УДК 681.3.06

МЕТОДЫ ОЦЕНИВАНИЯ И УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ

А.А. ЗАМУЛА, А.С. ОДАРЧЕНКО, А.А ДЕЙНЕКО

Обсуждаются актуальные проблемы оценивания рисков в современных информационно-телекоммуникационных системах. Даются рекомендации по управлению рисками информационной безопасности. Подробно рассматривается метод оценивания на основе нечеткой логики.

The paper is devoted to actual problems of estimating risks in modern information-telecommunication systems. Recommendutions on managing information risks of information security are provided. The fuzzy logic-based method of estimating risks are considered in detail.

ВВЕДЕНИЕ

Вопрос об оценивании информационных рисков становится все более актуальным. Сегодня построение и эффективная эксплуатация систем информационной безопасности (ИБ) невозможна без анализа и управления рисками такой системы. Ведь основной задачей данного направления является объективная идентификация угроз и оценка наиболее значимых информационных рисков для организации, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности деятельности предприятия.

Выделяют несколько основных подходов к управлению рисками, различающихся глубиной и уровнем формализма. Например, для некритичных систем, когда информационные ресурсы являются вспомогательными, а уровень информатизации невысокий, предъявляются минимальные требования к оценке рисков. В таких организациях следует вести речь о некотором базовом уровне ИБ, определяемом существующими стандартами, лучшими практиками и опытом. Однако стандарты, которые описывают некоторый базовый набор требований и механизмов безопасности, всегда оговаривают необходимость оценки рисков и экономической целесообразности применения тех или иных механизмов контроля, чтобы выбрать из общего набора требования и механизмов наиболее важные применительно к конкретной организации. Для критичных систем, в которых информационные активы не являются основными, но уровень информатизации очень высок и соответствующие риски могут существенно повлиять на основные бизнес процессы, оценку рисков применять необходимо. Когда же деятельность организации в значительной степени опирается на информационные ресурсы и риски информационной безопасности являются основными, для их оценки необходимо применять формальный подход и количественные методы.

На выбор подхода к оценке рисков помимо характера деятельности организации и уровня информатизации бизнес процессов, также оказывает влияние уровень зрелости организации. В стандарте COBIT и других стандартах. Разделяют три уровня зрелости.

На первом уровне осознание проблем оценивания рисков (ОР) как таковое отсутствует, и в организации предпринимаются фрагментарные меры по обеспечению ИБ, реализуемые специалистами службы защиты информации.

На втором уровне в организации определена ответственность за ИБ, делаются попытки применения интегрированных решений с централизованным управлением и внедрением отдельных процессов управления ИБ.

Третий уровень характеризуется применением процессного подхода к управлению ИБ. Система управления ИБ становится настолько значимой для организации, что рассматривается как необходимый составной элемент системы управления организацией. Однако полноценной системы управления ИБ еще не существует, т.к. отсутствует базовый элемент этой системы – процессы управления рисками.

Управление рисками ИБ – это бизнес задача, инициируемая руководством организации в силу своей информированности и степени осознания проблем ИБ, смысл которой заключается в защите деятельности организации от реально существующих угроз ИБ

1. АРБИТРАЖНАЯ МОДЕЛЬ РЕСУРСНОГО ОБЕСПЕЧЕНИЯ ИБ ОРГАНИЗАЦИОННЫХ СИСТЕМ

Ключевым элементом управления информационными рисками является эффективная методология их снижения за счет реализации определенных контрмер, направленных на ликвидацию существующих уязвимостей и угроз. Основой указанной методологии должен стать механизм эффективного использования имеющихся в наличии ресурсов (финансовых, организационных, технологических и т.д.).

Рассмотрим организационную систему (ОС), состоящую из управляющего центра и агентов $\{a_1,...,a_n\}$. Жизненный цикл основных мер по управлению ИБ может иметь следующий вид.

1. Центр устанавливает для i-го агента уровень допустимого риска $w_i^* \geq 0, i \in n$, который представляет собой приемлемый с точки зрения центра ущерб от реализации возможных угроз.

2. Центр (или агенты) проводят аудит ИБ и анализ рисков, по результатам которого определяется уровень текущего риска w_i^0, $i \in N$, который представляет собой ущерб от реализации возможных угроз до применения каких-либо контрмер, а также уровень остаточного риска $w_i^\infty, i \in N$, который никакими контрмерами не может быть устранен.

3. Агенты a_i сообщают значения $w_i^0, w_i^\infty, i \in n$, центру. Если для некоторого агента $k \in N : w_k^0 \le w_k^*$, то такой агент на данном цикле управления ИБ исключается из рассмотрения.

Для остальных агентов центр на основании установленных значений $w_i^* \ge 0$ и полученных значений $w_k^0, i \in n$, определяет количество ресурсов $b_i \ge 0$, необходимое агенту для снижения текущего уровня риска w_i^0 до уровня допустимого риска w_i^*. Значение $b_i \ge 0, i \in n$, рассматривается как заявка i-го агента. Считаем, что b_i – предполагаемые затраты на создание эффективной системы ИБ (принятие эффективных контрмер).

4. На основании вектора заявок $b = (b_1, ..., b_n)$ центр выделяет количество ресурсов $X = X(b)$. Будем предполагать, что $b_1 + ... + b_n \ge X(b)$, т.е. имеет место дефицит ресурса.

5. Центр, в соответствии с некоторым правилом распределяет ресурс X между агентами $a_i : \pi^*(X) = (\pi_1^*(X), ..., \pi_n^*(X))$, где $\pi_i^*(X) \ge 0$ – объем ресурса, выделенный i-му агенту. При этом $X(b) \ge \pi_1^*(X) + ... + \pi_n^*(X)$.

6. Агенты реализуют контрмеры в объеме полученного ресурса, после чего цикл управления ИБ повторяется.

Целью центра при управлении ИБ является снижение текущих уровней рисков агентов до уровней их допустимых рисков, используя для этого некоторый ресурс.

Пусть задан некоторый объем ресурса $X \ge 0$ и распределение данного ресурса $x = (x_1, ..., x_n)$, такое, что $x_i \ge 0$. Здесь x_i – ресурс, который затрачивается на реализацию контрмер для снижения риска агентом a_i. Сопоставим каждому агенту функцию риска $w_i = w_i(x)$ и предположим, что $w_i(x)$ обладает следующими свойствами:

1. Для $\forall x = (x_1, ..., x_n) : w_i(x) \ge 0, i \in N$.

2. $w_i(0, ..., 0) = w_i{}^0 \ge 0, i \in N$.

3. Для $\forall x^1 = (x_1{}^1, ..., x_n{}^1)$ и $x^2 = (x_1{}^2, ..., x_n{}^2)$, таких, что $x^1 \ge x_i^2, i \in N : w_j(x^1) \le w_j(x^2), j \in N$, причем, если для некоторого

$$k : x_k^1 > x_k^2, \text{ то } w_k(x^1) < w_k(x^2).$$

Из свойств 1-3 следует следующее свойство:

4. Для $\forall j \in N \exists w_j{}^\infty \ge 0$, такое, что $w_j(x) \ge w_j{}^\infty$, для $\forall x = (x_1, ..., x_n) : x_i \ge 0, i \in N$.

Более подробную информацию о функции риска можно получить, например, в [1]. Необходимо отметить что, как правило, конкретный вид функции риска лицу, принимающему решение (ЛПР), неизвестен. Детальный анализ свойств 1-4 функции риска приводится в [2, 3].

Далее предполагаем, что для агентов, участвующих в распределении ресурса, выполняется соотношение:

$$0 \le w_k^\infty \le w_k^* < w_k^0.$$

Обозначим

$$\pi(x) = \left\{ \begin{array}{l} \pi(x) = (\pi_1(x), ..., \pi_n(x)) : \pi_k(x) \ge 0, \\ k \in N, x \ge \sum_{k=1}^n \pi_k(x) \end{array} \right\}$$

– множество возможных распределений ресурса X, между агентами.

Предположим, что ЛПР известен конкретный вид функций риска для всех агентов. Тогда оптимальное распределение ресурса может быть найдено как решение следующей задачи:

$$\max_{i \in N} w_i(\pi(x)) \to \min_{\pi(x) \in \Pi(x)}.$$

Решением данной задачи будет подмножество дележей $\pi^*(X)$, таких, что

$$\pi^*(X) = \arg \min_{\pi(x) \in \Pi(x)} \max_{i \in N} w_i(\pi(x)).$$

Обозначим

$$\pi^*(X) = \left\{ \pi^*(X) = (\pi_1^*(X), ..., \pi_n^*(X)) \right\} \subseteq \pi(X)$$

– множество распределений, являющихся решением задачи.

Решение задачи может быть получено традиционными методами [6], при известных ЛПР функциях риска $w_i(.), i \in N$. Однако, если конкретный вид функций риска агентов неизвестен.

$b_i \ge 0, i \in N$, то задача усложняется.

Утверждение 1. Пусть $w_i(.), i \in N$, удовлетворяют свойствам 1-4, и существует распределение $\pi(X) = (\pi_1(X), ..., \pi_n(X)) \in \pi(X)$, такой, что $X = \sum_{k=1}^n \pi_k(X)$ и

$$w_i(\pi_1(X), ..., \pi_n(X)) = c = const, \text{ для } \forall i \in N.$$

Тогда $\pi(X)$ – единственное решение задачи.

Утверждение 1 показывает, что цель управления ИБ с точки зрения центра может быть сведена к задаче поиска распределения ресурса, приводящего к выравниванию уровней текущих информационных рисков всех агентов на текущем цикле организационного управления. Решение указанной задачи должно представлять собой единое для всех циклов управления ИБ правило распределения ресурса между агентами (организационный механизм управления ИБ), зависящее от заявок агентов.

2. КАЧЕСТВЕННЫЕ МЕТОДИКИ УПРАВЛЕНИЯ РИСКАМИ

Качественные методики управления рисками в технологически развитых странах приняты на вооружение большим количеством внутренних и внешних аудиторов. Эти методики достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 17799 – 2002. Качественные методики позволяют оценить необходимость финансовых затрат. Для качественного анализа необходимо проанализировать источники угроз, систематизировать их по степени возможных потерь, а необходимые контрмеры ранжировать по степени их эффективности [4].

3. КОЛИЧЕСТВЕННЫЕ МЕТОДИКИ УПРАВЛЕНИЯ РИСКАМИ

Актуальность количественных методик, обусловлена необходимостью решения различных оптимизационных задач, которые часто возникают в информационных системах. Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих. Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного WWW сайта или корпоративной E-mail) выбрать с учетом известных ограничений бизнес-ресурсов компании?» Для решения этих задач и разрабатываются методы и методики количественной оценки и управления рисками на основе структурных и реже объектно-ориентированных методов системного анализа и проектирования.

На практике такие методики управления рисками позволяют:

– создавать модели информационных активов компании с точки зрения безопасности;

– классифицировать и оценивать ценности активов;

– составлять списки наиболее значимых угроз и уязвимостей безопасности;

– ранжировать угрозы и уязвимости безопасности;

– обосновывать средства и меры контроля рисков;

– оценивать эффективность/стоимость различных вариантов защиты;

– формализовать и автоматизировать процедуры оценивания и управления рисками.

Одной из наиболее известных методик этого класса является методика CRAMM.

Другим важным направлением минимизации рисков является корпоративная система мониторинга и аудита всех систем, интегрируемая с системой обработки инцидентов.

4. МЕТОДИКА ОЦЕНКИ РИСКА НА БАЗЕ НЕЧЕТКОЙ ЛОГИКИ

В числе вышеперечисленных категорий и методик особый интерес представляет использование аппарата нечеткой логики. Нечеткие описания в структуре методов анализа риска появляются в связи с неуверенностью эксперта при принятии решения о классификации угроз. Методика может быть описана следующим образом.

Определяется переменная g (риск), которая принимает значения от нуля до единицы. Для произвольного отдельного показателя Xi задаем лингвистическую переменную Bi «Уровень показателя Xi». Далее строится набор отдельных показателей $X=\{Xi\}$, $(i=\overline{1,N})$ (в нашем случае $N=2$, $X=\{X1=$ «Величина воздействия», $X2=$ «Вероятность реализации угрозы»}).

Далее каждому показателю Xi ставится в соответствие уровень его значимости для анализа Ri. Чтобы оценить этот уровень, нужно расположить все показатели по порядку убывания значимости. Если система показателей проранжирована в порядке убывания их значимости, то значимость i-го показателя Ri можно определять по правилу Фишберна [5].

Далее строится классификация текущего значения g показателя степени риска как критерий разбиения этого множества на нечеткие подмножества и классификацию текущих значений x показателей X как критерий разбиения полного множества их значений на нечеткие подмножества вида B.

Затем проводится классификация текущих значений Xi по критерию значений x. Результатом проведенной классификации являются уровни принадлежности носителя Xi нечеткому подмножеству Bj.

Для нечетких множеств, как и для обычных, определены основные логические операции. Самыми основными, необходимыми для расчетов, являются пересечение и объединение. Пересечение двух нечетких множеств (нечеткое «И»): A B: $MFAB(x)=min(MFA(x),MFB(x))$. Объединение двух нечетких множеств (нечеткое “ИЛИ”): A B: $MFAB(x)=max(MFA(x),MFB(x))$.

В теории нечетких множеств разработан общий подход к выполнению операторов пересечения, объединения и дополнения, реализованный в так называемых треугольных нормах и конормах. Приведенные выше реализации операций пересечения и объединения – наиболее распространенные случаи t-нормы и t-конормы. Для описания нечетких множеств вводятся понятия нечеткой и лингвистической переменных. Нечеткая переменная описывается набором (N,X,A), где N - это название переменной, X – универсальное множество (область рассуждений), A – нечеткое множество на X. Значениями лингвистической переменной могут быть нечеткие переменные, т.е. лингвистическая переменная находится на

более высоком уровне, чем нечеткая переменная. Каждая лингвистическая переменная состоит из: названия, а также множества своих значений, которые называются базовым терм-множеством T универсального множества X; синтаксического правила G, по которому генерируются новые термы с применением слов естественного или формального языка; семантического правила P, которое каждому значению лингвистической переменной ставит в соответствие нечеткое подмножество множества X. Для каждого лингвистического терма из базового терм-множества T строят функции принадлежности.

Существует свыше десятка типовых форм кривых для задания функций принадлежности. Наибольшее распространение получили: треугольная, трапецеидальная и гауссова функции принадлежности.

Треугольная функция принадлежности (рис. 1) определяется тройкой чисел (a, b, c), и ее значение в точке x вычисляется согласно выражению:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b;\\ 1-\dfrac{x-c}{c-b}, b\le x\le c;\\ 0, \text{ в остальных случаях.}\end{cases}$$

При (b–a) = (c–b) имеем случай симметричной треугольной функции принадлежности, которая может быть однозначно задана двумя параметрами из тройки (a, b, c).

Аналогично для задания трапецеидальной функции принадлежности необходима четверка чисел (a, b, c, d). Значение функции вычисляется в соответствии с выражением:

$$MF(x)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b;\\ 1, b\le x\le c;\\ 1-\dfrac{x-c}{d-c}, c\le x\le c;\\ 0, \text{ в остальных случаях.}\end{cases}$$

При (b–a) = (d–c) трапецеидальная функция (рис.2) принадлежности принимает симметричный вид.

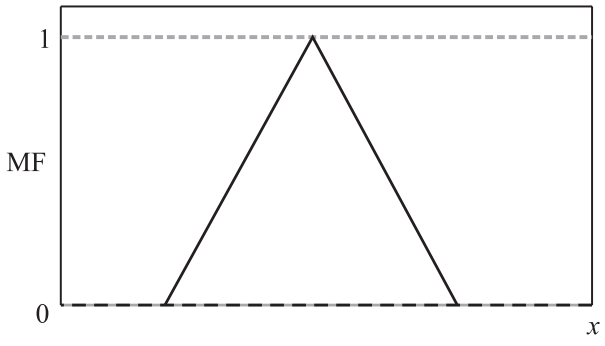

Рис. 1. Треугольная функция принадлежности

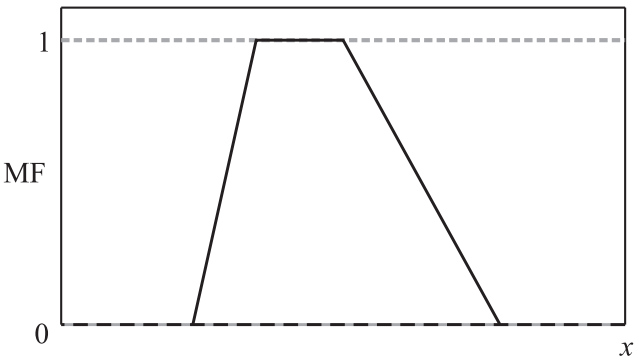

Рис. 2. Трапецеидальная функция

Функция принадлежности гауссова типа (рис. 3) описывается формулой

$$MF(x)=\exp\left[-\left(\frac{x-c}{\sigma}\right)^2\right],$$

и оперирует двумя параметрами: параметр c – обозначает центр нечеткого множества, а параметр σ – отвечает за крутизну функции.

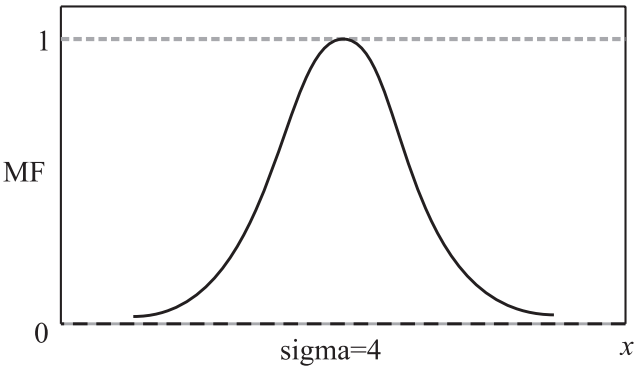

Рис. 3. Гауссова функция принадлежности

В результате применения данного подхода получаются лингвистическое описание степени риска и степень уверенности эксперта в правильности введенной классификации. Тем самым вывод о степени риска приобретает не только лингвистическую форму, но и характеризует качество приведенных утверждений.

Объединение оценок рисков по всем ресурсам дает общую величину риска при имеющейся архитектуре информационной системы и интегрированной в ней системы защиты информации.

Методика позволяет оценивать величину риска с учетом любого числа входных параметров, а также адекватно использовать качественные и количественные оценки входных параметров. Используемый в методике механизм получения оценок риска на основе нечеткой логики позволяет учитывать качество входной и полученной информации. Так, например, результатом оценки риска являются не только численное значение риска и лингвистическое описание степени риска, но и степень уверенности эксперта в правильности введенной классификации.

5. ОСНОВНЫЕ ПРИНЦИПЫ УПРАВЛЕНИЯ РИСКАМИ

Несмотря на различные методики, программные продукты и услуги аудиторов организации необходимо использовать следующие принципы управления рисками информационной безопасности:

– произвести оценивание рисков;

– установить централизованное управление рисками;

– внедрить необходимые политики и соответствующие средства контроля для мониторинга состояния информационных рисков;

– содействовать осведомленности сотрудников в области информационных рисков (ИР);

– контролировать и оценивать эффективность политик и механизмов контроля и управления ИР

Существенным фактором эффективного осуществления этих принципов является связующий цикл деятельности, гарантирующий, что управление информационной безопасностью постоянно нацелено на текущие риски. Важно, чтобы высший менеджмент организации признал наличие рисков нарушения бизнес-процессов, связанных с безопасностью информационных систем. Принятые шаги позволят увеличить осведомленность пользователей об информационных рисках. Эффективность средств контроля подлежит оценке путем различных исследований и аудиторских проверок. Полученные результаты обеспечивают подход к последующей оценке рисков и определяют необходимые изменения в политиках и средствах контроля. Все эти действия централизовано координируются службой безопасности, представителями бизнес-подразделений и менеджмента организации. Цикл управления рисками проиллюстрирован на рис. 4.

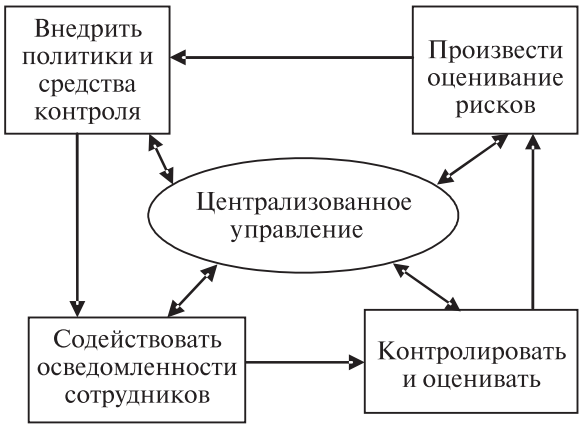

Рис. 4. Цикл управления рисками

6. УМЕНЬШЕНИЕ РИСКОВ

Уменьшение рисков предполагает определение приоритетов, проведение оценок и реализацию соответствующих средств управления сокращением рисков. Поскольку полное устранение риска, как правило, не осуществимо, высшее руководство организации, менеджеры функциональных и бизнес-подразделений несут ответственность за то, чтобы реализовать средства управления и контроля, позволяющие уменьшить риски до приемлемого уровня, с минимальным неблагоприятным воздействием на ресурсы организации. Уменьшение рисков является последовательной и систематизированной методологией, которая должна использоваться высшим руководством с целью уменьшения рисков ИБ.

Уменьшение рисков может быть достигнуто применением любой из перечисленных ниже опций по уменьшению риска.

1. Принятие риска. Принимать потенциальный риск и продолжать использовать информационно – телекоммуникационные системы, либо реализовать средства управления, позволяющие снизить риск до приемлемого уровня.

2. Предотвращение риска. Избегать рисков, устраняя причину риска и/или его последствия (например, воздержаться от использования некоторых функций системы, или закрыть систему, когда риски полностью идентифицированы).

3. Ограничение риска. Ограничивать имеющийся риск, на основе применения средств управления, которые минимизируют неблагоприятное воздействие осуществления угрозы для уязвимости (например, использование поддерживающего,

профилактического или детективного контроля).

4. Планирование риска. Управлять риском, путем разработки плана действий по уменьшению риска, который может предусматривать введение определенных приоритетов, реализацию и проведение контроля.

5. Исследование и уведомление. Уменьшить риск возможных потерь, путем уведомления о наличии уязвимости или недостатков в системе и исследования средств контроля для исправления уязвимости.

6. Перенос риска. Переместить риск, используя другие опции, чтобы получить компенсации за возможные потери, например, путем страхования информационных ресурсов и информационных рисков.

ЗАКЛЮЧЕНИЕ

Выбор подходов к оценке рисков, определяется характером деятельности организации, уровнем ее информатизации, а также уровнем зрелости организации.

При реализации подходов к оцениванию и управлению рисками в организации необходимо опираться, прежде всего, на здравый смысл, существующие стандарты и хорошо зарекомендовавшие себя методологии. Эффективность процесса управления рисками ИБ определяется точностью и полнотой анализа и оценки факторов риска, а также эффективностью используемых в

организации механизмов принятия управленческих решений и контроля их исполнения.

Литература.

[1] *Буянов В.П., Кирсанов К.А., Михайлов Л.М.* Рискология (управление рисками): Учебное пособие. 2-е изд.испр. и доп. / В.П. Буянов, К.А. Кирсанов, Л.М. Михайлов. – М.: «Экзамен», 2003. – 384 с.

[2] *Калашников А.О.* Управление информационными рисками с использованием арбитражных схем // Системы управления и информационные технологии. 2004, № 4 (16). С. 57–61.

[3] *Калашников А.О.* Управление информационными рисками с использованием математического аппарата арбитражных схем/ Материалы Международной конференции и российской научной школы «Системные проблемы надежности, качества информационных и электронных технологий. Информационные бизнес системы». – М.: Радио и связь, 2004. Часть 3. С. 166–174

[4] Сергей Петренко, Сергей Симонов «Методики и технологии управления информационными рисками», IT Manager.

[5] Фишберн П. Теория полезности для принятия решений. – М.: Наука, 1978.

[6] Подиновский В.В., Ногин В.Д. Парето-оптимальные решения многокритериальных задач – М: Наука, 1982. – 382 с.

Поступила в редколлегию 23.09.2009

Замула Александр Андреевич, профессор кафедры БИТ ХНУРЭ, кандидат технических наук, доцент. Область научных интересов: технологии защиты информации в информационно-телекоммуникационных системах.

Одарченко Александр Сергеевич, студент кафедры БИТ ХНУРЭ. Область научных интересов: методы, системы и средства защиты информации в информационно-телекоммуникационных системах.

Дейнеко Анастасия Александровна, студентка факультета компьютерных наук ХНУРЭ. Научные интересы: математическое моделирование, искусственный интеллект, аналитика, программирование, базы данных и компьютерные сети.