УДК: 004.512; 004.421

В.В. Бегун, С.А. Вахнин

Метод решения проблемы расчета техногенных рисков

Рассмотрена возможность применения типовых моделей для оценки величин риска объектов повышенной опасности и упрощенных, доступных широкому кругу пользователей интерфейса ввода–вывода и программного обеспечения для расчетов на основе применения методологии вероятностного моделирования.

Software concept using the typical calculation models for a risk value assessment of dangerous objects based on probability analysis methods with the simple input/output interface for the wide variety of users is proposed.

Розглянуто можливість застосування типових моделей для оцінки величин ризику об'єктів підвищеної небезпеки та спрощених, доступних широкому колу користувачів інтерфейсу вводу–виводу і програмного забезпечення для розрахунків на основі застосування методології ймовірнісного моделювання.

Введение. Необходимость и неизбежность перехода к риск-ориентированному подходу (РОП) в управлении безопасностью в Украине неоднократно обсуждалась, в том числе на уровне правительства. Принятие Постановления Кабмина № 37р [1] завершило все споры в пользу прогресса. Как было сказано [2], этот переход большинство стран совершили более 30 лет назад, Россия – около 15 лет. В целом это выгодно для государства по многим причинам, главная из которых – возможность качественных улучшений безопасности, возможность перехода к стратегии «предупреждения аварий», что в десятки раз сокращает расходы из бюджета. В Украине процессы перехода на передовые методы регулирования безопасности тормозились по ряду причин, одна из которых – сложность информационного и программного обеспечения. В данной статье авторы предлагают создать программное обеспечение с упрощенным интерфейсом пользователя для решения задач расчета рисков объектов повышенной опасности (ОПО).

Основные принципы риск-ориентированного подхода

В соответствии с современными международными стандартами [3–5] уровень безопасности каждого гражданина, промышленных объектов производства, территорий и общества в целом должен определяться уровнем риска. Безопасность – это приемлемый уровень риска. Риск, для целей расчета, определяется как произведение вероятности нежелательного события на его последствия. В каждом конкретном случае риск следует рассчитывать с учетом всех источников опасности, факторов и обстоятельств, способствующих появлению и развитию опасности. Все мероприятия по предотвращению рисков определяются расчетом, который согласуется с опытом. При этом необходимо придерживаться последовательности, рекомендуемой международными стандартами [3]. Порядок приоритетности предупредительных и регулирующих мер таков:

- устранение опасности/риска;
- ограничение опасности/риска в его источнике путем использования технических средств коллективной защиты или организационных мер;
- минимизация опасности/риска путем проектирования безопасных производственных систем, которые включают в себя меры административного ограничения суммарного времени контакта со вредными производственными факторами;
- там, где остались опасности/риски и не могут быть ограничены средствами коллективной защиты, работодатель должен бесплатно предос-

Ключевые слова: безопасность, риск, модель, интерфейс, алгоритм.

тавить соответствующие средства для индивидуальной защиты, включая спецодежду, и принять меры по гарантированному обеспечению их использования и технического обслуживания.

Алгоритм управления безопасностью на основе РОП и информационных технологий может быть представлен такими основными процедурами:

- определение (расчет) риска;
- определение допустимых значений риска;
- сравнение расчетных и допустимых значений;
- принятие решений по предупреждению аварий (уменьшение риска).

Как видим, началом процессов управления безопасностью на основе РОП, ключевой есть процедура определения риска.

Обзор программ расчета рисков

Расчеты рисков проводятся на основе соответствующих моделей. Мировым научным сообществом упорядочены известные типы моделей и методов в виде групп стандартов менеджмента риска [4, 5]. Методы и модели достаточно разнообразны, выбираются исследователем в зависимости от источников риска и целей расчета. Большинство моделей и методов имеют программную реализацию. Для количественного расчета техногенной опасности наиболее подходящими на сегодня считаются программы, основанные на вероятностных моделях, состоящих из вероятных сценариев развития аварийных ситуаций – деревьев событий (ДС) [6] и моделей вероятных отказов оборудования – деревьев отказов (ДО).

Наиболее распространенная программа, реализующая эти алгоритмы, – программа «*SAPHIRE*» (рис. 1). Последняя разработана в лаборатории «*INEEL*» США [6] для расчета рисков от атомных электростанций (АЭС). Первые ее варианты появились в начале 70-х годов прошлого столетия и были известны как программа «*IRRAS*». Это уникальное программное средство позволяет, как было написано в первых изданиях, ответить на вопросы:

Что может идти неправильно? Насколько это опасно? Как это можно предотвратить?

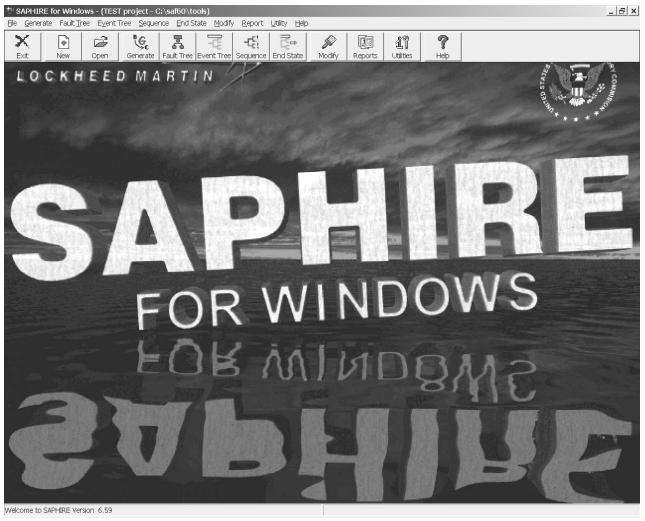

Рис. 1. Главное меню программы *SAPHIRE*

С помощью этой программы выполнены вероятностные анализы безопасности (ВАБ) практически для всех атомных блоков на Земле. Казалось, программа рассчитана на чисто технические системы, но применялась она и для других расчетов, в том числе социальных рисков. Главные из условий ее применения – знание методологии, умение общаться с непростым интерфейсом и, безусловно, доскональное знание моделируемой системы. Из этого следует, что работе с программой должно предшествовать соответствующее теоретическое обучение и практика, а также знание процессов моделируемой отрасли. Все это и высокая стоимость программы создают трудно преодолимый барьер ее массового использования в целях техногенной безопасности объектов повышенной опасности (не АЭС) в Украине. Как уже упоминалось, «*SAPHIRE*» – одна из лучших универсальных программ по многим параметрам, другие программы такого типа менее универсальны, но также требуют специальной подготовки пользователей. В ядерной отрасли все эксперты изначально проходили подготовку за рубежом, с конца 90-х годов была организована подготовка на кафедрах вузов Украины.

Программное обеспечение, ввиду возможных трансграничных угроз радиационных аварий, передавалось Украине бесплатно. Поскольку вначале нового столетия появились норма-

тивные и законодательные требования расчета риска для всех ОПО, необходимо было решать и соответствующие задачи моделирования и создания универсального (доступного) программного обеспечения (ПО).

Основные требования к расчетным моделям и ПО для оценок техногенных рисков, по аналогии с существующими моделями для АЭС, можно сформулировать так:

- модели процессов и систем должны быть достаточно детализированы, содержать элементы систем безопасности, отражать процессы с минимально достаточной неопределенностью.
- Модели должны быть достаточно полными, учитывать все режимы работы предприятия и уровень подготовки персонала.
- Интерфейс программного обеспечения должен быть доступен (понятен) для специалиста, незнакомого с методологией модели. Он должен быть естественным, к примеру, иметь вид анкеты.

Выполнение этих требований, упрощение задачи моделирования и расчетов возможно созданием *типовых моделей* по опасным отраслям производства.

Типовая модель

На основании опыта моделирования систем АЭС можно утверждать, что все объекты могут быть представлены в виде некоторого множества типовых (вероятностных) моделей.

Здесь и далее *типовой моделью* $М_т$ будем называть вероятностную структурно-логическую модель (ВСЛМ) однотипных объектов $\check{O}$:{n, S, P_n} отрасли с приблизительно одинаковым набором элементов $n \in N$ и систем безопасности S:{S_i(Б), S_i(ВБ), S_i(Н)} (одинаковый проект), предназначенных для достижения одинаковых целей и выполнения функций Φ_i при существующем уровне подготовки персонала P_n. Системы безопасности могут быть представлены разными подклассами, как в атомной энергетике: S_i(Б) – *системы безопасности*, находящиеся при нормальной работе в режиме «ожидания», S_i(ВБ) – *системы*, *важные для безопасности*, которые могут быть в работе при нормальных условиях и S_i(Н) – *системы нормальной эксплуатации.* Примером типовой модели могут быть модели: нефтебазы, автозаправки, котельной и др.

Поскольку число групп K однотипных объектов $\check{O}$ в отрасли ограничено, задача в такой постановке имеет смысл. Действительно, если существует типовая модель $М_т$:$\langle n, J, S_j, S_i \rangle$ объектов (например, нефтебаз) с приблизительно одинаковым набором элементов n (одинаковый проект), определенными исходными событиями J, то ВСЛМ может иметь одинаковые сценарии S_J – ДС, одинаковые модели систем S_i – ДО и, как следствие, тождественные расчеты и процедуры мониторинга. В типовой модели вероятностные характеристики базисных событий рассчитываются на основе среднестатистических данных по отрасли, а риск R есть функционалом на множестве основных параметров.

$$\check{O} \leftrightarrow R = \Phi(J, K, S_i(\text{Б}), S_i(\text{ВБ}), S_i(\text{Н}), P_\text{П}). \quad (1)$$

Создание типовой модели позволяет не только существенно упрощать расчеты риска конкретных ОПО, но и таким образом делает возможным мониторинг текущего риска объекта на основе этой модели $М_т$ [7]. Типовая модель $М_т$ по сути может быть принята в целях мониторинга, если у нее определены следующие составляющие (элементы): цель, критерии приемлемости риска $\{R_i\} < [R]$, анализ исходных событий (J), сценарии – S_J, анализы надежности систем – S_i, анализы надежности персонала P_n, если выполнено объединение модели – связывание $<М_т>$ и расчеты конечных состояний $<K_s>$. Таким способом расчет ВСЛМ объекта на основе типовой модели может быть сведен к простым процедурам учета отличий $<\Delta М_т>$.

Задача разработки типовой модели может выполняться специалистами самой высокой квалификации, компетентными как в теории моделирования, так и в практике применения расчетных программ и управления объектом. Заметим, что собственно так и происходили эти процессы в ядерной отрасли. Группа Расмуссена, выполнившая первые расчеты [6], создала типовую ВСЛМ атомного блока, все остальные тысячи расчетов фактически были не существенной модификацией, а в некоторых

случаях – их повтором с учетом надежности оборудования. Таким способом задачу моделирования ОПО с целью расчета риска можно свести к двум, решаемым последовательно:

- создание и анализ типовой модели $М_т$;
- расчет для конкретного объекта по образцу типовой модели для учета отличий $<\Delta М_т>$ реального объекта $\breve{О}$ и типового $\breve{О}_m$ (адаптация типовой модели).

Процедуры учета отличий модели объекта от типовой модели для мониторинга

Создание типовой модели – это возможность использования ВСЛМ, разработанной специалистами высокой квалификации для всех объектов отрасли путем учета отличий $<\Delta М_т>$ объекта от типового. Поскольку по определению индексы-размерности параметров модели (m) всегда больше индексов-размерностей параметров объекта (i), то алгоритм адаптации, по сути, есть алгоритмом упрощения:

- по количеству оборудования (n): $n_i \le n_m$;
- по системам: $S_i \le S_m$;
- по уровню подготовки персонала: $(P_П)_i > (P_П)_m$.

Если существует единая типовая модель $М_т$ безопасности родственных предприятий $\breve{О}$ на основе среднестатистических данных одной отрасли, то для оценки состояния безопасности конкретного предприятия можно пользоваться упрощенным алгоритмом на основе кода *SAPHIRE* (рис. 2):

1. Проверить соответствие перечня требований безопасности предприятия и тех, что учтены в модели. Все требования отрасли должны быть учтены и выполняться на предприятии.

2. Если какое-то требование безопасности отрасли не выполняется, вероятность соответствующего базисного события предприятия в типовой модели принимается за единицу, т.е. соответствующее событие модели учитывается как достоверное (не выполненное требование).

3. Выполнить обработку статистических данных по безопасности конкретного предприятия при условии существования среднестатистических данных одной отрасли на основе формул Байеса.

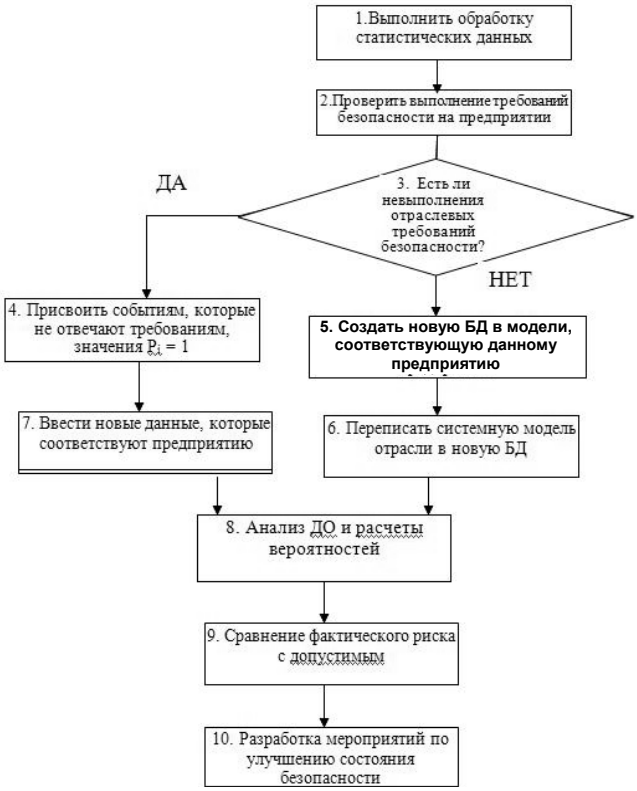

Рис. 2. Алгоритм адаптации типовой модели

4. Создать блок данных (в коде) в модели, после чего существующая модель оценки состояния безопасности отрасли копируется в эту новую базу данных.

5. Присвоить в модели всем базисным событиям, не соответствующим требованиям типовой модели отрасли значения $P_i = 1$ (достоверные события).

6. Переписать системную модель отрасли в новое семейство (проект). При этом переписываются все системные деревья отказов вместе с данными по безопасности в отрасли, существующие после создания модели оценки состояния безопасности отрасли на основе среднестатистических данных отрасли.

7. Ввести новые, определенные на втором и третьем шагах, данные, соответствующие этому предприятию и полученные при выполнении процедуры проверки.

8. Выполнить процедуры общего алгоритма ВАБ по анализу систем и расчетов [6].

Как видим, этот алгоритм значительно проще благодаря использованию типовой модели $М_т$, созданной заранее. Процедуры 1–4 – это подготовка данных, процедуры 7 и 8 – ввод данных и проведение расчетов, они не отличаются от общего алгоритма ВАБ [6].

Процедуры 5 и 6 – специфические процедуры программного кода *SAPHIRE*. Смысл этих процедур заключается в том, что модель приспосабливается под данные конкретного предприятия. Выполняются они одним действием на компьютере, т.е. очень просто [6]. Наиболее трудоемкие процедуры алгоритма создания модели – определение исходных и базисных событий, проведение анализа видов последствий и отказов (*FMEA*); построение ДС и ДО в этом алгоритме не выполняются, так как выполнены в типовой модели. Притом, что существуют единые требования к оценке безопасности предприятий одной отрасли, фактически просматриваются и изменяются только входные данные модели. В этом случае успех решения сложной задачи зависит только от интерфейса ввода исходных данных.

Требования к интерфейсу программ типовых моделей

Описанный алгоритм предполагает знание программного кода, но на основе типовых моделей возможны дальнейшие принципиальные упрощения**.** Типовая модель $М_т$ учитывает все требования моделирования ОПО одного класса и потому нет необходимости строить новую модель для каждого объекта $\check{O}$. В принципе отпадает необходимость в специалистах высокой квалификации. По сути, задача расчетчика сводится к подстановке (присвоении) определенных значений переменным модели (базисным событиям): типу объекта (проекта), исходным событиям, режимам работы, системам безопасности, уровню подготовки персонала. Поэтому смысл сложного интерфейса, основанного на структуре ВАБ, отпадает. Соответственные знания, знания моделирования и программы не требуются. Пользователь может относиться к программе расчета риска как к «черному ящику», корректируя параметры входа $[X]$ и получая параметры выхода $[Y]$ (рис. 3).

Рис. 3. Обобщенное представление типовой модели

Предлагается контекстный интерфейс, основанный на задачах проверки безопасности, которые коротко формулируются как процессы выбора:

- тип объекта – $\check{O}_i \leftrightarrow (М_т)_i$ – тип модели;
- источники риска – $<R> \leftrightarrow <J>$ – исходные события;
- системы и элементы безопасности $<S, n> \leftrightarrow <B>$ базисные события; (2)
- подготовка персонала $P_n \leftrightarrow B(P_n)$ учитываемый уровень и количество ошибок;
- представление результатов $<R_i> \leftrightarrow <C(B)>$ таблицы, полученные критерии риска.

Левая часть соотношений (2) может быть отображена в интерфейсе программы в форме подсказок–вопросов (типа анкеты). Рассмотрим требования к такому представлению интерфейса ввода–вывода более подробно, не вдаваясь в тонкости рассматриваемых моделей [6].

Тип объекта – должна быть отображена детализация в соответствии с имеющимися типовыми моделями: название объекта, номер проекта, технологические схемы, основное оборудование, системы безопасности и защит, размеры основных помещений, размеры промышленной площадки (границы объекта) и др.

Соответствие реального оборудования объекта проекту: емкости, насосы, системы безопасности, перечень всего оборудования, включенного в расчет (модель). Поскольку отказы оборудования представляют собой базисные события B_i, возникает необходимость подробного описания каждого элемента системы, включенного в расчет. Должны быть приведены все данные, необходимые для пересчета вероятностных характеристик элемента: соответствие проекту, ресурс элемента, количество отказов за период между проверками, дата последней проверки, соответствие условий эксплуатации проектным требованиям и пр. Все требования к интерфейсу ввода указывают разработчики типовой модели, соотношения для пересчета вероятностных ха-

рактеристик элементов и систем <S, n> также должны быть указаны в модели.

Степень подготовки персонала – должны быть уточнены: укомплектованность персоналом и стаж работы, аттестация и оценка знаний, нарушения производственной и трудовой дисциплины и другие данные, необходимые для пересчета вероятных ошибок персонала. Алгоритм пересчета (расчета) также приводится в модели, после ввода необходимых данных пересчет проводится автоматически. Необходим учет возможных ошибок человека по среднестатистическим данным о подготовке операторов на объекте, но при желании заказчика возможна и конкретизация данных по конкретным рабочим местам.

Такой подход имеет смысл для особо ответственных рабочих мест, где руководитель всегда стремится ставить операторов высокой компетенции. Модель $M_т$ вполне может предоставить такую возможность, поскольку все моделируемые ошибки могут иметь разные идентификаторы [6].

Источники риска – исходные события. Должны быть указаны внутренние и внешние исходные события и возможные ошибки персонала, которые относятся к классу <J>. Пользователь (инспектор) отмечает (выбирает) их из предложенного списка.

Представление результатов – каждая расчетная программа представляет возможности вывода всех результатов расчетов. При инспекционных проверках предлагается в вектор выходных параметров [Y] включать «протокол проверки безопасности объекта». Протокол должен содержать: дату проверки, тип объекта, регистрационный номер в реестре ОПО, тип модели, ее исходные и ссылочные данные, персональные данные состава комиссии и другие официальные данные. Из расчетных параметров в обязательном порядке должны быть указаны все параметры ввода (коррекция типовой модели) и результаты расчета. Последние должны отображать: значение обобщенного параметра безопасности, вероятности возможных конечных состояний при авариях, первые три минимальные срезы (сечения) для обобщенного параметра, таблица значимости базисных событий для обобщенного параметра, результаты расчета неопределенностей для обобщенного параметра R_i. Если значение обобщенного параметра ниже допустимых значений, вывод результатов расчета проводится по требованиям заказчика. Очевидно, будут необходимы исследования и рекомендации по снижению уровня риска.

Предполагаемые технологии для разработки программы расчета рисков

Для реализации программы используется язык программирования *Java*, что дает возможность запуска на практически любой современной операционной системе без необходимости изменения кода и даже перекомпиляции. Хотя для этого и необходимо наличие виртуальной *Java*-машины, которая занимает порядка 100 Мб в установленном виде.

Использование технологии *Hibernate* позволяет работать с разными базами данных на высоком уровне. В качестве локальной базы данных может выступить *H*2 или *SQLite* и удаленного сервера баз данных *PostgresSQL* или *Oracle*, но не исключена возможность использования и других.

Программа будет иметь оконный интерфейс, разработанный с применением библиотеки *Swing*.

Минимальные системные требования для программы с локальной базой данных:

- процессор: одноядерный процессор *Intel* с частотой не ниже 1,5 ГГц.
- ОЗУ: 512 Мб;
- свободное место на диске: 500 Мб;
- разрешение экрана 1024×768.

Детальный интерфейс ввода–вывода разрабатывают создатели типовой модели – разработчики. Примеры скриншотов разрабатываемого интерфейса в нашем понимании представлены на рис. 4 и 5. Важно представить общие принципы и требования моделирования пользователю на понятном ему языке (инженерном). Именно такое представление моделей с отображением реальных инженерных схем, оборудования в процессе аудита техногенной безопасности даст воз-

можность информатизации процессов регулирования безопасности. Модель – «черный ящик» может быть недоступна и неизвестна субъекту проверки риска (инженеру или инспектору).

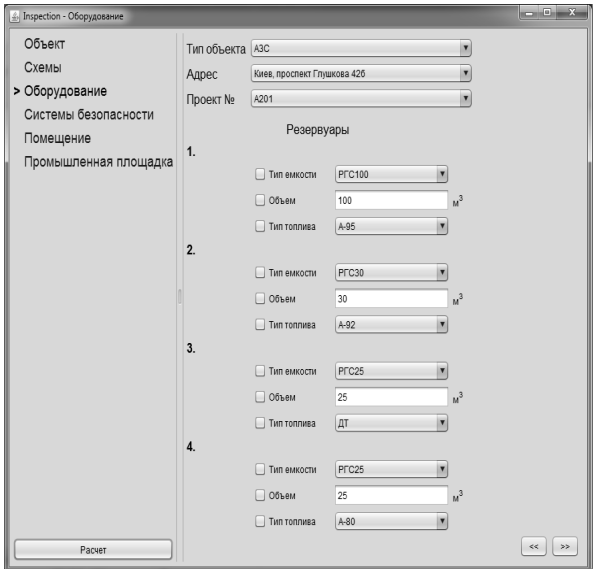

Рис. 4 . Ввод данных об объекте

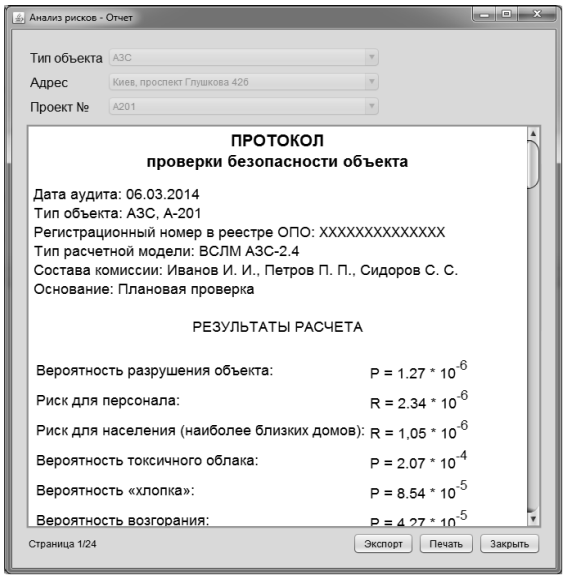

Рис. 5. Протокол проверки риска

В то же время, выполняя простые операции выбора из представляемых списков, инженер, инспектор способен выполнить расчет самостоятельно.

Заключение. На основе анализа процесса моделирования сложной системы доказана практическая возможность определения текущего уровня риска ОПО с малыми затратами времени и ресурсов. Поскольку создание модели ОПО – достаточно сложная и трудоемкая процедура, авторами предложено создание типовых моделей по отраслям производства и использование их для оценок риска объектов повышенной опасности в процессах мониторинга и других целей управления безопасностью.

В случае использования типовой модели возможно создание упрощенного интерфейса расчетных программ. Такой интерфейс позволит адаптировать сложную модель под конкретный объект и выполнить полный вероятностный анализ безопасности пользователям, не знакомым с принципами вероятностного моделирования.

1. *Постанова* КМУ «Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру» від 23.01.2014 № 37 р.
2. *Бєгун В.В.*, *Гречанінов В.Ф.*, *Клименко В.П.* Щодо питань про сучасні методи регулювання безпеки // Математичні машини і системи. – 2013. – № 4. – С. 135–146.
3. *Руководство* по системам управления охраной труда. МОТ–СУОТ 2001 / *ILO–OSH* 2001. – Женева: Международное бюро труда, 2003.
4. *Международный* Стандарт *ISO* 31000. Риск Менеджмент – Принципы и руководства. *ISO* 31000: 2009.
5. *ГОСТ* Р 51901.5-2005. Менеджмент риска: Руководство по применению методов анализа надежности. 01.02.2006.
6. *Вероятностный* анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко и др. – К.: Випол, 2000. – 558 с.
7. *Бегун В.В*. Мониторинг риска объектов повышенной опасности на основе предварительного моделирования: Зб. наук. праць «Моделювання та інформаційні технології». Міжнар. наук. сем. «Моделювання–2010». – К.: ІПМЕ ім. Г.Є. Пухова, 2010. – Т. 1. – С. 152–163.
8. *Java* Runtime Environment 7 Update 51. – http://skisoft.com.ua

Поступила 13.03.2014
Тел. для справок: +38 044 526-5549 (Киев)
E-mail: *begunw@ukr.net*, *sergey@fc*0.*org*