УДК 004.056 : 519.81

А.Ю. Быков, А.В. Гуров

ЗАДАЧА ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРИ НЕЧЕТКИХ ПАРАМЕТРАХ ФУНКЦИИ ЦЕЛИ

Рассмотрена задача выбора средств защиты информации от различных атак в автоматизированной системе: выполнена математическая постановка задачи в виде задачи нечеткого математического программирования с булевыми переменными. Введен показатель эффективности, определяемый через оценку среднего предотвращенного ущерба при использовании выбранных средств защиты, для расчета которого используют нечеткие параметры. В качестве ограничений в задаче используется суммарная стоимость выбранных средств защиты. Предложен подход к решению данной задачи, рассмотрен пример решения.

E-mail: abykov@bmstu.ru

Ключевые слова: *защита информации, средства защиты информации, нечеткое множество, нечеткое математическое программирование.*

При выборе средств защиты в автоматизированных системах (АС) могут быть использованы различные математические постановки задач [1, 2].

В работе [2] предложена математическая постановка задачи выбора средств защиты для вычислительной сети. Одним из показателей в этой постановке был показатель эффективности, задаваемый через оценку среднего предотвращенного ущерба при использовании выбранных средств защиты.

Кратко представим основные элементы этой постановки задачи.

Исходные данные. $A = \{a_1, a_2, ..., a_n\}$ – множество возможных актуальных классов атак на информационные ресурсы, $N = \{1, 2, ..., n\}$ – множество индексов этих классов атак;

$B = \{b_1, b_2, ..., b_m\}$ – множество средств защиты от возможных атак (угроз безопасности), $M = \{1, 2, ..., m\}$ – множество индексов средств защиты;

$T = [t_0, t_{\max}]$ – рассматриваемый период функционирования. k_i, $\forall i \in N$, $k_i \geq 0$ – среднее число реализаций *i*-й атаки на интервале *T*, определяется по данным статистики или с помощью экспертов;

$u_i, \forall i \in N$ – средний ущерб от неотражения i-й атаки при ее реализации;

$c_j, j \in M$ – стоимость j-го средства защиты;

$p_{ij}, \forall i \in N, j \in M, p_{ij} \in [0,1]$ – вероятность (или нечеткая мера) предотвращения последствий i-й атаки с помощью j-го средства защиты, определяется по данным статистики или с помощью экспертов.

Показатель качества выбора средств защиты. Введем булеву переменную $x_j \in \{0,1\}$, $\forall j \in M$,

$x_j = 1$, если j-е средство защиты будет применяться в АС для защиты от тех или иных атак;

$x_j = 0$, в противном случае, т. е., если j-е средство не применяется.

Тогда $\boldsymbol{X}$ – вектор булевых переменных $x_j, \forall j \in M$.

Введем показатель качества выбора средств защиты:

$$U(\boldsymbol{X}) = \sum_{i \in N} u_i k_i \max_{j \in M} \{p_{ij} x_j\}. \tag{1}$$

Этот показатель имеет смысл оценки среднего предотвращенного ущерба при использовании средств защиты, определяемых вектором $\boldsymbol{X}$, его значение необходимо максимизировать.

Ограничение.

$$\sum_{j \in M} c_j x_j \le C, \tag{2}$$

где C – максимально возможные затраты, выделенные на защиту информации в АС.

Этим условием ограничивается стоимость выбранных средств защиты.

Постановка задачи.

$$\begin{aligned} &U(\boldsymbol{X}) = \sum_{i \in N} u_i k_i \max_{j \in M} \{p_{ij} x_j\} \to \max_{X \in \Delta_{\text{доп}}} \\ &\Delta_{\text{доп}} : \sum_{j \in M} c_j x_j \le C. \end{aligned} \tag{3}$$

Здесь $\Delta_{\text{доп}}$ – множество допустимых альтернатив (значений компонент неизвестного вектора $\boldsymbol{X}$).

Решение задачи – нахождение всех неизвестных компонент вектора $\boldsymbol{X}$ и выбор тех средств защиты b_j, для которых компонента вектора $x_j(\forall j \in M)$ равна 1.

Поставленная задача является задачей булевого программирования. В работе [3] рассмотрен один из методов решения подобных задач – метод вектора спада.

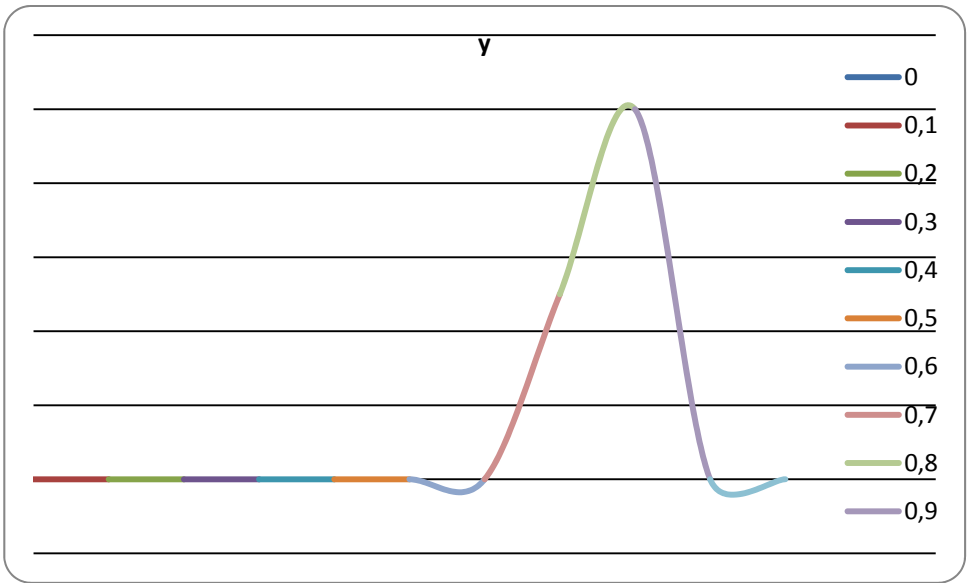
Сформулированная задача с четко определенными значениями параметров является достаточно грубой. Некоторые из исходных данных можно описать с помощью нечетких множеств, особенно те, которые определяются экспертами и для них, как правило, не существует точного значения, а есть некоторая оценка, находящаяся в заданном диапазоне. Проанализируем особенности нечеткого описания параметров.

Нечеткое описание параметров. В качестве примера рассмотрим описание параметров $p_{ij}, \forall i \in N, j \in M$ в виде нечеткого множества, для других параметров, которые могут иметь нечеткое описание, например, $k_i, \forall i \in N$ или $u_i, \forall i \in N$ можно использовать подобные рассуждения.

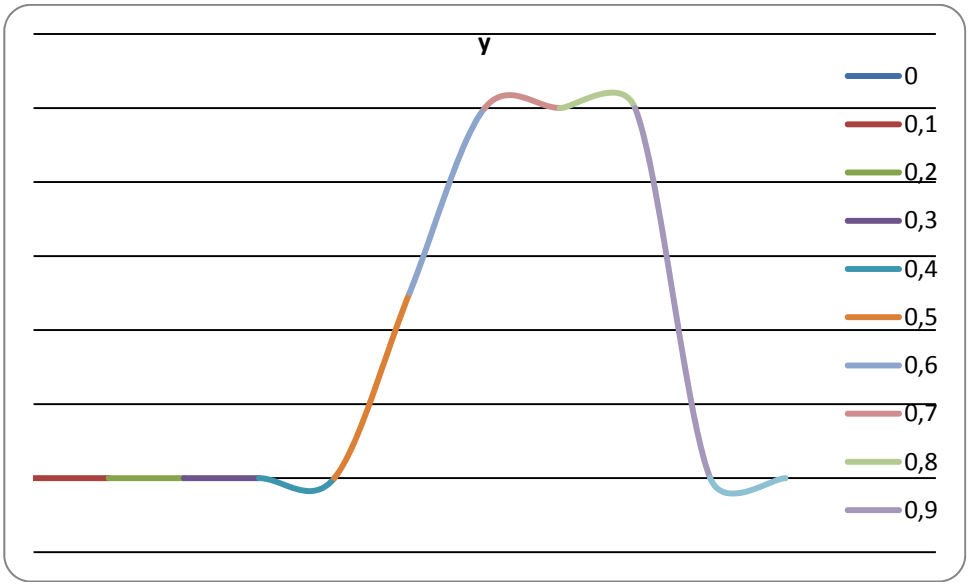
Для любого значения $p_{ij} \in [0,1]$ необходимо задать функцию принадлежности. В работе [4] рассмотрены различные способы задания функций принадлежности. Удобнее использовать аналитическое представление в виде некоторой простой математической функции, так как именно такое представление чаще всего применяют при описании параметров, которые можно измерить в некоторой количественной шкале. Рассмотрим задание функции принадлежности с помощью кусочно-линейных функций, например, треугольной или трапециевидной, вид которых представлен на рис. 1.

Следует отметить, что максимум функции принадлежности не обязательно равен 1, он может быть и меньше 1. Интерпретация данных функций принадлежности следующая: для любого значения $p_{ij}, \forall i \in N, j \in M$ значение функции принадлежности $\mu(p_{ij}) \in [0,1]$ означает степень доверия (уверенности) эксперта (экспертов), что данное значение соответствует истинному.

Рассмотрим первые два линейных участка функций: $\mu(p_{ij}) = 0$, значение $\mu(p_{ij})$ возрастает до максимума. На этих участках значение показателя качества выбора средств защиты (1) не убывает в зависимости от любого $p_{ij}, \forall i \in N, j \in M$ при заданном $\boldsymbol{X}$ точно так же, как и степень принадлежности p_{ij}. Поскольку показатель требуется максимизировать, то данные участки можно не рассматривать и для упрощения записи можно полагать, что функция принадлежности имеет вид, представленный на рис. 2.



а



б

Рис. 1. Функция принадлежности $y = \mu(p_{ij})$:

а – треугольная; *б* – трапециевидная

Интерпретация данных такой функций принадлежности следующая: для любого значения $p_{ij}, \forall i \in N, j \in M$ значение функции принадлежности $\mu(p_{ij}) \in [0,1]$ означает степень доверия (уверенности) эксперта (экспертов), что данное значение p_{ij} не превышает истинное значение. Подобные функции принадлежности можно представить в виде

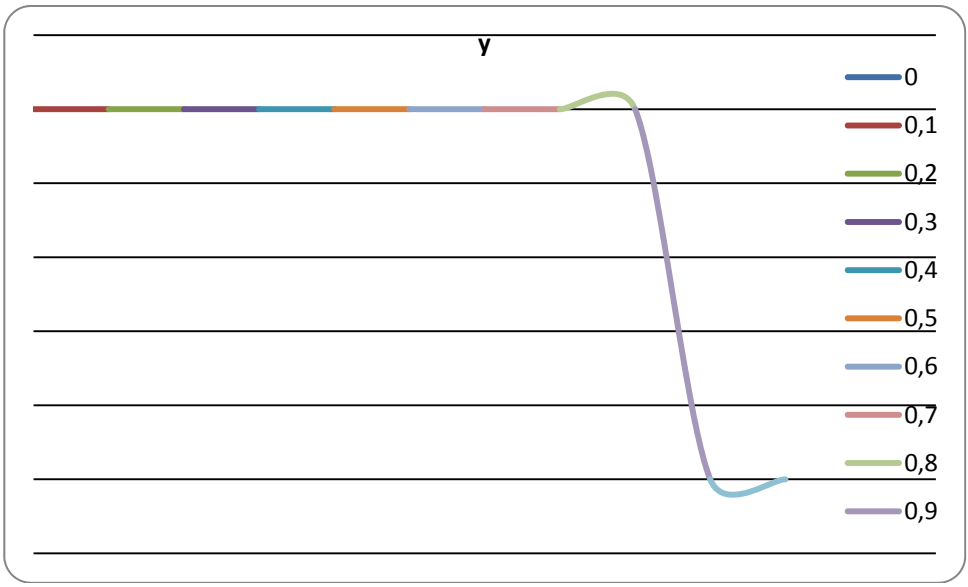


Рис. 2. Упрощенная функция принадлежности $y = \mu(p_{ij})$

$$\mu(p_{ij}, \beta_{ij}, \gamma_{ij}) = \begin{cases} 1, p_{ij} \le \beta_{i,j} \\ \dfrac{\gamma_{ij} - p_{ij}}{\gamma_{ij} - \beta_{ij}}, \beta_{ij} < p_{ij} \le \gamma_{ij}, \quad \forall i \in N, j \in M, \\ 0, p_{ij} > \gamma_{ij} \end{cases} \tag{4}$$

где β_{ij}, γ_{ij} – некоторые заданные числовые параметры функции, принимающие действительные значения и упорядоченные отношением $\beta_{ij} < \gamma_{ij}$. Применительно к конкретной функции, представленной на рис. 2, значения параметров следующие: $\beta_{ij} = 0,8, \gamma_{ij} = 0,9$.

Решение задачи. Задача (3) с нечеткими параметрами p_{ij}, $\forall i \in N$, $j \in M$ является задачей нечеткого математического программирования [5], в данном случае это задача с нечеткой функцией цели и обычными (т.е. четко описанными) ограничениями. Для упрощения записи введем матрицу P с компонентами $p_{ij}, \forall i \in N, j \in M$. Для любой матрицы P степень ее принадлежности нечеткому множеству в соответствии с работой [5] будем определять по формуле $\mu(P) = \min\limits_{i,j} \mu(p_{ij}, \beta_{ij}, \gamma_{ij})$.

Если для любой заданной матрицы P решать задачу (3), то полученное решение $\boldsymbol{X}^*$ (или любое из нескольких решений, если решение не единственное) характеризуется двумя значениями показателей: значением показателя (1) и степенью принадлежности $\varphi(\boldsymbol{X}^*, P) = \mu(P)$,

которую можно интерпретировать так, что степень недоминируемости решения $\boldsymbol{X}^*$ не ниже $\mu(P)$ [5]. Тогда для любого из решений задачи (3) можно определить степень его недоминируемости:

$$\varphi(\boldsymbol{X}^*) = \sup_P \varphi(\boldsymbol{X}^*, P). \tag{5}$$

Таким образом, для решений задачи (3) при разных P получаем два показателя, которые необходимо максимизировать – показатель (1) и (5). Один из подходов к решению задачи при нечетких исходных данных заключается в переходе к задаче оптимизации двух показателей. Решение может быть найдено среди множества Парето.

В работе [5] показано, что для нахождения решений с заданной степенью недоминируемости $\alpha \in [0,1]$ в задаче (3) с нечеткими параметрами требуется решить задачу максимизации показателя:

$$U(\boldsymbol{X}) = \sum_{i \in N} u_i k_i \max_{j \in M} \{ p_{ij} x_j \}, \tag{6}$$

при следующих ограничениях:

$$\sum_{j \in M} c_j x_j \le C, \tag{7}$$

$$\mu(p_{ij}, \beta_{ij}, \gamma_{ij}) \ge \alpha, \ \forall i \in N, j \in M. \tag{8}$$

Учитывая вид функции, заданной выражением (4), неравенства (8) можно записать в следующем эквивалентном виде:

$$p_{ij} \le \gamma_{ij} - \alpha(\gamma_{ij} - \beta_{ij}), \ \forall i \in N, j \in M. \tag{9}$$

Таким образом, получим задачу параметрического математического программирования с булевыми переменными.

Учитывая, что показатель (6), является неубывающим по любому параметру $p_{ij}, \forall i \in N, j \in M$, максимум показателя в зависимости от параметров p_{ij} достигается при максимальных значениях параметров $p_{ij}, \forall i \in N, j \in M$ для любого $\boldsymbol{X}$. Это означает, что неравенства (9) можно заменить на равенства. В соответствии с ограничением (9) максимальные значения параметров p_{ij} не зависят от $\boldsymbol{X}$ и $p_{ij}^{(1)} = \gamma_{ij} - \alpha(\gamma_{ij} - \beta_{ij}), \ \forall i \in N, j \in M.$ Если при значениях $p_{ij} = p_{ij}^{(1)}$

решить задачу максимизации показателя (6) по вектору $\boldsymbol{X}$ с ограничением (7), то получим решение $\boldsymbol{X}^{(1)}$, степень недоминируемости которого равна α. Если считать, что $\alpha = 1$, то в соответствии с (9) максимальные значения параметров $p_{ij}^{(2)} = \beta_{ij}, \forall i \in N, j \in M$. Если при значениях $p_{ij} = p_{ij}^{(2)}$ решить задачу максимизации показателя (6) по вектору $\boldsymbol{X}$ с ограничением (7), то получим решение $\boldsymbol{X}^{(2)}$, степень недоминируемости которого равна 1, значение показателя для этого решения не может превышать значения показателя со степенью недоминируемости α, но может быть ему равным. В этом случае решение $\boldsymbol{X}^{(1)}$ не входит в множество Парето. Варьируя значения α можно получать решения с разной степенью недоминируемости и определять границы множества Парето.

Практическая постановка задачи и численные расчеты. Для демонстрации использования приведенной математической постановки задачи рассмотрим небольшой пример исходных данных для рассматриваемой задачи.

В табл. 1 приведены три возможных класса атак для АС. Данные о среднем числе атак за год и о среднем ущербе от одной атаки в случае ее неотражения сильно зависят от специфики деятельности организации и не являются объектом исследования данной статьи, поэтому выбраны произвольно.

Таблица 1

Среднее число атак за год и средний ущерб от неотражения атаки

Атака	Среднее число реализаций за год	Средний ущерб от неотражения атаки, руб.
Несанкционированное вторжение в сеть для перехвата трафика	40	900 000
Вирусная атака	100	50 000
DDoS атака на Web сервер организации	10	500 000

В табл. 2 представлены некоторые средства защиты от атак, их стоимость (или стоимость лицензий на 1 год) для сертифицированных версий и вероятности отражения атак (значения β_{ij}, γ_{ij}). Стоимость средств защиты соответствует организации с 200–300 рабочими станциями и несколькими серверами. Данные о стоимости лицензий конкретных средств защиты можно найти на сайте компании SoftLine [6] или на сайтах производителей. Вероятности предотвращения атак разными средствами защиты определены на основе ре-

зультатов тестов: для антивирусов данные представлены на сайте независимой лаборатории AV-test [7], по межсетевым экранам данные представлены в рейтинге [8], по средствам обнаружения вторжений в статье [9].

Таблица 2

Средства защиты от возможных атак, их стоимости и вероятности отражения атак

Средство защиты	Стоимость средства (или лицензии на 1 год), руб.	Вероятность отражения атаки, значения β_{ij}, γ_{ij} (если вероятность не равна 0)		
		Несанкционированное вторжение в сеть	Вирусная атака	DDoS атака
Антивирус № 1	220 000	0	0,65; 0,9	0
Антивирус № 2	230 000	0	0,6; 0,99	0
Межсетевой экран № 1	160 000	0,75; 0,95	0	0,7; 0,8
Межсетевой экран № 2	130 000	0,5; 0,99	0	0,7; 0,8
Средство обнаружения вторжений № 1	270 000	0,7; 0,9	0	0,8; 0,95
Средство обнаружения вторжений № 2	150 000	0,6; 0,9	0	0,7; 0,99

Продемонстрируем, какие данные необходимы для решения задачи выбора средств защиты от различных атак. Анализ всех существующих атак и средств защиты выходит за рамки данной статьи, поэтому приведенные данные не претендуют на полноту. Будем считать, что готовой бюджет организации, который может быть потрачен на средства защиты информации, составляет 500 000 рублей, минимальная степень недоминируемости решения $\alpha = 0,5$.

При этих исходных данных необходимо максимизировать показатель

$$U(\boldsymbol{X}) = 900000 \cdot 40 \cdot \max\left\{p_{13}x_3, p_{14}x_4, p_{15}x_5, p_{16}x_6\right\} +$$

$$+ 50000 \cdot 100 \cdot \max\left\{p_{21}x_1, p_{22}x_2\right\} +$$

$$+ 500000 \cdot 10 \cdot \max\left\{p_{33}x_3, p_{34}x_4, p_{35}x_5, p_{36}x_6\right\}.$$

Ограничения имеют следующий вид:

$$220000 \cdot x_1 + 230000 \cdot x_2 + 160000 \cdot x_3 +$$

$$+130000 \cdot x_4 + 270000 \cdot x_5 + 150000 \cdot x_6 \le 500000;$$

$p_{13} = 0{,}95 - \alpha \cdot 0{,}2;\ p_{14} = 0{,}99 - \alpha \cdot 0{,}49;\ p_{15} = 0{,}9 - \alpha \cdot 0{,}2;$

$p_{16} = 0{,}9 - \alpha \cdot 0{,}3;\ p_{21} = 0{,}9 - \alpha \cdot 0{,}25;\ p_{22} = 0{,}99 - \alpha \cdot 0{,}39;\ p_{33} = 0{,}8 - \alpha \cdot 0{,}1;$

$p_{34} = 0{,}8 - \alpha \cdot 0{,}1;\ p_{35} = 0{,}95 - \alpha \cdot 0{,}15;\quad p_{36} = 0{,}99 - \alpha \cdot 0{,}29.$

При такой небольшой размерности задача может быть решена методом полного перебора, при бóльшей размерности требуется привлекать методы булевого программирования.

Результаты решения при различных α представлены в табл. 3.

Таблица 3

Результаты решения задачи

Степень недоминируемости решения α	Оценка среднего предотвращенного ущерба, руб.	Решение, значение компонент вектора $\boldsymbol{X}$
1	33 750 000	1 0 1 0 0 0
0,9	34 645 000	1 0 1 0 0 0
0,8	35 540 000	1 0 1 0 0 0
0,7	36 435 000	1 0 1 0 0 0
0,6	37 360 000	0 1 1 0 0 0
0,5	38 325 000	0 1 1 0 0 0

Таким образом, при заданных условиях получено два решения из множества Парето: выбор антивируса № 1 и межсетевого экрана № 1, выбор антивируса № 2 и межсетевого экрана № 1. При этом для этих решений могут использоваться разные недоминируемые оценки двух показателей: степени недоминируемости решения и оценки среднего предотвращенного ущерба.

СПИСОК ЛИТЕРАТУРЫ

1. Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. – Киев: Диасофт, 2002. – 688 с.
2. Овчинников А. И., Журавлев А. М., Медведев Н. В., Быков А. Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение.– 2007. – № 3. – С. 115–121.
3. Овчинников А. И., Медведев Н. В., Быков А. Ю. Применение метода вектора спада для решения задачи поиска вариантов защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение.– 2008. – № 2. – С. 73–82.
4. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2005. – 736 с.

5. Зайченко Ю. П. Исследование операций: Нечеткая оптимизация. – Киев: Выща шк., 1991. – 191 с.
6. http://www.softline.ru (дата обращения:16.04.2012).
7. http://www.av-test.org/index.php?L=1 (дата обращения:16.04.2012).
8. http://www.matousec.com (дата обращения:16.04.2012).
9. Абдебов А. Ж., Заркумова Р. Н. Выбор средства эффективной защиты с помощью методов теории игр // Вопросы защиты информации. – 2010. – № 2. – С. 26–31.

Статья поступила в редакцию 14.05.2012

Авторы статей

Алехова Елена Юрьевна – аспирант кафедры «Математическая кибернетика» МГУ им. М.В. Ломоносова.

Алфимцев Александр Николаевич – канд. техн. наук, доцент кафедры «Информационные системы и телекоммуникации» МГТУ им. Н.Э. Баумана.

Андреев Арк Михайлович – канд. техн. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана.

Булдакова Татьяна Ивановна – д-р техн. наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Быков Александр Юрьевич – канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Гречищев Константин Михайлович – студент IV курса кафедры «Компьютерные системы и сети». Программист ФГУП «Концерн Системпром».

Губарь Александр Михайлович – канд. тех. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана.

Гуров Андрей Валерьевич – студент VI курса кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Девятков Владимир Валентинович – д-р техн. наук, профессор, заведующий кафедрой «Информационные системы и телекоммуникации» МГТУ им. Н.Э. Баумана.

Джалолов Ахмад Шарофиддинович – аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана.

Жирков Владимир Филиппович – канд. техн. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н. Э. Баумана.

Иванова Галина Сергеевна – д-р техн. наук, профессор кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана.

Матвеев Валерий Александрович – руководитель НУК ИУ, профессор, д-р технических наук, заслуженный деятель науки РФ, лауреат Государственных премий СССР и РФ, лауреат премий Правительства РФ в области науки и образования.

Маянц Алексей Юрьевич – аспирант кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана.

Можаров Геннадий Петрович – канд. техн. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана.