожающим. Под приемлемым риском следует понимать такой уровень риска, который в данной ситуации с учетов факторов внешней и внутренней среды является допустимым, целесообразным и обоснованным исходя из социально-экономических соображений [14].

В словаре Уэбстера [26] риск определяется как «опасность, возможность убытка или ущерба». Следовательно, применительно к анализу конечного экономического результата риск отождествляется с возможностью поступления какого-либо неблагоприятного события, влияющего на такой результат: например, потери некоторой части или всего дохода, появление дополнительных расходов и т. п. Другими словами, под риском понимается возможная опасность потерь, вытекающая из специфики тех или иных явлений природы и человеческой деятельности.

В общем случае риск следует рассматривать с различных позиций. Соответственно, риск может «выступать» в качестве различных категорий: это и историческая, и социально-психологическая, и экономическая категории, в том числе и формально-математическая категория [27]. Необходимо отметить, в частности, что риск как экономическая категория обуславливается группой случайных событий, каждое из которых может произойти или не произойти. При реализации конкретного события из указанной группы соответствующие оценки конечного результата на качественном уровне могут характеризовать три типа возможных экономических результатов [28]:

- отрицательный (проигрыш, ущерб, убыток);
- нулевой (статус-кво);
- положительный (выигрыш, выгода, прибыль).

По мнению авторов работы [12], риск в широком смысле – это непредсказуемость состояния системы или течения процесса как результат неполноты информации при принятии решения. При этом под обеспечением устойчивости системы подразумевается достижение достаточно низкого уровня риска, оцениваемого величиной возможных потерь, связанных с принятием решений в условиях неполной информации. Это в свою очередь требует применения процедуры управления риском. Под управлением риском понимается управление системой или процессом, непременным атрибутом которого являются процедуры учета и оценки факторов риска в целях максимального снижения неопределенности при принятии решений и обеспечения устойчивости системы [12].

В работе [29] показано, что наиболее часто под риском понимается сочетание вероятности (частоты) нанесения ущерба и тяжести ущерба, при этом управление рисками в сложных ОТС, как правило, осуществляется в условиях нестохастической неопределенности. Эти условия характеризуются тем, что неопределенные факторы относятся к неслучайным, не обладают статистической устойчивостью и не описываются каким-либо законом распределения вероятности. Об этих факторах невозможно получить достаточно достоверной информации, а вероятность риск-событий, связанных с воздействием этих факторов, с требуемой точностью определить невозможно. Это обусловлено следующим причинами [29]:

- неполнотой и недостаточностью информации о системе;
- нечеткостью, неоднозначностью или противоречивостью выделения и описания границ системы или ее состояний, а также входных и выходных воздействий, условий ее функционирования, поведения или реакций окружающей среды;
- сложностью типизации и уникальностью оцениваемых явлений;
- сложностью оценки реального «размера» задач управления рисками;
- сложностью получения оценки вероятности проявления риска;
- зависимостью последствий риска от момента, когда риск выявлен и от возможной тяжести его последствий;
- сложностью получения точной оценки необходимых ресурсов для предотвращения или снижения риска.

Авторы работы [30] указывают на то, что риск в ОТС нельзя рассматривать в отрыве от эффективности ее функционирования. В самом общем случае эффективность – это уровень соответствия результатов какой-либо деятельности поставленным задачам, а риск – это вероятность срыва выполнения этих задач. При этом неуспех может сопровождаться и другими негативными последствиями: авариями, человеческими жертвами или материальными убытками. Чем выше эффективность, тем больше риск. Соответственно, если стараться максимально снизить риск, эффективность может оказаться на неприемлемо низком уровне. Именно поэтому в процессе управления всегда необходимо учитывать оба эти параметра. При анализе деятельности экономической системы эффективностью является приносимая прибыль, а риском – возможность понести убытки. При этом и на тот, и на другой параметр влияет множество

взаимосвязанных факторов, таких как эффективность управления, действия конкурентов, рыночная конъюнктура и т. д. [30].

Таким образом, большинством экспертов риск ассоциируется с вероятностью события либо определяется с учетом вероятности. Кроме этого, в научной литературе существуют не только различия в понимании содержания термина «риск», но и разные точки зрения по поводу объективной и субъективной природы риска. В явлении «риск» в экономических системах можно выделить следующие основные элементы, составляющие его содержание [31].

1) Возможность отклонения от предполагаемой цели, ради которой осуществлялась выбранная альтернатива.
2) Вероятность достижения желаемого результата.
3) Возможность материальных, нравственных и других потерь, связанных с осуществлением выбранной в условиях неопределенности альтернативы.

Анализ исследований в области создания математических моделей оценки и управления рисками экономической деятельности показал, что схожие с информационным противоборством по физическому смыслу процессы протекают в страховых организациях. Соответствующие вопросы находятся в ведении актуарной математики, формализующей процесс изменения фонда денежных средств страховой компании. При этом источниками дохода являются страховые взносы клиентов, а расходы связаны с выплатами по наступлению страховых случаев. Естественно предположить, что, во-первых, моменты наступления страховых случаев случайны и не являются последствием целенаправленных действий внешних сил, и, во-вторых, в рамках указанных моделей описаны условия как разорения страховой компании (отрицательное значение величины фонда денежных средств в определенный момент времени), так и получение прибыли на определенном промежутке времени. Таким образом, целесообразно рассмотреть возможность использования соответствующих моделей актуарной математики при формализации показателя информационного превосходства, интерпретировав процесс функционирование страховой компании в схожий процесс информационного противоборства. При такой интерпретации в качестве противостоящей стороны будут выступать застрахованные клиенты.

Анализ подходов к оценке и управлению рисками в информационных системах

Оценка и управление рисками представляет собой один из основных современных разделов теории принятия решений при управлении сложными системами. Использование данной концепции обосновано особенностями построения и функционирования сложных информационной систем [32, 33]:

- многозадачность;
- сложность структуры;
- многокомпонентность;
- многочисленные протекающие процессы;
- необходимость учета большого количества параметров;
- динамичное изменение структуры;

- неполнота исходной информации;
- разнообразие воздействий рискообразующих системных и внешних факторов вероятностного и нестохастического характера;
- наличие сложных нелинейных зависимостей между параметрами;
- необходимость оперативного принятия управленческих решений;
- ограниченные возможности экспериментальных исследований;
- невозможность создания и использования общих аналитических моделей системы и процессов функционирования сложных информационной систем;
- необходимость использования различных подходов к моделированию систем и использование результатов моделирования для оперативного управления ими;
- возможность оперативного управления системами только в псевдореальном масштабе времени, обусловленном их инерционностью.

Основными этапами управления рисками в системах информационной безопасности являются [34-36]:

- идентификация угроз нарушения безопасности информационных систем;
- анализ угроз нарушения безопасности информационных систем;
- планирование мероприятий для противодействия рискам на каждом из уровней управления рисками;
- мониторинг эффективности проведения вышеуказанных мероприятий.

Как показано в работах [37-39], комплексное управление рисками нарушения безопасности информационных систем исследуется такими учеными, как А.Н. Аверкин, А.Е. Алтунин, С.В. Артюхов, О.А. Базюкин, И.З. Батыршин, А.А. Башлыкова, В.Е. Бенинг, Л.С. Берштейн, Е.В Бодянский, А.Н. Борисов, В.В. Борисов, Ю.И. Бродский, Н.П. Бусленко, А.А. Вавилов, В.Н. Вагин, А.Н. Васильев, В.Н. Волкова, А.А. Воронов, А.И. Галушкин, Д. Дюбуа, В.В. Емельянов, А.П. Еремеев, Н.В. Замятина, А.Г. Ивахненко, В.В. Калашников, В.И. Капалин, Ю.Г. Карпов Л.Г. Комарцовой, В.Ю. Королев, А. Кофман, С.Я. Коровин, О.А. Крумберг, А.А. Кудрявцев, О.П. Кузнецов, В.М. Курейчик, Е.И. Кучеренко, Н. Г. Загоруйко, Л.А. Заде, Д.А. Тархов, С.В. Емельянов, А.И. Орлов, О.И. Ларичев, В.Г. Лисиенко, С.И. Макаренко, Е. Мамдани, А.И. Миков, А.Н. Мелихов, А.И. Михалев, Д.А Мокогон, А.С. Нариньяни, В.В. Окольнишников, С.А. Орловский, Г.С. Осипов, Б.В. Палюх, Г.С. Плесневич, А.Б. Петровский, В.Э. Попов, Д.А. Поспелов, А. Прад, Г.В. Рыбина, Ю.И. Рыжиков, А.А. Самарский, М.В. Семухин, В.Б. Силов, В.А. Смирнов, Б.Я. Советов, В.П. Тарасик, В.Б. Тарасов, В.В. Троицкий, С. Федулов, В.К. Финн, И.Б. Фоминых, В.Ф. Хорошевский, И.И. Чукляев, Е.Э. Ширков, С.Я. Шоргин, С.А. Яковлев, Н.Г. Ярушкин, и других.

Понятие «риск информационной безопасности» появилось сравнительно недавно. До средины 90-х годов прошлого века угрозы наступления негативных событий в информационной сфере именовались угрозами безопасности информации. При этом, угрозы безопасности информации ассоциировались с негативными последствиями только для информации и информационных систем.

Понятие «информационный риск» позволяет связать негативные события в информационной подсистеме ОТС с результатами воздействия этих событий на те процессы и объекты ОТС, которые используют информацию. Такое совершенствование причинно-следственной цепочки дает возможность провести более глубокий анализ последствий от негативных событий в информационной сфере ОТС. В результате появляются новые возможности оценки информационных рисков и привлечения менеджмента предприятия к управлению этими рисками.

Таким образом, определение информационного риска может быть представлено в следующем виде. Информационный риск – это возможность наступления случайного события в информационной подсистеме ОТС, приводящего к нарушению процессов ее нормального функционирования, снижению качества информации, в результате которых наносится ущерб ОТС.

Предложенный подход к пониманию сущности информационного риска в информационных системах позволяет выделить ряд характерных особенностей информационных систем [40]:

- информационная система включает все взаимоувязанные компоненты, задействованные в процессах получения, хранения, обработки, передачи, представления и использования информации;
- эффективность информационной системы ОТС оценивается с учетом конечных результатов целевых процессов и функций ОТС;
- подсистема управления имеет возможность изменять параметры функционирования информационной подсистемы.

Наступление случайного события нарушения безопасности информационной системы связано, в первую очередь, с внешними воздействиями. Кроме того, рассмотрение информационной системы как части ОТС позволяет перейти к категории информационный риск как интегральной оценки влияния воздействий на эффективность этой ОТС в целом.

Таким образом, оценка и управление рисками в информационных системах преследуют, главным образом, цель противодействия внешнему деструктивному воздействию, предотвращению (снижению) ущерба от действий нарушителя. Соответственно, решения, принятые на основе моделей управления рисками, не способны повлиять на самого нарушителя, нанести ему урон или заставить отказаться от попытки произвести эти деструктивные воздействия. В связи с этим, актуальным направлением совершенствования научно-методического аппарата оценки и управления рисками в информационных системах должен стать учет при расчете показателя эффективности информационного противоборства действий противостоящей стороны, как системы, заинтересованной в его снижении. При формализации действий противостоящей стороны особое внимание следует уделить математическому описанию законов распределения ущерба от них, и, в дальнейшем, учесть данное описание в моделях процесса функционирования информационных систем, которые аналогичны процессам функционирования страховых компаний. Таким образом, необходимо интерпретировать моменты выплаты страховых премий клиентам как

результат целенаправленного внешнего деструктивного воздействия, в отличии от классической теории актуарной математики, где эти моменты случайны.

Математические модели оценки и управления рисками

Анализ публикаций, имеющихся в открытом доступе, показал, что математические модели, которые могут лечь в основу расчета показателя информационного превосходства, описаны в работах [41-53]. При этом стоит отметить, что автор вполне допускает возможность упущения отдельных исследований в силу различного рода обстоятельств.

Проведем анализ возможности использования в качестве основы для формализации показателя информационного превосходства динамической модель коллективного риска страховой компании, описанной в работе [41]. Текущий резерв страховой компании складывается из начального капитала R_0 и страховых премий, внесенных каждым из клиентов, заключивших контракт в течение интервала времени [0, t], за вычетом страховых выплат по страховым случаям в течение этого интервала. Пусть ζ_i – страховой взнос i-го клиента. Тогда доход страховой компании за время [0, t] равен:

$$R_+(t) = \sum_{i=1}^{N_+(t)} \zeta_i ,$$

где $N_+(t)$ – количество контрактов, заключенных за время [0, t].

Пусть X_j,, $j \geq 1$ – последовательности моментов и размеров страховых выплат. Тогда суммарные потери страховой компании за время [0, t] будут равны:

$$R_-(t) = \sum_{j=1}^{N_-(t)} X_j .$$

Таким образом, «динамическая компонента» резерва страховой компании в момент времени t равна

$$R_d(t) = R_+(t) - R_-(t) = \sum_{i=1}^{N_+(t)} \zeta_i - \sum_{j=1}^{N_-(t)} X_j . \quad (1)$$

Процесс

$$R(t) = R_0 + R_d(t),$$

где $R_d(t)$ определяется соотношением (1), называют процессом риска. Момент разорения τ определяется как:

$$\tau = \inf\left\{t : R_0 + R_d(t) < 0\right\}. \quad (2)$$

где inf (t) – наименьшее значение t из множества $\{t\}$, иными словами момент времени, когда значение величины резерва страховой компании впервые становится отрицательным.

Поскольку процесс $R_+(t)$, а также величины T_i, $i \geq 1$ и X_j, $j \geq 1$, предполагаются случайными, то и процесс риска $R(t)$, и момент разорения τ также случайны, причем в задачах, представляющих практический интерес, случайная величина τ является несобственной в том смысле, что $P(\tau < 0) < 1$.

Величина:

$$\beta(R_0) = P\left(\tau < \infty \middle| R(0) = R_0\right)$$

называется вероятностью разорения на бесконечном промежутке времени при начальном капитале R_0. Пусть $t \geq 0$. Тогда величина

$$\beta(\tau, R_0) = P\left(\tau \leq t \middle| R(0) = R_0\right) \quad (3)$$

называется вероятностью разорения на конечном промежутке времени [0, t] при начальном капитале R_0.

Выражение для вероятности неразорения имеет вид:

$$\nu(\tau, R_0) = 1 - \beta(\tau, R_0). \quad (4)$$

Развитие моделей риска страховой компании сопряжено с предположением о виде процессов $N_+(t)$ и $N_-(t)$ как однородных пуассоновских с некоторыми интенсивностями λ_+ и λ_- соответственно. Данное предположение позволяет описать случайный процесс получения дохода страховой компании $R_+(t)$ линейной функцией:

$$R_+(t) \approx b\lambda_+ t, \quad (5)$$

где b – математическое ожидание размера страхового взноса i-го клиента ζ_i.

Таким образом, процесс риска страховой компании описывается выражением:

$$R(t) = R_0 + ct - \sum_{k=1}^{N_-(t)} X_k, \quad t \geq 0, \quad (6)$$

где $c>0$, $N_-(t)$ – моменты выплат страховых премий выплат страховых премий, X_k, $k=1,\ldots, N_-(t)$ – независимые случайные величины выплат страховых премий с функцией распределения $F(X_k)$ такой, что $F(0)=0$.

Процесс риска страховой компании, описываемый выражением (6), в актуарной математике называют процессом риска Спарре Андерсена.

Формализация показателя информационного превосходства предусматривает следующую интерпретацию описанной исходной модели.

Под резервом компании следует понимать временное преимущество, полученное в ходе выполнения мероприятий цикла управления. Величины ζ_i и X_j – прирост временного превосходства стороны 1 (стороны 2) вследствие i-го (j-го) информационного контакта с объектами информационного пространства стороны 2 (стороны 1). Значение R_0 – начальное временное преимущество стороны 1. Под значениями $N_+(t)$ и $N_-(t)$ следует понимать общее количество информационных контактов стороны 1 (стороны 2). Показателем информационного превосходства является величина $\nu(\tau, R_0)$ (4), отображающая вероятность того, на определенном интервале времени τ, который отображает длительность цикла управления, сторона 1 будет иметь временное превосходство над стороной 2. Соответственно, $\beta(\tau, R_0)$, определяемое выражением (3), – обратная относительно $\nu(\tau, R_0)$ величина, показывающая вероятность отсутствия временного превосходства стороны 1 над стороной 2. Следует отметить, что в полной вероятности исхода информационного противоборства

должна присутствовать величина вероятности равенства сторон по приросту временного превосходства с учетом начального преимущества стороны 1 ($R_0>0$), стороны 2 ($R_0<0$) или отсутствия преимущества у каждой из сторон ($R_0=0$). Таким образом, с учетом принятой интерпретации процесс информационного противоборства будет описываться выражением

$$R_d(t) = R_0 + \sum_{i=1}^{N_+(t)} \zeta_i - \sum_{j=1}^{N_-(t)} X_j .$$

Показатель информационного превосходства, определяемый выражением (4), нуждается в дальнейшей адаптации в целях адекватного отображения цели ведения информационного противоборства. Так, момент разорения τ, определяемый выражением (2), обозначает момент, в который резерв страховой компании впервые становится отрицательным. Вместе с тем, применительно к процессу информационного противоборства получение одной сторон временного преимущества на определенном этапе цикла управления не означает достижения информационного превосходства на этом цикле в целом. Кроме того, предположение о пуассоновском распределении плотности вероятностей поступления страховых премий и наступления моментов страховых выплат, позволяющее существенно упростить описание процесса риска страховой компании, нуждается в дополнительном анализе на предмет возможности его использования при описании количества информационных контактов каждой из сторон в ходе информационного противоборства. Как показано в работах [42-53], распределение плотности вероятностей ущерба систем вследствие действий нарушителя может характеризоваться различными законами. Нахождение закона распределения для плотности вероятностей как количества информационных контактов сторон, так и временного преимущества, полученного ими в результате этих контактов, является крайне интересным развитием моделей процесса риска страховой компании применительно к формализации показателя информационного превосходства.

Заключение

Проведенный анализ показал, что искомые для формализации показателя информационного превосходства математические модели должны включать в себя как подходы, принятые в актуарной математике для описания процесса функционирования страховой компании, так и элементы математической теории оценки и управления рисками в информационных системах. Подобный симбиоз делает возможным описание информационного противоборства как двустороннего процесса, с оценкой вероятности получения временного преимущества для каждой из сторон.

Новизной такого подхода является взаимосвязь показателя информационного превосходства, в общем виде определяемого выражением (4), с показателями эффективности подсистем РМ и РЭБ – прироста временного превосходства вследствие общего количества информационных контактов с объектами информационного пространства противостоящей стороны. Определение законов распределения для плотности вероятностей этих величин позволит

формализовать оптимальное количество информационных контактов из $N_+(t)$ для каждой из подсистем РМ и РЭБ в целях максимизации величины временного превосходства на цикле управления $\sum_{i=1}^{N_+(t)} \zeta_i$ и, следовательно, показателя информационного превосходства $\nu(\tau, R_0)$ в целом.

Литература

1. Донсков Ю. Е., Зимарин В. И., Илларионов Б. В. Подход к построению систем радиоэлектронной борьбы в условиях реализации сетецентрических концепций развития вооруженных сил // Военная мысль. 2015. № 2. С. 40-48.

2. Выпасняк В. И., Гуральник А. М., Тиханычев О. В. Система поддержки принятия решений как «виртуальный штаб» // Военная мысль. 2015. № 2. С. 23-29.

3. Воробьев И. Н., Киселев В. А. Киберпространство как сфера непрямого вооруженного противоборства // Военная мысль. 2014. № 12. С. 21-28.

4. Скоков С. И., Грушка Л. В. Влияние концепции сетецентризма на эволюцию и функционирование системы управления Вооруженными Силами Российской Федерации // Военная мысль. 2014. № 12. С. 33-41.

5. Кузнецов В. И., Донсков Ю. Е., Никитин О. Г. К вопросу о роли и месте киберпространства в современных боевых действиях // Военная мысль. 2014. № 3. С. 13-17.

6. Богданов А. Е., Попов С. А., Иванов М. С. Перспективы ведения боевых действий с использованием сетецентических технологий // Военная мысль. 2014. № 3. С. 3-12.

7. Антонович П. И., Макаренко С. И., Михайлов Р. Л., Ушанев К. В. Перспективные способы деструктивного воздействия на системы военного управления в едином информационном пространстве // Вестник Академии военных наук. 2014. № 3 (48). С. 93-101.

8. Троценко К. А. Информационное противоборство в оперативно-тактическом звене управления // Военная мысль. 2016. № 8. С. 20-25.

9. Михайлов Р. Л. Анализ научно-методического аппарата теории координации и его использования в различных областях исследований // Системы управления, связи и безопасности. 2016. № 4. С. 1-29. URL: http://sccs.intelgr.com/archive/2016-04/01-Mikhailov.pdf (дата обращения 05.12.2017).

10. Черноруцкий И. Г. Методы принятия решений. – СПб.: БХВ-Петербург, 2005. – 416 с.

11. Антонова А. С., Аксенов К. А. Многокритериальное принятие решений в условиях риска на основе интеграции мультиагентного, имитационного, эволюционного моделирования и численных методов // Инженерный вестник Дона. 2012. Т. 23. № 4-2. С. 99.

12. Горелик В. А., Золотова Т. В. Общий подход к моделированию процедур управления риском и его применение к стохастическим и

иерархическим системам // Управление большими системами: сборник трудов. 2012. № 37. С. 5-24.

13. Болдырева Н. Б. Стоимостный подход интегрированному управлению рисками коллективного инвестиционного фонда. Диссертация … докт. экон. наук: 08.00.10. – Екатеринбург: Уральский государственный экономический университет, 2011. – 317 с.

14. Хрусталев Б., Вяцкая Н. Концептуальные и научные подходы к управлению рисками предприятий строительного комплекса // РИСК: Ресурсы, Информация, Снабжение, Конкуренция. 2014. № 2. С. 260-265.

15. Милль Дж. С. Основы политической экономии. – М.: Прогресс, 1981.

16. Райзберг Б. А. Предпринимательство и риск. – М.: Знание, 1992. – 64 с.

17. Хохлов Н. В. Управление риском. – М.: ЮНИТИ-ДАНА, 1999. – 239 с.

18. Грачева М. В. Анализ проектных рисков. – М.: Финстатинформ, 1999. – 216 с.

19. Чернова Г. В., Кудрявцев А. А. Управление рисками. – М.: Проспект, 2008. – 160 с.

20. Альгин А. П. Риск и его роль в общественной жизни. – М.: Мысль, 1989. –187 с.

21. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций. – М.: Дашков и Ко, 2003. – 544 с.

22. Воронцовский А. А. Управление рисками. – М.: ЮНИТИ-ДАНА, 2004. – 458 с.

23. Рыхтикова Н. А. Анализ и управление рисками организации. – М.: ИНФРА-М, 2007. – 240 с.

24. Порфирьев Б. Н. Концепция риска, который никогда не равен нулю // Энергия. 1989. № 8. С. 31-33.

25. Ступаков В. С., Токаренко Г. С. Риск-менеджмент. – М.: Финансы и статистика, 2005. – 288 с.

26. New Webster’s Dictionary of the English Language. College Edition. – Delhi: Subject Publications, 1999.

27. Балабанов И. М. Риск-менеджмент. – М.: Финансы и статистика, 1996. – 313 с.

28. Доля В. К., Лежнева Е. И. К управлению рисками в системах логистики // Вісник Дніпропетровського національного університету залізничного транспорту ім. академіка В. Лазаряна. 2008. № 25. С. 149-151.

29. Сеньков А. В., Борисов В. В., Боряков А. В., Гаврилов А. И. Подход к управлению рисками в сложных организационно-технических системах // Вестник МЭИ. 2013. № 5. С. 156-161.

30. Алексеев В. В., Соложенцев Е. Д. Логико-вероятностный подход к управлению риском и эффективностью в структурно-сложных системах // Информационно-управляющие системы. 2009. № 6. С. 67-71.

31. Клочкова Н. В. Управление финансовыми рисками как инструмент управления финансовыми ресурсами энергетических компаний // Финансы и кредит. 2007. № 22 (262). С. 45-49

32. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.

33. Морозов А. В., Майбуров Д. Г., Чукляев И. И. Информационное оружие: теория и практика применения // Проблемы безопасности российского общества. 2014. № 2. С. 177-183.

34. ГОСТ Р 51897–2002 Менеджмент риска. Термины и определения. Издания. Международный стандартный книжный номер. Использование и издательское оформление. – М.: Изд-во стандартов, 2002. – 5 с.

35. Макаренко С. И., Чукляев И. И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1 (2). С. 13-21.

36. Чукляев И. И. Управление рисками защищенности распределенных информационно-вычислительных систем // Системы компьютерной математики и их приложения. 2015. № 16. С. 110-112.

37. Чукляев И. И. Метод и модели комплексного управления рисками нарушения защищенности информационно-управляющих систем. Монография. – Смоленск: ВА ВПВО ВС РФ, 2015. – 141 с.

38. Борисов В. В., Круглов В. В., Федулов А. С. Нечеткие модели и сети. Монография. – М: Горячая линия - Телеком, 2012. – 284 с.

39. Чукляев И. И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. № 4 (17). С. 61-71.

40. Завгородний В. И. Информационные риски и информационные системы // Информационные технологии в проектировании и производстве. 2008. № 1. С. 138-140.

41. Королев В. Ю., Бенинг В. Е., Шоргин С. Я. Математические основы теории риска. – М.: Физматлит, 2011. – 591 с.

42. Остапенко А. Г. Методика расчета риска и его параметров для дискретных распределений вероятностей ущерба // Информация и безопасность. 2006. № 1. С. 124-126.

43. Остапенко О. А. Методика оценки параметров риска с применением непрерывных распределений вероятностей ущерба // Информация и безопасность. 2006. № 4. С. 55-58.

44. Остапенко А. Г., Афанасьев А. С. Железняк В. П. Функции относительной чувствительности риска к изменению параметров безопасности для распределения Маркова-Пойа // Информация и безопасность. 2007. № 1. С. 559-564.

45. Остапенко О. А., Нартов А. Н., Боев С. А. Непрерывное Бета-распределение плотности вероятностей ущерба систем при оценке их рисков и защищенности // Информация и безопасность. 2006. № 2. С. 94-97.

46. Остапенко О. А., Барабанщиков И. П., Сазонова Е. А. Оценка рисков и защищенности систем для непрерывного U-распределения плотности вероятностей ущерба защищенности // Информация и безопасность. 2006. № 2. С. 86-89.

47. Остапенко Г. А., Казьмин О. А., Субботина Е. В., Пентюхин А. В. Методика оценки защищенности для пуассоновского дискретного распределения вероятностей ущерба от компьютерных атак // Информация и безопасность. 2006. № 1. С. 100-103.

48. Линец А. Л., Остапенко О. А., Кобышев В. Г., Субботина Е. В., Назаров А.Н. Безопасность систем при Коши-распределении плотности вероятностей их ущерба // Информация и безопасность. 2006. № 1. С. 96-99.

49. Остапенко А. Г., Попова Е. В. Чувствительность нормированного риска для величины вероятности ущерба, распределенной по закону Паскаля // Информация и безопасность. 2007. № 3. С. 503-506.

50. Суботина Е. В., Остапенко О. А., Александров И. С. Логарифмическое нормальное распределении плотностей вероятностей ущерба систем в задачах оценки рисков и их защищенности // Информация и безопасность. 2006. № 2. С. 98-101.

51. Паниткин Д. В., Щербаков В. Б. Оценка риска и защищенности систем для гипергеометрического дискретного распределения вероятностей ущерба защищенности // Информация и безопасность. 2007. № 3. С. 515-518.

52. Андреев Д. А., Остапенко А. Г., Филиппов Ю. Е. К вопросу о принятии решения при управлении риском // Информация и безопасность. 2007. № 3. С. 469-474.

53. Остапенко Г. А., Карпеев Д. О., Плотников Д. Г., Батищев Р. В., Гончаров И. В., Маслихов П. А., Мешкова Е. А., Морозова Н. М., Рязанов С. А., Субботина Е. В., Транин В. А. Риски распределенных систем: методики и алгоритмы оценки и управления // Информация и безопасность. 2010. № 4. С. 485-530.

References

1. Donskov Y. E, Zimarin V. I., Illarionov B. V. An Approach to Construction of Electronic Warfare System in the Conditions of Realized Network-Centric Concepts of the Armed Forces' Development. *Military Thought*, 2015, no. 2, pp. 40-48 (in Russian).

2. Vypasnyak V. I., Guralnik A. M., Tikhanychev O. V. Decision Support System as a «Virtual Headquarters». *Military Thought*, 2015, no. 2, pp. 23-29 (in Russian).

3. Vorobyov I. N, Kiselyov V. A. Cyberspace as a Sphere of Indirect Armed Confrontation. *Military Thought*, 2014, no. 12, pp. 21-28 (in Russian).

4. Skokov S. I., Grushka L. V. Influence of Network Centrism Concept on Evolution and Functioning of the Control System of the Armed Forces of the Russian Federation. *Military Thought*, 2014, no. 12, pp. 33-41 (in Russian).

5. Kuznetsov V. I., Nikitin O. G. On the Role of Cyberspace in Modern Warfare. *Military Thought*, 2014, no. 3, pp. 13-17 (in Russian).

6. Bogdanov A. Ye., Popov S. A., Ivanov M. S. Prospects of Warfare Using Network-Centric Technologies. *Military Thought*, 2014, no. 3,. pp. 3-12 (in Russian).

7. Antonovich P. I., Makarenko S. I., Mihailov R. L., Ushanev K. V. New Means of Destructive Effects on Network Centric Military Command, Control and Communication Systems in the Common Information Space. *Vestnik Akademii voennykh nauk*, 2014, no. 3, pp. 93-101 (in Russian).

8. Trotsenko K. A. Information Warfare at the Operational-Tactical Level of Control. *Military Thought*, 2016, no. 8, pp. 20-25 (in Russian).

9. Mikhailov R. L. An Analysis of the Scientific and Methodological Apparatus of Coordination Theory and its Use in Various Fields Of Study. *Systems of Control, Communication and Security*, 2016, no. 4, pp. 1-29. URL: http://sccs.intelgr.com/archive/2016-04/01-Mikhailov.pdf (accessed 18 September 2017) (in Russian).

10. Chernorutskii I. G. *Metody priniatiia reshenii* [Methods of Decision Making]. Saint-Peterburg, BKhV-Peterburg Publ, 2005. 416 p. (in Russian)

11. Antonova A. S., Aksenov K. A. Mnogokriterial'noe priniatie reshenii v usloviiakh riska na osnove integratsii mul'tiagentnogo, imitatsionnogo, evoliutsionnogo modelirovaniia i chislennykh metodov [Multi-Criteria Decision-Making under Risk Based on the Integration of Multi-Agent, Simulation, Evolutionary Modeling and Numerical Methods]. *Engineering journal of Don*, 2012, no 4-2. vol. 23. p. 99 (in Russian).

12. Gorelik V. A., Zolotova T. V. Obshchii podkhod k modelirovaniiu protsedur upravleniia riskom i ego primenenie k stokhasticheskim i ierarkhicheskim sistemam [General Approach to Modeling of Risk Management Procedures and Its Application to Stochastic and Hierarchical Systems]. *Large-scale Systems Control*, 2012, no 37, pp. 5-24 (in Russian).

13. Boldyreva N. B. *Stoimostnyi podkhod integrirovannomu upravleniiu riskami kollektivnogo investitsionnogo fonda*. Dis. dokt. ekon. nauk [The Cost Approach to Integrated Risk Management of a Collective Investment Fund. Ph.D. Tesis]. Ekaterinburg, Ural State University of Economics, 2011. 317 p. (in Russian).

14. Khrustalev B., Viatskaia N. Kontseptual'nye i nauchnye podkhody k upravleniiu riskami predpriiatii stroitel'nogo kompleksa [The Conceptual and Scientific Approaches to the Risk Management of Construction Enterprises]. *RISK: Resursy, Informatsiia, Snabzhenie, Konkurentsiia*, 2014, no 2, pp. 260-265 (in Russian).

15. Mill J. S. *Fundamentals of political economy*. London, 1848.

16. Raizberg B. A. *Predprinimatel'stvo i risk* [Entrepreneurship and Risk]. Moscow, Znanie Publ., 1992. 64 p. (in Russian).

17. Khokhlov N. V. *Upravlenie riskom* [Management Risk]. Moscow, IuNITI-DANA Publ., 1999. 239 p. (in Russian).

18. Gracheva M. V. *Analiz proektnykh riskov* [Analysis of Design Risks]. Moscow, Finstatinform Publ., 1999. 216 p. (in Russian).

19. Chernova G. V., Kudriavtsev A. A. *Upravlenie riskami* [Management of Risks]. Moscow, Prospekt Publ., 2008. 160 p. (in Russian).

20. Al'gin A. P. *Risk i ego rol' v obshchestvennoi zhizni* [Risk and its Role in Public Life]. Moscow, Mysl' Publ., 1989. 187 p. (in Russian).

21. Shapkin A. S. *Ekonomicheskie i finansovye riski. Otsenka, upravlenie, portfel' investitsii* [Economic and Financial Risks. Evaluation, Management, Investment Portfolio]. Moscow, Dashkov i Ko Publ., 2003. 544 p. (in Russian).

22. Vorontsovskii A. A. *Upravlenie riskami* [Management of Risks]. Moscow, IuNITI-DANA Publ., 2004. 458 p. (in Russian).

23. Rykhtikova N. A. *Analiz i upravlenie riskami organizatsii* [Analysis and Risk Management of the Organization]. Moscow, INFRA-M Publ., 2007. 240 p. (in Russian).

24. Porfir'ev B. N. Kontseptsiia riska, kotoryi nikogda ne raven nuliu [The Concept of Risk, Which is Never Equal to Zero]. *Energiia*, 1989, no 8, pp. 31-33 (in Russian).

25. Stupakov V. S., Tokarenko G. S. *Risk-menedzhment* [Risk Management]. Moscow, Finansy i statistika Publ., 2005. 288 p. (in Russian).

26. New Webster's Dictionary of the English Language. College Edition. Delhi, Subject Publications, 1999.

27. Balabanov I. M. *Risk-menedzhment* [Risk Management]. Moscow, Finansy i statistika Publ., 1996. 313 p. (in Russian).

28. Dolia V. K., Lezhneva E. I. K upravleniiu riskami v sistemakh logistiki [To Risk Management in Logistics Systems]. *Visnik Dnipropetrovs'kogo natsional'nogo universitetu zaliznichnogo transportu im. akademika V. Lazariana*, 2008, no. 25, pp. 149-151 (in Russian).

29. Sen'kov A. V., Borisov V. V., Boriakov A. V., Gavrilov A. I. Podkhod k upravleniiu riskami v slozhnykh organizatsionno-tekhnicheskikh sistemakh [The Approach to Risk Management in Complex Organizational and Technical Systems]. *Vestnik MEI*, 2013, no 5, pp. 156-161 (in Russian).

30. Alekseev V. V., Solozhentsev E. D. A Logical and Probabilistic Approach to Risk and Efficiency Management in Structural Complex Systems. *Informatsionno-upravliaiushchie sistemy*, 2009, no 6, pp. 67-71 (in Russian).

31. Klochkova N.V. Financial Risk Management as a Tool for Managing the Financial Resources of Energy Companies. *Finance and credit*, 2007, vol. 262, no. 22, pp. 45-49 (in Russian).

32. Avetisian A. I., Belevantsev A. A., Chukliaev I. I. Technologies for Static and Dynamic Analysis of Software Vulnerabilities. *Voprosy kiberbezopasnosti*, 2014, vol. 4, no. 3, pp. 20-28 (in Russian).

33. Morozov A. V., Maiburov D. G., Chukliaev I. I. Informatsionnoe oruzhie: teoriia i praktika primeneniia [Information Weapons: Theory and Practice of Application]. *Problemy bezopasnosti rossiiskogo obshchestva*, 2014, no 2, pp. 177-183 (in Russian).

34. State Standard of Russia 51897–2002. Management of Risk. Terms and Definitions. Moscow, Standartov Publ., 2002. 5 p. (in Russian).

35. Makarenko S. I., Chucklyaev I. I. The Terminological Basis of the Informational Conflict Area. *Voprosy kiberbezopasnosti*, 2014, vol. 2, no. 1, pp. 13-21 (in Russian).

36. Chukliaev I. I. Upravlenie riskami zashchishchennosti raspredelennykh informatsionno-vychislitel'nykh sistem [Management of security risks of distributed information and computing systems]. *Sistemy komp'iuternoi matematiki i ikh prilozheniia*, 2015, no. 16, pp. 110-112 (in Russian).

37. Chukliaev I. I. *Metod i modeli kompleksnogo upravleniia riskami narusheniia zashchishchennosti informatsionno-upravliaiushchikh sistem. Monografiia* [The Method and Models of Complex Risk Management for the Violation of Information Management Systems. Monography]. Smolensk, Military Academy of Anti-Aircraft Defense Publ., 2015, 141 p. (in Russian).

38. Borisov V. V., Kruglov V. V., Fedulov A. S. *Nechetkie modeli i seti.* [Fuzzy models and networks. Monography]. Moscow, Goryachaya liniya-Telecom Publ, 2012. 284 p. (in Russian).

39. Chukliaev I. I. Nauchno-metodicheskoe obespechenie kompleksnogo upravleniia riskami narusheniia zashchishchennosti funktsional'no-orientirovannykh informatsionnykh resursov informatsionno-upravliaiushchikh sistem [Scientific and Methodical Support of Complex Risk Management for the Violation of the Protection of Functionally-Oriented Information Resources of Information-Control Systems]. *Voprosy kiberbezopasnosti*, 2016, vol. 17, no. 4, pp. 61-71 (in Russian).

40. Zavgorodnii V. I. Informatsionnye riski i informatsionnye sistemy [Information Risks and Information Systems]. *Informatsionnye tekhnologii v proektirovanii i proizvodstve*, 2008, no 1, pp. 138-140 (in Russian).

41. Korolev V. Iu., Bening V. E., Shorgin S. Ia. Matematicheskie osnovy teorii riska [Mathematical Foundations of the Theory of Risk]. Moscow, Fizmatlit Publ., 2011. 591 p. (in Russian).

42. Ostapenko A. G. Metods of Calculation of Risks and Their Parametres for Discrete Damage Probability Distributions. *Information and Security*, 2006, no. 1, pp. 124-126 (in Russian).

43. Ostapenko O. A. Methods of Assessment of Risks Parameters Using Continuous Damage Probabilities. *Information and Security*, 2006, no. 4. pp. 55-58 (in Russian).

44. Ostapenko A. G., Afanas'ev A. S. Zhelezniak V. P. The Functions of Relative Sensitivity of Risk for Variation of Systems Security Parameters for Markov-Polya's Distribution. *Information and Security*, 2007, no. 1, pp. 559-564 (in Russian).

45. Ostapenko O. A., Nartov A. N., Boev S. A. Continuous Beta-Distribution of the Density of System Damage Probabilities when Assessing its Risks and Proofness. *Information and Security*, 2006, no. 2, pp. 94-97 (in Russian).

46. Ostapenko O. A., Barabanshchikov I. P., Sazonova E. A. Assessment of Risks and Proofness of the Systems for Continuous Normal Selective U-Distribution of the Density of Damage Probabilities. *Information and Security*, 2006, no. 2, pp. 86-89 (in Russian).

47. Ostapenko G. A., Kaz'min O. A., Subbotina E. V., Pentiukhin A. V. Method of Proofness Assessment for the Poisson Discrete Distribution of Damage Probabilities in Computer Attacks. *Information and Security*, 2006, no. 1. pp. 100-103 (in Russian).

48. Linets A. L., Ostapenko O. A., Kobyshev V. G., Subbotina E. V., Nazarov A. N. The Systems Security in the Case of Cauchy-Distribution of Their Damage Probabilities Density. *Information and Security*, 2006, no. 1, pp. 96-99 (in Russian).

49. Ostapenko A. G., Popova E. V. The Sensitivity of the Normalized Risk for the Damage Probability by the Pascal Distribution. *Information and Security*, 2007, no. 3, pp. 503-506 (in Russian).

50. Subotina E. V., Ostapenko O. A., Aleksandrov I. S. Logarithmically Normal Continuous Distribution of the Density of Damage Probabilities in the Tasks of Assessment of Risks and Systems Proofness. *Information and Security*, 2006, no. 2, pp. 98-101 (in Russian).

51. Panitkin D. V., Shcherbakov V. B. The Assessment of Risks and Security of Systems for Hyper Giometric Distribution of Probabilities of Damage Occurrence. *Information and Security*, 2007, no. 3. pp. 515-518 (in Russian).

52. Andreev D. A., Ostapenko A. G., Filippov Iu. E. On the Issue of Decision-Making for Risk Management. *Information and Security*, 2007, no. 3, pp. 469-474 (in Russian).

53. Ostapenko G. A., Karpeev D. O., Plotnikov D. G., Batishchev R. V., Goncharov I. V., Maslihov P. A., Meshkova E. A., Morozova N. M., Ryazanov S. A., Subbotina E. V., Tranin V. A. Risks of the Disributed Systems: Techniques ad Algorithms of the Estimation of Management. *Information and Security*, 2010, no. 4. pp. 485-530 (in Russian).

Статья поступила 9 декабря 2017 г.

Информация об авторе

Михайлов Роман Леонидович – кандидат технических наук. Научно-педагогический работник. Череповецкое высшее военное инженерное училище радиоэлектроники. Область научных интересов: информационное противоборство, маршрутизация информационных потоков, координация подсистем наблюдения и воздействия. E-mail: mikhailov-rom2012@yandex.ru

Адрес: 162622, Вологодская обл., г. Череповец, Советский пр., д. 126.

Analysis of Approaches to the Formalization of the Indicator of Information Superiority Based on the Theory of Assessment and Risk Management

R. L. Mikhailov

Relevance. *Present time, in the armed forces of developed countries, there is a steady trend towards the introduction of the concept of combat management in a network-centric manner. An inherent attribute of this concept is information warfare, that is, a bilateral conflict in the information sphere, which is entrusted to the command, radio monitoring and electronic warfare subsystems at the tactical and operational levels of control. At the same time, the well-known author does not have a formal description of the index of information superiority - a key indicator of the effectiveness of information warfare, which would link the performance indicators of each of these subsystems.* ***The aim of this paper*** *is the analysis of mathematical models of the theory of assessment and risk management for their use in a new subject area - in the field of information warfare.* ***Methods used.*** *The solution of the problem is based on the use of methods of system analysis, as well as methods of induction and deduction of the theory of logic.* ***Result.*** *Based on the analysis of more than 50 sources, the features of mathematical assessment and management of risks in the economic sphere and in the field of information systems security are revealed. Mathematical models that can form the basis for the formalization of the information superiority index are analyzed, ways of their improvement are shown in the interests of an adequate display of the information confrontation process.* ***Novelty.*** *The element of novelty of work is the determination of the need to take into account the purposeful actions of the opposing party in the course of information warfare on the basis of a mathematical apparatus in the field of ensuring the security of information systems, as well as taking into account the playful nature of its conduct and, accordingly, models of risk assessment and management in economic systems, which allow to assess both the possible income due to management decisions and the loss in assets.* ***Practical significance.*** *The presented analysis can be used by specialists to justify new technological solutions in the field of information warfare, as well as by military specialists - to justify new forms and methods of organizing the interaction of diverse forces and means in the conduct of armed struggle. In addition, this analysis will be useful to researchers and job seekers conducting scientific research in the field of coordination in complex multi-level control systems.*

Key words: *risk assessment, risk management, information warfare, information superiority, network-centric principle.*

Information about Author

Roman Leonidovich Mikhailov – Ph.D. of Engineering Sciences. Scientific and pedagogical worker. Cherepovets Higher Military Engineering School of Radio Electronics. Field of research: information warfare, routing of data flow, unified influence of monitoring and rejection means on communication networks. E-mail: mikhailov-rom2012@yandex.ru

Address: Russia, 162622, Vologda region, Cherepovets, Sovetskiy prospect, 126.