УДК 629.039: 351.749

Гончаренко Ю.Ю., д.т.н.; **Касаткина Н.В.,** к.т.н.;
Камышенцев Г.В., **Лазаренко С.В.,** к.т.н.

ОСНОВНЫЕ ПОДХОДЫ К ОЦЕНКЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИЕЙ ТЕРРОРИСТИЧЕСКОГО ХАРАКТЕРА КАК СОСТАВНОЙ ЧАСТИ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

Goncharenko Yu.Yu., Kasatkina N.V., Kamyshentsev G.V., Lazarenko S.V. The main approaches to evaluating the effectiveness of emergency management of a terrorist nature, as part of the risk management process.

The analysis of the origin of the concept of risk and the existing systems of its classification is made in this work, and it was revealed that in modern management systems this concept is used to evaluate potentially dangerous phenomena or as a model of a real phenomenon constructed with the help of certain mathematical tools. The mathematical estimation of risk from the point of view of probability theory and from positions of the theory of fuzzy sets is considered. It is shown that in the description of risks, a function that depends on an infinitely large number of parameters is reduced to the form of the distribution function of one variable using such numerical characteristics of a positive random variable as mathematical expectation, median, quantile, etc. It is proposed as the main criterion for assessing the effectiveness of emergency management of a terrorist Character on the protected object, consider the probability of detection of an attacker on the approaches to the object in certain standard conditions that are provided by the invasion scenario and allow the physical protection system to respond in a timely manner and to suppress the actions of the attackers.

Key words: security, emergency, terrorist attack, the protected object, the object of critical infrastructure, and risk management.

Гончаренко Ю.Ю., Касаткіна Н.В., Камишенцев Г.В., Лазаренко С.В. Основні підходи до оцінки ефективності управління надзвичайною ситуацією терористичного характеру як складової частини процесу управління ризиками.

У роботі виконано аналіз виникнення поняття ризику та існуючих систем його класифікації, при цьому виявлено, що в сучасних управлінських системах це поняття використовується для оцінки потенційно небезпечних явищ або як модель реального явища, що побудована за допомогою певних математичних засобів. Розглянуто математичне оцінювання ризику з точки зору теорії ймовірностей і з позицій теорії нечітких множин. Показано, що при описі ризиків функцію, яка залежить від нескінченно великого числа параметрів, зводять до вигляду функції розподілу однієї змінної, використовуючи такі числові характеристики позитивної випадкової величини, як математичне очікування, медіана, квантилі і ін. Пропонується основним критерієм оцінки ефективності управління надзвичайною ситуацією терористичного характеру на об'єкті, що охороняється, вважати ймовірність виявлення зловмисника на підходах до об'єкта в певних стандартних умовах, які передбачені сценарієм вторгнення і дозволяють системі фізичного захисту своєчасно реагувати і припиняти дії зловмисників.

Ключові слова: забезпечення безпеки, надзвичайна ситуація, терористичний акт, об'єкт критичної інфраструктури, що охороняється, управління ризиками.

Гончаренко Ю.Ю., Касаткина Н.В., Камышенцев Г.В., Лазаренко С.В. Основные подходы к оценке эффективности управления чрезвычайной ситуацией террористического характера как составной части процесса управления рисками.

В работе выполнен анализ возникновения понятия риска и существующих систем его классификации, при этом выявлено, что в современных управленческих системах это понятие используется для оценки потенциально опасных явлений либо как модель реального явления, построенная с помощью определенных математических средств. Рассмотрено математическое оценивание риска с точки зрения теории вероятностей и с позиций теории нечетких множеств. Показано, что при описании рисков функцию, зависящую от бесконечно большого числа параметров, сводят к виду функции распределения одной переменной, используя такие числовые характеристики положительной случайной величины, как математическое ожидание, медиана, квантили и др. Предлагается основным критерием оценки эффективности управления чрезвычайной ситуацией террористического характера на охраняемом объекте считать вероятность обнаружения злоумышленника на подходах к объекту в определенных стандартных условиях, которые предусмотрены сценарием вторжения и позволяют системе физической защиты своевременно реагировать и пресекать действия злоумышленников.

Ключевые слова: обеспечение безопасности, чрезвычайная ситуация, террористический акт, охраняемый объект, объект критической инфраструктуры, управление рисками.

Введение

В административно-экономической структуре любого суверенного государства имеется совокупность элементов различных инфраструктур, от деятельности которых зависит жизнь граждан и существование всего общества. Выход из строя или нарушение их функционирования в результате террористического акта может вызвать коллапс, паралич или хаос на общегосударственном уровне. Комплекс таких элементов принято называть критической инфраструктурой [1, 2]. В конце 90-х годов в связи с возрастанием террористической угрозы в развитых странах начались дискуссии об уязвимости национальных инфраструктур [3, 4]. В 1998 году директивой 63-го президента США была определена критическая инфраструктура как основные системы, которые имеют материальную или виртуальную платформу и воздействуют на фундаментальность экономики государства [5].

Разработка вопросов безопасности этих объектов является актуальной научной проблемой. Отечественные и зарубежные специалисты в области безопасности охраняемых объектов критической инфраструктуры, несмотря на различные концептуальные подходы в вопросах физической защиты, едины в следующем. Во-первых, главной целью управления чрезвычайной ситуацией террористического характера является недопущение террористического акта на охраняемом объекте. Во-вторых, процесс управления чрезвычайной ситуацией террористического характера начинается с момента законодательного выбора площадки под строительство объекта критической инфраструктуры. В-третьих, процесс управления чрезвычайной ситуацией террористического характера является составной частью процесса управления рисками [6-15]. В связи с этим возникает вопрос, имеющий научное и прикладное значение, – как оценить эффективность управления чрезвычайной ситуацией террористического характера.

1. Постановка цели и задач научного исследования

Целью данной работы является рассмотрение основных подходов к оценке эффективности управления чрезвычайной ситуацией террористического характера на охраняемом объекте критической инфраструктуры как составной части процесса управления рисками.

Для достижения поставленной цели необходимо решить следующие научные задачи. Во-первых, проанализировать закономерности возникновения понятия риска, существующие его классификации и методы использования в управленческих системах. Во-вторых, рассмотреть математическое оценивание риска методами теории вероятностей. В-третьих, рассмотреть оценку риска с позиций теории нечетких множеств. В-четвертых, обосновать возможность оценки эффективности процесса управления чрезвычайной ситуацией террористического характера путем оценки работы системы физической защиты охраняемого объекта критической инфраструктуры, направленной на своевременное обнаружение и пресечение деятельности злоумышленников.

2. Использование понятия риска в управленческих системах

Риск – это характеристика ситуации, имеющей неопределённость исхода при обязательном наличии неблагоприятных последствий [6]. Идти на риск – это значит иметь в виду возможную опасность или действовать наудачу в надежде на счастливый исход.

Слово «риск», по мнению Фасмера, является заимствованным из французского и итальянского языков, которые, в свою очередь, позаимствовали его из древнегреческого от слова, означающего утес или подножие горы. Отсюда термин «рисковать» переводится с французского и итальянского как «лавировать между скал» [7].

Одни авторы термин «риск» применяют к реальному явлению (риск пожара, риск автомобильно-транспортного происшествия), другие – к модели реального явления, построенной с помощью тех или иных математических средств, например, аппарата теории

вероятностей и математической статистики, теории нечетких множеств, интервальной математики.

«Риск – это нежелательная возможность» [8]. Здесь термин «риск» применяется для описания реального события. «Риск – вероятность возникновения убытков или недополучения доходов по сравнению с прогнозируемым вариантом» [9]. В этом случае термин «риск» используется в процессе моделирования реального события с помощью теории вероятностей. Иногда это создает путаницу.

Достаточно типичным является следующее определение [10], которое применяется при разработке автоматизированных систем прогнозирования и предотвращения происшествий на авиационном транспорте. Риск – это мера количественного многокомпонентного измерения опасности с учетом величины ущерба от воздействия угроз для безопасности, вероятности возникновения этих угроз и неопределенности в величине ущерба и вероятности. Авторы этой статьи отмечают, что при выполнении проекта они на каждом этапе выбирают свое, наиболее приемлемое описание риска. На первом этапе они вынуждены остановиться на вероятностно-статистической модели риска, которая характеризуется вероятностью реализации опасности и описанием случайного ущерба его математическим ожиданием. Использование квантилей функции распределения случайного ущерба, а также моделей оценки, анализа и управления рисками на основе теории нечетких множеств и статистики интервальных данных является предметом рассмотрения на следующих этапах выполнения проекта.

Проблема учета безвозвратных людских потерь и потерь, связанных с нанесением вреда здоровью людей, решается путем обращения к данным страховых компаний. Каждым проектом также предусмотрен мониторинг принятых в авиакомпании, заказывающей автоматизированную систему, используемых показателей уровня безопасности полетов с обеспечением автоматизированной процедуры расчета их текущих значений.

Риск сравнительно редко связан с деятельностью субъекта. Объектами риска могут быть материальные объекты, имущественные или иные интересы, жизнь и здоровье человека, окружающая среда. Современная ситуация в теории рисков характеризуется тем, что подавляющая часть работ по оценке, анализу и управлению рисками относится к той или иной конкретной области, например, риску выпуска дефектной продукции, рискам конкурентного окружения, безопасности полетов, рискам персонала, промышленным авариям, экологической безопасности, террористическим рискам, и т. д., и т. п.

В работе [11] описаны основные составляющие риска – единые методы моделирования и описания, анализа характеристик риска, управления им. Наличие общих подходов, понятий и терминов, моделей, оптимизационных постановок управления, позволяющих строить базовые основы теорий риска в конкретных областях, и означает существование единой теории риска. Выделение единой теории риска позволяет единообразно развивать ее частные теории. Здесь также приведена классификация рисков, условно разделенных на шесть групп.

1) Планетарные риски, которые происходят на уровне планеты Земля в целом:

– стихийные бедствия – землетрясения, извержения вулканов, цунами, смерчи, ураганы, наводнения, засухи;

– риски, связанные с космическим пространством – столкновение Земли с астероидом, смена магнитных полюсов планеты Земля;

– риски мировых эпидемий, прежде всего, опасных для жизни;

– риск наступления мирового финансового кризиса или мирового экономического кризиса;

– риски, связанные с изменением климата – глобальное потепление или похолодание и т. д.

2) Глобальные риски, возникающие на уровне одного или нескольких государств:

– риски возникновения революций, переворотов, заговоров;

– риски, связанные с изменением политического или экономического курса государства;

– риски вооруженной агрессии;

– риски международных санкций;

– риски террористических актов;

– демографические и миграционные риски;

– экологические риски и риски истощения природных ресурсов

– риски, связанные с голодом;

– риск возникновения глобальных техногенных катастроф, например, взрыв на АЭС или химическом предприятии;

– риск неспособности государства отвечать по своим долгам (риск дефолта) и пр.

3) Финансовые риски:

– инфляционный риск – риск того, что при росте цен получаемые денежные доходы с точки зрения реальной покупательной способности обесцениваются быстрее, чем растут;

– риск изменения ставки рефинансирования центрального банка;

– риск изменения ставок по процентам;

– риски, связанные с изменением курсов валют;

– риски, связанные с нестабильностью законодательства;

– риски, связанные с противоречивостью нормативных правовых актов и др.

4) Коммерческие риски – риски на уровне непосредственного окружения компании.

5) Производственные (внутренние) риски:

– риск производства дефектной продукции;

– риски, связанные с промышленной безопасностью;

– экологические риски в процессе производства;

– риски ошибок при проектировании продукции и технологии производства;

– социальные риски на производстве и риски персонала;

– риски, связанные с противоправной деятельностью;

– риски потерь, не связанных с сознательной деятельностью людей.

6) Личные риски:

– риск заболевания или внезапной смерти;

– риск нехватки средств существования и риск несчастного случая, не приводящего к смерти;

– риск нанесения вреда со стороны государственных органов и риск получения вреда от природных явлений;

– риск подвергнуться влиянию криминальных элементов и пр.

3. Математическое оценивание риска с точки зрения теории вероятностей

Для оценки риска необходимо определить возможность наступления нежелательного события и ущерб, порожденный риском. В вероятностной модели оценка возможности наступления нежелательного события сводится к вычислению вероятности, то есть оценка возможности возникновения риска является безразмерной величиной, принимающей значения от 0 до 1.

Пусть величина ущерба, порожденного риском, описывается случайной величиной X с функцией распределения $F(x)=P(X<x)$, где x – действительное число, а $P(X<x)$ – вероятность случайного события $X<x$.

Поскольку случайная величина X интерпретируется как величина ущерба, то она является неотрицательной случайной величиной [12]. В зависимости от предположений о свойствах функции распределения $F(x)$ вероятностные модели риска делятся на параметрические и непараметрические [13].

В первом случае предполагается, что функция распределения входит в одно из известных семейств распределений – нормальное (т.е. гауссовское), экспоненциальное или иное. Однако обычно такое предположение является недостаточно обоснованным, так как реальные данные выходят за рамки заранее заданного семейства. Тогда необходимо применять непараметрические статистические методы, не предполагающие, что

распределение ущерба взято из того или иного популярного среди математиков семейства. При использовании непараметрических статистических методов обычно делают допущение, что функция распределения $F(x)$ является непрерывной функцией числового аргумента x [14].

Часто говорят, что поскольку величина ущерба зависит от многих причин, то она должна иметь так называемое нормальное распределение. Это утверждение недостаточно корректно. Всё зависит от способа взаимодействия причин.

Если причины действуют аддитивно, вызванные ими эффекты складываются, то, действительно, в силу Центральной предельной теоремы теории вероятностей есть основание использовать нормальное (гауссово) распределение.

Если же причины действуют мультипликативно, вызванные ими эффекты перемножаются, то в силу той же Центральной предельной теоремы теории вероятностей следует приближать распределение величины ущерба X с помощью логарифмически нормального распределения.

Если же основное влияние оказывает «слабое звено» – заранее известный набор параметров, то согласно теоремам, доказанным академиком АН УССР Б. В. Гнеденко, следует описывать изменение величины ущерба X с помощью распределения из семейства Вейбулла-Гнеденко. Возможно также использование двух других типов предельных распределений крайних членов вариационного ряда [10].

Рассмотрим ситуацию, когда возможная величина ущерба, связанного с риском, описывается функцией распределения $F(x)=P(X<x)$.

Обычно стараются свести функцию, зависящую от большого количества параметров, к функции с минимальным числом переменных, путем введения постоянных величин, прямо или косвенно характеризующих процесс. С этой целью для исследования положительной случайной величины (величины ущерба) часто рассматривают такие ее числовые характеристики, как математическое ожидание, медиана, квантили, т.е. значения $x=x(a)$, при которых функция распределения достигает определенного значения a. Другими словами, значение квантили $x=x(a)$ находится из уравнения $F(x)=a$.

Кроме того, используются такие числовые характеристики случайной величины, как дисперсия σ^2, среднее квадратическое отклонение (квадратный корень из дисперсии, т. е. σ), коэффициент вариации (отношение среднего квадратического отклонения к математическому ожиданию), линейная комбинация математического ожидания и среднего квадратического отклонения (например, правило трех сигм), математическое ожидание функции потерь и т. д. [7-10]. Тогда задача оценки ущерба может сводиться к анализу той или иной из перечисленных выше характеристик.

Чаще всего оценку проводят по эмпирическим данным (по выборке величин ущербов, соответствующих происшедшим ранее аналогичным случаям). При отсутствии эмпирического материала следует использовать экспертные оценки. Наиболее обоснованным является модельно-расчетный метод, опирающийся на модели управленческой, экономической, социально-психологической, эколого-экономической ситуации, позволяющий рассчитать характеристики ущерба.

4. Математическое оценивание риска с позиций теории нечетких множеств

Если модель риска строится в терминах теории нечетких множеств, то риск моделируется нечетким множеством, а его оценка – та или иная характеристика этого множества так же нечеткое множество [15].

Пусть $X=\{x\}$ – универсальное множество, т.е. множество, охватывающее всю проблемную область. Нечеткое множество $A\subseteq X$ представляет собой набор пар $\{(x,\mu^A(x))\}$, где $x\in X$ и $\mu^A: X\to[0,1]$ – функция принадлежности, которая представляет собой некоторую субъективную меру соответствия элемента x нечеткому множеству A.

Величина $\mu^A(x)$ может принимать значения от нуля, который обозначает абсолютную непринадлежность, до единицы, которая, наоборот, говорит об абсолютной принадлежности элемента *x* нечеткому множеству *A*. Иногда удобно рассматривать значение $\mu^A(x)$ как степень совместимости элемента *x* с размытым понятием, представленным нечетким множеством *A*. Часто нечеткое множество $A \subseteq X$ и его функцию принадлежности $\mu^A(x)$ рассматривают как взаимозаменяемые понятия. Если множество $[0,1]$ заменить на $\{0,1\}$, то функция принадлежности будет представлять собой характеристическую функцию обыкновенного (не нечеткого) множества.

Описание риска с помощью вероятностных моделей на первый взгляд отличается от описания с помощью нечетких интервальных моделей, поскольку они по-разному формализуют неопределенность. В теории вероятностей рассматривается статистическая неопределенность, например, «вероятность брака детали равна 0,1». Теория нечетких множеств нацелена на работу с лингвистической неопределенностью, например, «высокая доля брака». Причем последняя называется лингвистической переменной, которая может принимать значения фраз из естественного или искусственного языка. Так, лингвистическая переменная «температура» может принимать значения «высокая» и «низкая». Фразы, значение которых принимает переменная, в свою очередь, являются именами нечетких переменных и описываются нечетким множеством. Однако теория нечетких множеств может быть сведена к теории случайных множеств и тем самым – к теории вероятностей.

Для оценки значений неизвестных переменных иногда удобно использовать методы статистики интервальных данных. С их помощью можно, например, оценить размер инфляции. Эти методы хорошо подходят и для оценки рисков. В рамках интервальной парадигмы под риском для выбранного критерия эффективности понимается возможность получения отрицательного результата, оцениваемая числом *r*, которое может принимать значения от нуля до единицы, то есть $0 \le r \le 1$. Понятие возможности аналогично понятию вероятности, но не опирается на гипотезу о случайности и не предполагает задание плотности вероятности на интервале неопределенности.

5. Оценка эффективности процесса управления чрезвычайной ситуацией террористического характера

Между процессом управления чрезвычайной ситуацией террористического характера на охраняемом объекте и процессом управления рисками совершения террористического акта на охраняемом объекте критической инфраструктуры можно поставить знак равенства, так как непосредственное предотвращение террористического акта возлагается на системы физической защиты, когда действия злоумышленников носят явно враждебный характер, и должны решительно пресекаться.

По существу система физической защиты конкретного объекта должна противостоять системе террористического вторжения на объект. От того, насколько эффективно система физической защиты способна противостоять подготовленной акции, зависит защищенность и целостность охраняемого объекта.

Составной частью системы физической защиты является комплексная система безопасности, которая представляет собой организационно-техническую систему, состоящую из алгоритмически объединенных систем, обеспечивающих защиту объекта от угроз различной природы. В состав этой системы входят сигнализационные рубежи, физические барьеры, персонал контролеров контрольно-пропускных пунктов, стационарных и мобильных постов наблюдения, операторы центрального пульта управления.

Главный принцип построения любой системы обеспечения безопасности – это превентивность. Применительно к системам физической защиты объекта реализация этого принципа означает, что чем раньше будет обнаружена угроза вторжения на объект, и чем своевременнее она будет устранена, тем эффективнее работает система. Иначе говоря,

дальность обнаружения злоумышленников на подходах к объекту является ключевой характеристикой, которая и определяет вероятность обнаружения злоумышленников.

При построении и оценке эффективности систем физической защиты существует два полярных подхода. Первый подразумевает ввод в систему большого штата сил охраны и разработку организационных мероприятий, при этом основной упор делается на человеческий фактор. Второй подход, наоборот, состоит в максимальном использовании технических средств, а силы охраны используются в основном для пресечения действий нарушителей или злоумышленников. Безусловно, оптимальное решение носит промежуточный характер между первым и вторым подходом.

Главной проблемой построения систем физической защиты является разработка сценария вторжения, одна из упрощенных схем которого представлена на рис. 1.

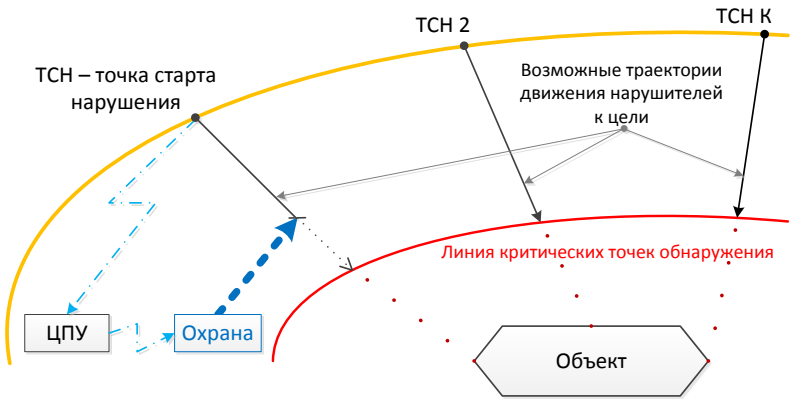

Рис. 1. Схема сценария вторжения на объект

Предполагается, что нарушитель (злоумышленник, террорист, диверсант и пр.) определенным образом движется к охраняемому объекту – объекту террористического акта. На линии точек старта нарушителя (ТСН) срабатывает система обнаружения нарушителя, и сигнал тревоги передается на центральный пульт управления (ЦПУ). Здесь лицом, принимающим решение, дается команда подразделению охраны, которое реагирует и пресекает действия нарушителей, которые должны быть такими, чтобы они успевали перехватить нарушителя до его сближения с объектом, где он может выполнить запланированный террористический акт.

Критическая точка обнаружения – это ближайшая к объекту точка на возможной траектории движения нарушителя, в которой подразделение охраны успевает его нейтрализовать. Построенная линия критических точек обнаружения вокруг охраняемого объекта позволяет определить необходимое количество подразделений для его защиты. Однако следует учитывать тот факт, что злоумышленник может продвигаться самым различным, порой неожиданным, образом, например, ползком, используя средства маскировки, на автомобиле, развивая огромную скорость, на парашюте или дельтаплане, воспользовавшись восходящими потоками воздуха, и т. п.

Кроме того, при разработке сценария вторжения необходимо учитывать, что для достижения цели террористического акта злоумышленники могут использовать самые современные достижения науки и техники. Поэтому в сценарии вторжения для каждого вида средств обнаружения (оптоэлектронных, инфракрасных, акустических, радиолокационных и др.) принимается определенное значение дальности обнаружения злоумышленника, которое принято называть стандартной дальностью обнаружения. Она определяет конкретное значение вероятности обнаружения злоумышленника в контролируемой зоне охраняемого объекта. Это значение является стандартной вероятностью обнаружения злоумышленника $P_{ст}$ и характеризует эффективность работы системы физической защиты по предотвращению

или управлению чрезвычайной ситуацией террористического характера на охраняемом объекте.

В реальной, постоянно изменяющейся обстановке, в зависимости от времени суток (утро, день, ночь, вечер), времени года (зима, весна, лето, осень), гидрометеоусловий (дождь, туман, снег), естественных и искусственных помех дальность обнаружения злоумышленника изменяется, что приводит к изменению вероятности обнаружения злоумышленника в контролируемой зоне. Соответственно, уменьшение вероятности $P_{\text{тек}}$ по сравнению со стандартной свидетельствует об уменьшении эффективности работы системы физической защиты по предотвращению или управлению чрезвычайной ситуацией террористического характера на охраняемом объекте.

Когда принятыми мерами текущее значения дальности обнаружения злоумышленника увеличивается, и, соответственно, текущее значение вероятности обнаружения возрастает и становится больше, чем $P_{\text{ст}}$, эффективность работы системы физической защиты по предотвращению или управлению чрезвычайной ситуацией террористического характера на охраняемом объекте возрастает. Значит, эффективность управления чрезвычайной ситуацией террористического характера на охраняемом объекте может оцениваться как разница значений текущей и стандартной вероятностей обнаружения в контролируемой зоне охраняемого объекта, то есть:

$$P_{\text{эф}} = P_{\text{тек}} - P_{\text{ст}} . \quad (1)$$

Выводы

Основным критерием оценки эффективности управления чрезвычайной ситуацией террористического характера на охраняемом объекте является вероятность обнаружения злоумышленника на подходах к объекту в контролируемой зоне в определенных стандартных условиях, предусмотренных сценарием вторжения, которая позволяет системе физической защиты своевременно реагировать и пресекать действия злоумышленников. Эффективность управления ситуацией в текущий момент времени будет определяться разностью значений текущей и стандартной вероятностей обнаружения злоумышленника в контролируемой зоне охраняемого объекта. Положительное значение разницы будет говорить о положительном, а отрицательное – о негативном эффекте управления.

Список использованной литературы

1. Critical infrastructure – content, structure and problems of its protection [Електронний ресурс] / – Режим доступу: https://www.google.com.ua/?gfe_rd=cr&ei=gVWAWMT9FNKBYOfZnOAE.

2. Хофрейтер Л. Критическая инфраструктура – содержание, структура и проблемы ее защиты [Електронний ресурс] / – Режим доступу: http:/jml2012.indexcopernicus.com/fulltxt.php?ICID=1129729.

3. Hofreiter, L. Ochrana objektov kritickej dopravnej infraštruktúry [Електронний ресурс] / – Режим доступу: http:/jml2013.indexcopernicus.com/fulltxt.php.

4. Linhart, P., Richter, R. Ochrana kritické. [Електронний ресурс] / – Режим доступу: http.//www.mvcr.cz/casopisy/112/3_2003/linhart.html.

5. Presidential Decision Directive 63 [Електронний ресурс] / – Режим доступу: https://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

6. Риск – Википедия [Електронний ресурс] / – Режим доступу: https://ru.wikipedia.org/wiki/%D0%A0%D0 %B8%D1%81%D0%BA.

7. Этимологический онлайн словарь русского языка Макса Фасмера. [Електронний ресурс] / – Режим доступу: https://vasmer.lexicography.online.

8. Орлова А.И. Эконометрика. – М.: Экзамен, 2004. – 576 с.

9. Литовских А.М. Финансовый менеджмент. – Таганрог: Изд. ТРТУ, 2008. – 238 с.

10. Орлов А.И. Экономическая оценка рисков при управлении безопасностью полетов / А.И. Орлов, В.М. Рухлинский, В.Д Шаров // Материалы I Международной конференции

«Стратегическое управление и контроллинг в некоммерческих и публичных организациях: фонды, университеты, муниципалитеты, ассоциации и партнерства»: Выпуск №1 / Под научн. ред. С.Л. Байдакова и С.Г. Фалько. – М.: НП «ОК», 2011. – С. 108–114.

11. Орлов А.И., Пугач О.В. Подходы к общей теории риска [Електронний ресурс] / – Режим доступу: file:///C:/Users/%D0%95%D0%BB%D0%B5%D0%BD%D0%B0/Downloads/UBS4003.pdf.

12. Орлов А.И. Непараметрическое точечное и интервальное оценивание характеристик распределения / А.И. Орлов // Заводская лаборатория. – 2004. – Т. 70, №5. – С. 65–70.

13. Орлов А.И. Об оптимизации выборочного контроля качества продукции / А.И. Орлов // Стандарты и качество. – 1989. – №3. – С. 91–94.

14. Орлов А.И. Организационно-экономическое моделирование в условиях неопределенности и риска / А.И. Орлов // Доклад на научном семинаре Лаборатории экономико-математических методов в контроллинге МГТУ им. Н.Э. Баумана [Електронний ресурс] / – Режим доступу: http://ibm.bmstu.ru/nil/biblio.html#stats-14-neopr.

15. Орлов А.И. Организационно-экономическое моделирование. Ч.2. Экспертные оценки. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2011. – 486 с.

Автори статті

Гончаренко Юлія Юріївна – доктор технічних наук, доцент, Державна установа «Інститут геохімії навколишнього середовища НАН України», Київ, Україна. Тел. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Касаткіна Наталія Вікторівна – кандидат технічних наук, старший науковий співробітник, Державна установа «Інститут геохімії навколишнього середовища НАН України», Київ, Україна. Тел. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Камишенцев Геннадій Володимирович – аспірант, Державна установа «Інститут геохімії навколишнього середовища НАН України», Київ, Україна. Тел. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Лазаренко Сергій Володимирович – кандидат технічних наук, доцент, завідувач кафедри Систем технічного захисту інформації, Державний університет телекомунікацій, Київ, Україна. Тел. +38 067 244 78 67. E-mail: stzi.dut@ukr.net

Authors of the article

Honcharenko Yuliya Yuriyivna – doctor of Science (technic), assistant professor, State Institution "Institute of Environmental Geochemistry NAS of Ukraine", Kyiv, Ukraine. Tel. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Kasatkina Nataliya Viktorivna – candidate of Science (technic), senior researcher, Deputy Director of Research, State Institution "Institute of Environmental Geochemistry NAS of Ukraine", Kyiv, Ukraine. Tel. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Kamyshentsev Gennadiy Volodymyrovych – post-graduate student, State Institution "Institute of Environmental Geochemistry NAS of Ukraine", Kyiv, Ukraine. Tel. +38 067 692 88 02. E-mail: stzi.dut@ukr.net

Lazarenko Sergiy Volodymyrovych - candidate of Science (technic), associate professor, Head of Department of Technical Information protection systems, State University of Telecommunications, Kyiv, Ukraine. Tel. +38 067 244 78 67. E-mail: stzi.dut@ukr.net

Дата надходження в редакцію: 28.03.2017 р. Рецензент: д.т.н., проф. В.Л. Бурячок