СИСТЕМНИЙ АНАЛІЗ

В.И. НОРКИН, А.А. ГАЙВОРОНСКИЙ, В.А. ЗАСЛАВСКИЙ, П.С. КНОПОВ

УДК 330.115

МОДЕЛИ ОПТИМАЛЬНОГО РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ДЛЯ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ[1]

Аннотация. Рассмотрены возможности применения моделей и методов теории исследования операций к планированию защиты объектов критической инфраструктуры. Адаптация этих моделей включает учет стохастической, информационной и поведенческой неопределенности террористов. В частности, рассмотрены соответствующие обобщения задач антагонистической игры нападения и защиты, оптимального распределения защитных ресурсов и предложены методы решения возникающих оптимизационных задач.

Ключевые слова: защита критической инфраструктуры, распределение ресурсов, двухуровневое стохастическое программирование, иерархическое динамическое программирование.

ВВЕДЕНИЕ

Террористические угрозы характеризуются значительной неопределенностью, разнообразием, изощренностью и катастрофической опасностью. К новым угрозам относятся атаки на критическую инфраструктуру общества и государства, кибертерроризм и уличный терроризм. Эти угрозы ставят новые задачи научного обеспечения общественной безопасности. Необходимы модели террористических угроз и атак, учитывающие высокую степень неопределенности, разнообразие и злонамеренный характер возможных атак. В работах [1–6] обсуждаются возможности теории исследования операций для борьбы с террористическими угрозами.

В настоящей статье показано, что задачи защиты объектов критической инфраструктуры сводятся к решению двухуровневых игровых стохастических минимаксных задач. Задачи эшелонированной (многоступенчатой) обороны критически важных объектов описываются деревьями угроз и решаются методами иерархического и сетевого динамического программирования.

ОПТИМАЛЬНОЕ РАСПРЕДЕЛЕНИЕ РЕСУРСОВ ДЛЯ АКТИВНОЙ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Критическая инфраструктура — это объекты, системы и сети, предназначенные для передачи и распространения денег, энергии, информации, воды, товаров и имеющие важное значение для обеспечения безопасности и качества жизни населения. Защита критической инфраструктуры от предполагаемых террористических атак является основной задачей структур, которые занимаются вопро-

[1]Работа поддержана грантом CPEA-ST-2016/10002, The Norwegian Centre for International Cooperation in Education (SIU).

сами безопасности государства. Сложность этой задачи заключается в том, что атаки бывают неожиданными, могут быть направлены на большое число разнообразных целей при ограниченных ресурсах обороны и с возможными катастрофическими последствиями. Проблема идентификации нападающего подобна проблеме поиска иголки в стоге сена. После известной террористической атаки 11 сентября 2000 года в США было разработано множество методологических подходов к планированию защиты критической инфраструктуры [7–17]. Модели стохастического программирования также нашли новое применение для моделирования неопределенностей в задаче распределения ресурсов для защиты критической инфраструктуры [18–23].

В [7] представлена следующая формула для оценки террористического риска:

$$\textit{Ожидаемый риск} = \textit{Вероятность атаки} \times \textit{Вероятность успешности атаки при условии, что она произошла,} \times \textit{Последствия успешной атаки.}$$

Иными словами

$$\textit{Риск} = \textit{Угроза} \times \textit{Уязвимость} \times \textit{Следствие}.$$

В работах [24, 25] эта формула подвергнута критике, поскольку «она неспособна оптимально диверсифицировать защитные инвестиции, учитывать корреляции и зависимости между факторами в ее правой части, выявить затраты и выгоды альтернативных решений по управлению рисками, использовать четко определенные концепции, которые явно улучшают, а не путают и затмевают принятие решений». Авторы работы [26] подчеркивают различия в информации, доступной террористам и доступной защитникам, способность террористов искать и использовать информацию и активно изучать различные варианты нападений, прежде чем принимать решение к действиям. Они делают акцент на то, чтобы не ограничивать себя анализом надежности защиты системы, а моделировать поведение изобретательных террористов.

Для моделирования неопределенности поведения нападающего при принятии решений защитником изучалось и применялось множество теоретико-игровых моделей (например, [10–13]).

Базовая модель [27, 28] предполагает, что целью защитника является минимизация общих ожидаемых потерь от террористических атак, т.е.

$$\min_{x_1,\dots,x_n \ge 0} \sum_{i=1}^{n} h_i(x_1,\dots,x_n)\, p(x_i) V_i \tag{1}$$

при ограничении

$$\sum_{i=1}^{n} x_i \le B, \tag{2}$$

где n — число целей; x_i — ресурсы защитника, выделенные на защиту цели i; B — общий бюджет защитника; V_i — ценность цели i для защитника; $h_i(x_1,\dots,x_n)$ — вероятность атаки на цель i; $p(x_i)$ — вероятность успеха атаки на цель i в зависимости от ресурсов, выделенных для защиты цели.

Нападающий наблюдает за распределением ресурсов защитника $\{x_i\}$ и затем выбирает цель с наиболее высоким выигрышем исходя из любых оборонительных инвестиций

$$\max_i \; p(x_i) U_i, \tag{3}$$

где U_i — полезность (важность) цели i для атакующего. Поскольку предполагается, что защитник не уверен в предпочтениях выбора атакующего, целевые

оценки U_i атакующего моделируются как случайные величины. Этим определяются вероятности атаки на цель j: $h_j(x_1, \dots, x_n) = \Pr\{\arg\max_i p(x_i)U_i = j\}$.

В [28, 29] предполагается, что вероятность успеха атаки на цель i определяется как $p(x_i) = e^{-\lambda_i x_i}$, поэтому λ_i является мерой экономической эффективности оборонительных инвестиций. Экономическую эффективность в этой модели можно рассматривать как меру снижения риска на единицу затрат. В [30] предлагаются другие функции $p(x_i)$.

В несложных ситуациях важность цели U_i для атакующего может измеряться величиной ущерба: $U_i = r_i(x_i, \omega)$, причиненного успешной террористической атакой при информированности нападающего (имеющейся информации) ω, а оценка защитника V_i цели i при информированности нападающего ω' определяется как $V_i = r_i(x_i, \omega')$. В [7] величина $r_i(x_i, \omega)$ была представлена как функция недостаточности средств: $r_i(x, \omega) = \max\{0, a_i(\omega) - x_i\}^2$. В [21] она представлена в виде $r_i(x, \omega) = \max\{0, a_i(\omega) - x_i\}$, а в [23] — в виде $r_i(x, \omega) = -b_i(\omega)x_i$, где $a_i(\omega)$ — необходимые инвестиции в фортификацию объекта i с учетом обстоятельств ω и $b_i(\omega)$ — коэффициент полезности оборонительных инвестиций в объект i. В [7] и [21] также была рассмотрена многоцелевая постановка задачи распределения защитных инвестиций. В отчете RAND Corporation [7] строится так называемая функция неправильного распределения бюджета $M_k(x, \omega) = \sum_i \max\{0, a_{ki}(\omega) - x_i\}^2$, где $a_{ki}(\omega)$ — желаемая доля средств, выделенных на защиту цели i по критерию k; $A = \{a_{ki}(\omega)\}$ — случайная матрица риска, $a_{ki}(\omega) \ge 0$, $\sum_i a_{ki}(\omega) = 1$; $\{x_i\}$ — фактическое долевое распределение защитных инвестиций.

В настоящей статье мы обобщаем модель (1)–(3) в том аспекте, что вероятности атаки на цели $i = 1, \dots, n$ не известны полностью, а известно лишь множество, которому принадлежат эти вероятности, например когда заданы только границы вероятностей и когда нападающий решает свою оптимизационную задачу.

Модель принятия решений атакующей стороны. Предположим, что защитник должен защищать объекты $i = 1, \dots, n$, выделяя ресурс/бюджет $x_i \ge 0$ на объект i, пусть $x = (x_1, \dots, x_n)$. Общий ресурс/бюджет равен $B \ge \sum_{i=1}^n x_i$. Обозначим $i = 0$ фиктивный объект (атака на фиктивный объект означает отсутствие атак на реальные объекты). Предположим, что атакующий знает вектор распределения защитных ресурсов x. Затем он выбирает объекты для атаки с некоторыми вероятностями (смешанная стратегия) $(y_1, \dots, y_n) = y \in Y_a(x, \omega_a)$, где $\sum_{i=0}^n y_i \le 1$; $Y_a(x, \omega_a)$ представляет множество допустимых стратегий/вероятностей атакующего, ω_a является информационным вектором атакующего из информационного множества Ω_a, индекс a обозначает, что соответствующие величины относятся к нападающему. В двух крайних случаях $Y_a(x, \omega_a)$ может быть точкой $Y_a(x, \omega_a) = \{p_i(x, \omega_a)\}$ или симплексом $Y_a(x, \omega_a) = Y^{n+1} = \left\{ y_i \ge 0, \sum_{i=0}^n y \le 1 \right\}$.

Множество распределений вероятностей $Y_a(x, \omega_a)$ называется множеством выборов, которое может задаваться посредством решения некоторой оптимизационной задачи или с помощью некоторых ограничений-неравенств. Например, эксперты могут устанавливать нижнюю и верхнюю границы для вероятностей y_i, $l_i \le y_i \le u_i$, или упорядочивать вероятности $y_i \le y_j$ для некоторых i, j.

Пусть $q_i(x_i, \omega_a)$ — вероятность успеха атаки на объект i, если она произойдет, например $q_i(x_i, \omega_a) = q_i^0(\omega_a)e^{-\lambda_i x_i}$. Пусть также $r_i(x_i, \omega_a)$ — средняя ве-

личина ущерба для объекта i в случае успешной атаки на него. Тогда задача принятия решений атакующего может состоять в максимизации ожидаемого ущерба защищающейся стороне при ограничении $y \in Y_a(x, \omega_a)$:

$$Y_a^*(x, \omega_a) = \operatorname*{argmax}_{y \in Y_a(x, \omega_a)} \left(\sum_{i=1}^{n} y_i q_i(x_i, \omega_a) r_i(x_i, \omega_a) \right). \tag{4}$$

В случае симплекса $Y_a(x, \omega_a) = \left\{ y \geq 0 : \sum_{i=1}^{n} y_i \leq 1 \right\}$ из (4) получаем величину ущерба в виде (3):

$$f(x, \omega_a) = \max_{1 \leq i \leq n} q_i(x_i, \omega_a) r_i(x_i, \omega_a).$$

Заметим, что постановка (4) не моделирует и не учитывает (ограниченные) ресурсы для проведения атаки на объекты $i = 1, \ldots, n$. Чтобы учесть этот аспект, нужно получить зависимости величин $q_i(x_i, \omega_a)$, $r_i(x_i, \omega_a)$ от ресурсов $(z_1, \ldots, z_n) = z \in Z$, выделенных атакующим для атаки на соответствующие объекты. Тогда задача (4) принимает вид

$$Y_a^*(x, \omega_a) = \operatorname*{arg\,max}_{y \in Y_a(x, \omega_a)} \max_{z \in Z} \left(\sum_{i=1}^{n} y_i (q_i(x_i, z_i, \omega_a) r_i(x_i, z_i, \omega_a) - z_i) \right).$$

Модель принятия решений защищающейся стороны. Если бы защитнику было известно множество выборов атакующего $Y_a^*(x, \omega_a)$, то он мог бы свести к минимуму свои худшие ожидаемые потери:

$$\mathbf{E}_{\omega_d, \omega_a} \max_{y \in Y_a^*(x, \omega_a)} \left(\left(1 - \sum_{i=1}^{n} y_i \right) \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i \left(q_i(x_i, \omega_d) r_i(x_i, \omega_d) + \sum_{i=1}^{n} x_i \right) \right) =$$

$$= \mathbf{E}_{\omega_d, \omega_a} \max_{y \in Y_a^*(x, \omega_a)} \left(\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i q_i(x_i, \omega_d) r_i(x_i, \omega_d) \right) =$$

$$= \sum_{i=1}^{n} x_i + \mathbf{E}_{\omega_d, \omega_a} \max_{y \in Y_a^*(x, \omega_a)} \sum_{i=1}^{n} y_i q_i(x_i, \omega_d) r_i(x_i, \omega_d) \to \min_{x \in X}. \tag{5}$$

Здесь X — множество допустимых решений $(x_1, \ldots, x_n) = x \in X$ защитника; ω_d является информационным вектором защищающегося; символ $\mathbf{E}_{\omega_d, \omega_a}$ обозначает математическое ожидание по вероятностной мере P_{ω_d, ω_a}, определенной на множестве Ω возможных значений информационного вектора (ω_d, ω_a) (как оно воспринимается защитником); индексы d, a приписываются соответственно величинам, относящимся к защитнику и атакующему. Множество X включает бюджетное ограничение (2) и другие ограничения на вектор решения x.

Возможна ситуация, когда $Y_a(x, \omega_a) = \left\{ y \geq 0 : \sum_{i=1}^{n} y_i \leq 1 \right\}$,

$$\operatorname*{arg\,max}_{1 \leq i \leq n} q_i(x_i, \omega_a) r_i(x_i, \omega_a) = \operatorname*{arg\,max}_{1 \leq i \leq n} q_i(x_i, \omega_d) r_i(x_i, \omega_d),$$

т.е. защищающаяся сторона предвидит выбор (решение $Y_a^*(x, \omega_a)$) нападающей стороны, хотя оценки ожидаемых ущербов у них могут быть разные. Тогда задача (5) принимает вид задачи минимаксного стохастического программирования:

$$\sum_{i=1}^{n} x_i + \mathbf{E}_{\omega_d} \max_{1 \leq i \leq n} q_i(x_i, \omega_d) r_i(x_i, \omega_d) \to \min_{x \in X}.$$

Однако, как правило, защитник не знает множества выборов $Y_a^*(x,\omega_a)$ и информационного вектора ω_a атакующего. Поэтому защитнику приходится сводить к минимуму самые худшие ожидаемые потери при условии его понимания $Y_d(x,\omega_d)$ множества $Y_a^*(x,\omega_a)$ и на основе его информационного вектора ω_d:

$$\sum_{i=1}^{n} x_i + \mathbf{E}_{\omega_d} \max_{y\in Y_d(x,\omega_d)} \sum_{i=1}^{n} y_i q_i(x_i,\omega_d) r_i(x_i,\omega_d) \to \min_{x\in X}. \qquad (6)$$

Другая минимаксная постановка имеет следующий вид:

$$\sum_{i=1}^{n} x_i + \max_{\omega_d\in\Omega_d} \max_{y\in Y_d(x,\omega_d)} \sum_{i=1}^{n} y_i q_i(x_i,\omega_d) r_i(x_i,\omega_d) \to \min_{x\in X}. \qquad (7)$$

Рассматриваемые задачи относятся к двухуровневым задачам стохастического программирования, где вектор x является решением первого уровня (решением лидера, защитника), а вектор y — решением второго уровня (решением последователя, нападающего), причем целевая функция первого уровня зависит от решений y второго уровня. Сложность этих стохастических задач состоит не только в нелинейном и негладком характере оптимизируемых функций, но и в зависимости множества вероятностных стратегий атакующей стороны $Y_d(x,\omega_d)$ (в понимании защищающейся стороны) от переменных x первого уровня. Методы решения таких задач обсуждаются в работах [31–35].

Отметим важные особенности задач (6), (7).

Задача второго уровня (4) является линейной с коэффициентами целевой функции, зависящими от решений первого уровня.

Ограничения задачи второго уровня могут иметь вид симплекса $Y_a(x,\omega_a)=\left\{ y\ge 0 : \sum_{i=1}^{n} y_i \le 1 \right\}$ или пересечения симплекса и параллелепипеда $Y_a(x,\omega_a)=\left\{ 0\le y_i \le p_i : \sum_{i=1}^{n} y_i \le 1 \right\}$.

Функции $q_i(x_i,\omega_a)r_i(x_i,\omega_a)$, $q_i(x_i,\omega_d)r_i(x_i,\omega_d)$ естественно предполагать монотонно убывающими (к нулю) по переменным x_i. Проблема состоит в разработке эффективных методов решения задач вида (6), (7). В частном случае, когда $Y_d(x,\omega_d)=Y_d(\omega_d)$, т.е. не зависит от x, задача (6) преобразуется в задачу минимаксного стохастического программирования

$$\mathbf{E}_{\omega_d} \max_{y\in Y_d(\omega_d)} \left(\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i q_i(x_i,\omega_d) r_i(x_i,\omega_d) \right) \to \min_{x\in X}$$

и может быть решена методом стохастических квазиградиентов [36–38].

В другом частном случае, когда $Y_d(x,\omega_d)=\left\{ y_i \ge 0, \sum_{i=0}^{n} y \le 1 \right\}$, $\Omega_d=\overline{\omega}_d$, $X=\left\{ x_i \ge 0 : \sum_i x_i \le R \right\}$, задача (6) сводится к виду

$$\min_{x\in X} \left[\sum_{i=1}^{n} x_i + \max_{1\le i\le n} q_i(x_i,\overline{\omega}_d) r_i(x_i,\overline{\omega}_d) \right] =$$

$$= \min_{0\le r\le R} \left[r + \min_{\left\{ x_i\ge 0 : \sum_{i=1}^{n} x_i \le r \right\}} \max_{1\le i\le n} q_i(x_i,\overline{\omega}_d) r_i(x_i,\overline{\omega}_d) \right].$$

При этом внутренняя задача (оптимизации по x)

$$f(r) = \min_{\left\{x_i \geq 0 : \sum_{i=1}^{n} x_i \leq r\right\}} \max_{1 \leq i \leq n} q_i(x_i, \overline{\omega}_d)\, r_i(x_i, \overline{\omega}_d) \qquad (8)$$

может быть решена методом динамического программирования (описание в следующем разделе), а внешняя задача — перебором по $r \in [0, R]$.

Другой подход к решению внутренней задачи (8) основан на следующем наблюдении. В оптимальном решении $x^*(r) = (x_1^*, \ldots, x_n^*)$ должно выполняться соотношение

$$\max_{1 \leq i \leq n} q_i(x_i^*, \overline{\omega}_d)\, r_i(x_i^*, \overline{\omega}_d) = q_j(x_j^*, \overline{\omega}_d)\, r_j(x_j^*, \overline{\omega}_d)$$

для всех j таких, что $x_j^* > 0$. В противном случае оптимальное значение функции $\max_{1 \leq i \leq n} q_i(x_i, \overline{\omega}_d)\, r_i\,(x_i, \overline{\omega}_d)$ может быть уменьшено за счет перераспределения ресурсов. Для произвольного $h \in [0, \max_{1 \leq i \leq n} q_i(0, \overline{\omega}_d)\, r_i(0, \overline{\omega}_d)]$ обозначим $x_i(h)$ неотрицательное решение уравнения $h = q_i(x_i, \overline{\omega}_d)\, r_i(x_i, \overline{\omega}_d)$, если оно существует, и положим $x_i(h) = 0$ в противном случае. Обозначим $S(h) = \sum_{i=1}^{n} x_i(h)$. Функции $x_i(h)$ и, следовательно, $S(h)$ монотонно убывают по h. Теперь решение задачи (8) сводится к нахождению минимального решения неравенства $S(h) \leq r$, которое может быть определено методом дихотомии.

ИЕРАРХИЧЕСКАЯ МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ЗАЩИТНЫХ РЕСУРСОВ

В настоящем разделе подход Ушакова [39] к оптимальному распределению защитных ресурсов дополняется новой вычислительной процедурой иерархического динамического программирования для эффективного решения возникающих в этом подходе невыпуклых экстремальных задач.

Предположим, что защищаемая система состоит из подсистем. Защищенность всей системы сложным иерархическим образом зависит от защищенности подсистем. Для каждой подсистемы $j \in L$ самого низкого уровня экспертным образом построены показатели уровня защищенности $f_j(x_j)$ как функции вложенных ресурсов x_j. Обозначим $x = \{x_j,\ j \in L\}$ неотрицательный вектор распределения ресурсов для защиты подсистем нижнего уровня, который удовлетворяет ресурсному ограничению: $\sum_{j \in L} x_j \leq R$. Показатели защищенности могут отображать, например, вероятность атаки, вероятность успешности атаки на подсистему, ущерб от атаки и т.п. Показатель защищенности f какой-либо подсистемы, следующей за самым низким уровнем, строится из функций защищенности $f_j(x_j)$, $j \in J_f$, подчиненных подсистем с помощью некоторой монотонной ассоциативной операции $A_f \in \{\Sigma, \Pi, \max, \min, \ldots\}$, например $f = \sum_{j \in J_f} f_j(x_j)$, $f = \prod_{j \in J_f} f_j(x_j)$, $f = \min_{j \in J_f} f_j\,(x_j)$, $f = \max_{j \in J_f} f_j(x_j)$ и т.п. Отметим, что показатель защищенности f вершины на любом уровне может непосредственно зависеть от показателей $f_j(x_j)$ некоторых подсистем самого нижнего уровня $j \in L_f$. Если для защиты подсистемы выделен ресурс $r_f = \sum_{j \in L_f} x_j$, то максимальный уровень защиты $f^*(r_f)$ этой подсистемы и оптимальный план распределения ресурсов x_j^*, $j \in L_f$, при общем выделенном ресурсе r_f можно найти методом динамического программирования. Аналогично могут быть найдены уровни максимальной защиты для подсистем следующего уровня и так далее до корневого уровня.

Пример 1. (Защита отдельного объекта.) Рассмотрим задачу распределения ресурсов для минимизации террористического риска:

$$Риск\,(x_1, x_2, x_3) = Угроза\,(x_1) \times Уязвимость\,(x_2) \times$$
$$\times Следствие\,(x_3) \to \min_{x_1, x_2, x_3}$$

при ограничениях $x_1 \ge 0,\ x_2 \ge 0,\ x_3 \ge 0,\ x_1 + x_2 + x_3 \le R$. Функции $Угроза\,(x_1)$, $Уязвимость\,(x_2)$, $Следствие\,(x_3)$ зависят от объемов инвестиций x_1, x_2, x_3 в мероприятия по снижению вероятности угрозы атаки, вероятности успешности атаки и величины ущерба от атаки. Эти функции считаются заданными экспертно.

Пример 2. (Защита резервированием.) Пусть система состоит из однотипных дублирующих подсистем. Система в целом является работоспособной, если исправна хотя бы одна из подсистем. Пусть $f_j(x_j)$ — показатели уровня защищенности подсистем как функции вложенных в их защиту ресурсов x_j, $j = 1, \ldots, n$. Тогда уровень защищенности системы в целом может задаваться функцией $f(x) = \max_{j=1,\ldots,n} f_j(x_j)$ с ограничением на ресурсы $\sum_{j=1}^{n} x_j \le R$.

Если показатели уровня защищенности подсистем $f_j(x_j)$ являются вероятностями неуспешности атаки на (независимые) подсистемы, то при единичной атаке вероятность того, что хотя бы одна подсистема останется работоспособной, равна

$$f(x) = 1 - \prod_{j=1}^{n} (1 - f_j(x_j)).$$

Таким образом, задача максимизации функции $f(x)$ сводится к задаче минимизации:

$$\prod_{j=1}^{n} (1 - f_j(x_j)) \to \min_{\{x_j \ge 0\}},\ \sum_{i=1}^{n} x_i \le R.$$

Пример 3. (Защита последовательной системы.) Пусть система состоит из последовательно работающих подсистем, причем она работоспособна, если рабочими являются все подсистемы. Пусть показатель защищенности f_j каждой подсистемы j как функция вложенных в защиту ресурсов x_j описывается функцией $f_j(x_j)$. Тогда уровень защищенности системы может задаваться функцией $f(x) = \min_{j=1,\ldots,n} f_j(x_j)$.

Если показатели уровня защищенности подсистем $f_j(x_j)$ являются вероятностями неуспешности атаки на (независимые) подсистемы, то при единичной атаке вероятность того, что все подсистемы будут работоспособны, равна

$$f(x) = \prod_{j=1}^{n} f_j(x_j).$$

В работе [40] в качестве меры защищенности системы элементов, соединенных в последовательно-параллельную схему, использовалась минимально необходимая стоимость оптимально организованной атаки на систему как функция вложенных защитных ресурсов.

Метод иерархического динамического программирования. Пусть защищенность системы описывается графом в виде дерева (в общем случае ациклического ориентированного графа), в вершинах которого находятся функции (показатели) защищенности этих вершин. Примерами могут быть дерево отказов сложной системы [41, 42], модели многоуровневого проектирования сложных систем [43], дерево угроз [44, 45], дерево многоступенчатой защиты [39]. Функции защищенности листьев (концевых вершин графа) считаются экспертно заданными функция-

ми от объемов инвестиций в защиту этих вершин. Эти функции могут быть заданы экспертами таблично для некоторого перечня значений и интерполироваться для промежуточных значений [39]. Естественно считать их возрастающими и вогнутыми функциями от вложенного ресурса. Однако они могут быть и дискретными функциями от булевых или целочисленных переменных и описывать надежность элементов в зависимости от степени и характера резервирования [43, 46]. Защищенность промежуточных вершин зависит от защищенности дочерних вершин. Будем считать, что вершины дерева занумерованы числами $i = 1, 2, \ldots$ и корневая вершина имеет номер $i = 1$. Функция (показатель) защищенности f_i промежуточной вершины i выражается через функции (показатели) защищенности f_j дочерних вершин $j \in J_i$ с использованием некоторых операций агрегации $A_i(y_1, \ldots, y_{n_i}) \in \Im$, $f_i = A_i(f_{j_1}, f_{j_2}, \ldots, f_{j_{n_i}})$, $j_1, j_2, \ldots, j_{n_i} \in J_i$. Например, семейство операций $\Im$ может включать операции суммирования, перемножения, максимизации, минимизации, $\Im = \{\Sigma, \Pi, \max, \min\}$. Некоторые функции $f_{j_1}, f_{j_2}, \ldots, f_{j_{n_i}}$ могут принадлежать листьям дерева, в частности быть просто переменными оптимизации. Обозначим L_i множество подчиненных вершине i листьев дерева, тогда L_1 содержит все листья дерева.

Таким образом, функция защищенности системы (корня дерева) f_1 сложным образом зависит от ресурсов $\{x_l, l \in L_1\}$, вложенных в защиту листьев дерева $l \in L_1$, и выражается записью $f_1(\{x_l, l \in L_1\})$. Пусть функции защищенности листьев f_l зависят от вложенных в их защиту ресурсов $x_l \geq 0$ и при этом имеется бюджетное (ресурсное) ограничение: $\sum_{l \in L_1} x_l \leq R$. Задача состоит в максимизации функции $f_1(\{x_l, l \in L_1\})$. В работе [40] рассмотрен частный случай этой задачи с агрегирующими функциями $\Im = \{\Sigma, \Pi\}$ для параллельно-последовательных систем и с линейными функциями защищенности в листьях, которые выражают стоимость атаки на элемент как функцию вложенных защитных ресурсов, для некоторых разумных стратегий атакующей стороны.

Если функции $f_j(x_j)$, $j \in L_1$, в листьях дерева вогнуты, а остальные агрегирующие функции $f_i(\cdot)$, $i \notin L_1$, вогнутые и неубывающие по своим аргументам, например $f_i \in \{\Sigma, \min, \sqrt{\Sigma}, \sqrt{\min}, -\exp\{\Sigma\}, -\exp\{\min\}, \ldots\}$, то корневая целевая функция $f_1(\{x_l, l \in L_1\})$ является вогнутой в области $\{0 \leq x_j \leq R, j \in L_1\}$, а задача распределения защитных ресурсов (в том числе с несколькими видами ресурсов) может быть решена методами выпуклого программирования. (Этот случай, по существу, был уже рассмотрен в работе [29].) В общем случае она является многоэкстремальной задачей с несепарабельной целевой функцией, имеющей иерархическую древовидную структуру. Такая задача может быть эффективно решена иерархическим методом динамического программирования. Различные обобщения стандартного последовательного метода динамического программирования рассмотрены в [47–49].

Предположим, что все показатели защищенности $f_i(y_1, \ldots, y_{n_i})$ являются монотонными неубывающими непрерывными или полунепрерывными сверху функциями своих аргументов $(y_1, \ldots, y_{n_i}) \in \mathrm{R}^{n_i}$.

Очевидно, функции защищенности, заданные операциями $\Im = \{\Sigma, \Pi, \max, \min\}$, удовлетворяют этому предположению. При таком предположении все задачи вида $f_i^*(y_i) = \max_{\{x_j \geq 0, \sum_{j \in L_i} x_j \leq y_i\}} f_i(\{x_j, j \in L_i\})$ имеют решения и функции $f_i^*(y_i)$ являются монотонными неубывающими полунепрерывными сверху функциями своих аргументов y_i.

Предположим, что потомки разных неподчиненных вершин не пересекаются, т.е. $L_i \cap L_j = \varnothing$ для всех $i \neq j$, $i \notin L_j$, $j \notin L_i$, и пусть вершины $\{j_1, \ldots, j_{n_i}\} = J_i$ являются дочерними для вершины i. Тогда в силу иерархической структуры и монотонности функций $f_i(\cdot)$ имеет место

$$f_i^*(y_i) = \max_{\left\{ x_j \geq 0,\ j \in L_i : \sum_{j \in L_i} x_j \leq y_i \right\}} f_i(\{x_j, j \in L_i\}) =$$

$$= \max_{\left\{ y_j \geq 0, j \in J_i : \sum_{j \in J_i} y_j \leq y_i \right\}} f_i\left(\left\{ \max_{\left\{ x_k \geq 0, k \in L_j : \sum_{k \in L_j} x_k \leq y_j \right\}} f_j(\{x_k, k \in L_j\}), j \in J_i \right\} \right) =$$

$$= \max_{\left\{ y_{jk} \geq 0 : \sum_{jk \in J_i} y_{jk} \leq y_i \right\}} f_i(f_{j_1}^*(y_{j_1}), \ldots, f_{j_k}^*(y_{j_k}), \ldots, f_{j_{n_i}}^*(y_{j_{n_i}})),$$

т.е. функция оптимальной защищенности $f_i^*(\cdot)$ вершины i может быть вычислена через аналогичные функции $f_j^*(\cdot)$ дочерних вершин $j \in J_i$. Следующие леммы обосновывают это утверждение.

Лемма 1. Пусть функции $\varphi_k(x_k)$, $x_k \in X_k$, $k = 1, \ldots, n$, полунепрерывны сверху на замкнутых множествах X_k, а функция $f(z_1, \ldots, z_n)$ — неубывающая и полунепрерывна сверху на множестве $[\inf_{x_1 \in X_1} \varphi_1(x_1), \sup_{x_1 \in X_1} \varphi_1(x_1)] \times \ldots$ $\ldots \times [\inf_{x_n \in X_n} \varphi_n(x_n), \sup_{x_n \in X_n} \varphi_n(x_n)]$. Тогда функция $f(\varphi_1(x_1), \ldots, \varphi_n(x_n))$ — полунепрерывна сверху на множестве $X_1 \times \ldots \times X_n$. Очевидно, если все функции f, φ_k являются непрерывными, то и суперпозиция $f(\varphi_1(x_1), \ldots, \varphi_n(x_n))$ является непрерывной функцией.

Лемма 2 [50, разд. 3.1]). Если функция $f_j(\{x_k, k \in L_j\})$ непрерывна (полунепрерывна сверху) на множестве $X_j = [0, r]^{|L_j|}$, где $|L_j|$ — число элементов в множестве L_j, то маргинальная функция $f_j^*(y_j) =$ $= \max_{\left\{ x_k \geq 0, k \in L_j : \sum_{k \in L_j} x_k \leq y_j \right\}} f_j(\{x_k, k \in L_j\})$ непрерывна (полунепрерывна сверху) по $y_j \in [0, r]$.

Лемма 3. Пусть функции $f_k(x_k)$, $x_k = (x_{k1}, \ldots, x_{km_k})$, $k = 1, \ldots, n$, полунепрерывны сверху на множествах $X_k = [0, r]^{m_k}$ $(r \geq 0)$, а функция $f(z_1, \ldots, z_n)$ — неубывающая и полунепрерывна сверху на множестве $[\inf_{x_1 \in X_1} f_1(x_1),$ $\sup_{x_1 \in X_1} f_1(x_1)] \times \ldots \times [\inf_{x_n \in X_n} f_n(x_n), \sup_{x_n \in X_n} f_n(x_n)]$. Обозначим симплексы

$$S(r) = \left\{ (x_1, \ldots, x_n) \in X_1 \times \ldots \times X_n : \sum_{k=1}^n \sum_{i=1}^{m_k} x_{ki} \leq r \right\}$$

и

$$S_k(y) = \left\{ x_k \in X_k : \sum_{i=1}^{m_k} x_{ki} \leq y \right\}, \quad k = 1, \ldots, n.$$

Тогда

$$\max_{(x_1, \ldots, x_n) \in S(r)} f(f_1(x_1), \ldots, f_n(x_n)) =$$

$$= \max_{\left\{ y_k \geq 0 : \sum_{k=1}^n y_k \leq r \right\}} f\left(\max_{x_1 \in S_1(y_1)} f_1(x_1), \ldots, \max_{x_n \in S_n(y_n)} f_n(x_n) \right).$$

Функция защищенности f_i каждой промежуточной вершины i зависит от распределения ресурсов x_i, выделенных на защиту листьев L_i, которые являются потомками данной вершины i. Максимальный достижимый уровень защищенности f_i^* данной промежуточной вершины i определяется общей суммой инвестиций y_i в подчиненные ей листья L_i и находится путем максимизации f_i по всем распределениям ресурсов $\{x_l, l \in L_i\}$ при ограничении $\sum_{l \in L_i} x_i \le y_i$.

Принцип иерархического динамического программирования состоит в том, что максимальный уровень защищенности каждой промежуточной вершины i достигается при таком распределении ресурсов между листьями $\{x_l^*, l \in L_i\}$, которое обеспечивает максимальный уровень защищенности всех вершин j, подчиненных данной вершине i, при ограничениях $\sum_{l \in L_j} x_l \le \sum_{l \in L_j} x_l^*$. Поэтому задача максимизации защищенности корневой вершины может быть решена последовательно путем построения функций максимальной защищенности вершин, непосредственно предшествующих листьям, и дальнейшего продвижения от листьев к корню дерева. При этом каждая функция максимальной защищенности f_i^* зависит от общих ресурсов, вложенных в защиту подчиненных ей листьев L_i. Оптимальное распределение ресурсов находится в обратном порядке: от корня к листьям путем нахождения оптимального распределения ресурсов между дочерними вершинами корня, оптимального распределения ресурсов между внучатыми вершинами и так далее до достижения листьев.

На каждом шаге метода иерархического динамического программирования необходимо решать задачи следующего вида:

$$\max_{\{x_1 \ge 0, \dots, x_n \ge 0 : x_1 + \dots + x_n \le r\}} A(f_1(x_1), \dots, f_n(x_n)).$$

Эти задачи также могут быть решены методом динамического программирования. Пусть функции агрегации $A(y_1, \dots, y_n) \in \Im$, $f = A(f_1, f_2, \dots, f_n)$, с переменным числом аргументов n обладают следующими свойствами:

$$A(y_1) = y_1, \ y_1 \in \mathrm{R}^1;$$

$$A(y_1, \dots, y_k) = A(A(y_1, \dots, y_{k-1}), y_k), \ y_1 \in \mathrm{R}^1, \ \dots, \ y_k \in \mathrm{R}^1;$$

$$A(y_1, \dots, y_k) \le A(y_1', \dots, y_k'), \text{ если } y_1 \le y_1', \ \dots, \ y_k \le y_k'.$$

Примерами таких функций A являются функции суммирования $y_1 + \dots + y_k$ и перемножения $y_1 \times \dots \times y_k$ аргументов, функции максимума $\max\{y_1, \dots, y_k\}$ и минимума $\min\{y_1, \dots, y_k\}$.

Определим функции Беллмана $V_k(y)$, $0 \le y \le r$:

$$V_1(y) = \max_{0 \le x_1 \le y} f_1(x_1),$$

$$V_k(y) = \max_{x_1 \ge 0, \dots, x_k \ge 0, \ x_1 + \dots + x_k \le y} A(f_1(x_1), \dots, f_k(x_k)), \ k = 1, 2, \dots, n.$$

Уравнение Беллмана в данной задаче имеет вид

$$V_{k+1}(y) = \max_{x_1 \ge 0, \dots, x_{k+1} \ge 0, \ x_1 + \dots + x_{k+1} \le y} A(f_1(x_1), \dots, f_k(x_k), f_{k+1}(x_{k+1})) =$$

$$= \max_{x_1 \ge 0, \dots, x_{k+1} \ge 0, x_1 + \dots + x_{k+1} \le y} A(A(f_1(x_1), \dots, f_k(x_k)), f_{k+1}(x_{k+1})) =$$

$$= \max_{0\le x_{k+1}\le y} A\left(\max_{x_1\ge 0,\dots,x_k\ge 0,\, x_1+\dots+x_k\le y-x_{k+1}} A(f_1(x_1),\dots,f_k(x_k)), f_{k+1}(x_{k+1}) \right) =$$

$$= \max_{0\le x_{k+1}\le y} A(V_k(y-x_{k+1}), f_{k+1}(x_{k+1})).$$

После построения функций Беллмана нахождение оптимального решения происходит в обратном порядке путем решения задач

$$x_n^* \in \arg\max_{0\le x_n\le r} A(V_{n-1}(r-x_n), f_n(x_n)),$$

$$x_{n-1}^* \in \arg\max_{0\le x_{n-1}\le r-x_n^*} A(V_{n-2}(r-x_n^*-x_{n-1}), f_{n-1}(x_{n-1}))$$

и т.д. до $n=1$.

ЗАКЛЮЧЕНИЕ

В работе ряд моделей теории исследования операций по оптимальному распределению ресурсов адаптированы к задаче планирования защиты объектов критической инфраструктуры от террористических атак. Дальнейшие исследования могут быть направлены на детальную проработку моделей угроз в зависимости от ресурсов и планов защиты, т.е. на аппроксимацию множества вероятностных стратегий атакующей стороны $Y_a^*(x,\omega_a)$, вероятностей успешности атаки $q_i(x_i,\omega_a)$ и разработку методов решения задач двухуровневого стохастического программирования вида (6), (7). Рассмотренный метод иерархического динамического программирования обоснован в предположении непересечения потомков не подчиненных одна другой вершин $i\ne j$ дерева угроз ($L_i\cap L_j=\varnothing$ для $i\notin L_j$, $j\notin L_i$). Он может быть обобщен на случай пересечения потомков, как это имеет место в сетевом динамическом программировании [47, 49].

СПИСОК ЛИТЕРАТУРЫ

1. Wright P.D., Liberatore M.J., Nydick R.L. A survey of operations research models and applications in homeland security. *Interfaces*. 2006. Vol. 36, N 6. P. 514–529.
2. Herrmann J.W. Using operations research methods for homeland security problems. *Handbook of Operations Research for Homeland Security.* Herrmann J.W. (Ed.). *International Series in Operations Research & Management Science*. Vol. 183. New York: Springer, 2013. P. 1–24.
3. Ermoliev Y., von Winterfeldt D. Systemic risks and security management. *Managing Safety of Heterogeneous Systems. Decisions under Uncertainty and Risks*. Ermoliev Y., Makowski M., Marti K. (Eds.). *Lecture Notes in Economics and Mathematical Systems*. 2012. Vol. 658. Berlin; Heidelberg: Springer-Verlag, 2012. P. 19–49.
4. Гайворонский А.А., Ермольев Ю.М., Кнопов П.С., Норкин В.И. Математическое моделирование распределенных катастрофических и террористических рисков. *Кибернетика и системный анализ.* 2015. Т. 51, № 1. С. 97–110.
5. Норкин В.И. Математические модели и методы планирования операций для АТО. *Тези доп. Міжнар. наук. конф. «Сучасна інформатика: проблеми, досягнення та перспективи розвитку»* (Київ, 13–15 грудня 2017 р.). Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2017. С. 114–116.
6. Норкин В.И. Оптимизационные модели антитеррористической защиты. *Кибернетика и системный анализ* (В печати).
7. Willis H.H., Morral A.R., Kelly T.K., Medby J.J. Estimating terrorism risk. Santa Monica: RAND Corporation, 2005. 94 p. URL: https://www.rand.org/pubs/monographs/MG388.html.

8. Brown G., Carlyle M., Salmeryn J., Wood K. Defending critical infrastructure. *Interfaces*. 2006. Vol. 36, N 6. P. 530–544.

9. Masse T., O'Neil S., Rollins J. The Department of homeland security's risk assessment methodology: Evolution, Issues, and Options for Congress. CRS report for Congress RL33858. Washington: Congressional Research Service, 2007. 33 p. URL: https://fas.org/sgp/crs/homesec/RL33858.pdf.

10. Risk analysis of security threats. Bier V.M., Azaiez M.N. (Eds.). New York: Springer, 2009. 236 p.

11. Cox L.A. Jr. Game theory and risk analysis. *Risk Analysis*. 2009. Vol. 29, N 8. P. 1062–1068.

12. Sandler T., Siqueira K. Games and terrorism: recent developments. *Simul. Gamin*g. 2009. Vol. 40, N 2. P. 164–192.

13. Guikema S.D. Game theory models of intelligent actors in reliability analysis: An overview of the state of the art. *Risk Analysis of Security Threats.* Bier V.M., Azaiez M.N. (Eds.). New York: Springer, 2009. P. 13–31.

14. Ezell B.C., Bennett S.P., von Winterfeldt D., Sokolowski J., Collins A.J. Probabilistic risk analysis and terrorism risk. *Risk Analysis.* 2010. Vol. 30, N 4. P. 575–589.

15. Handbook of operations research for homeland security. Herrmann J.W. (Ed.). *International Series in Operations Research & Management Science.* 2013. Vol. 183. New York: Springer, 2013. 221 p.

16. Безопасность критических инфраструктур: Математические и инженерные методы анализа и обеспечения. Харченко В.С. (ред.). Харьков: Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2011. 641 с.

17. Зелена книга з питань захисту критичної інфраструктури в Україні. Зб. матеріалів міжнар. експертних нарад. За заг. ред. О.М. Суходолі. Київ: Національний інститут стратегічних досліджень, 2015. 176 с.

18. Cormican K.J., Morton D.P., Wood R.K. Stochastic network interdiction. *Oper. Res*. 1998. Vol. 46. P. 184–197.

19. Morton D.P. Stochastic network interdiction. *Wiley Encyclopedia of Operations Research and Management Science.* Cochran J.J. (Ed.). Hoboken, NJ: John Wiley & Sons, 2010. P. 1–15.

20. Wang C. Allocation of resources for protecting public goods against uncertain threats generated by agents. IIASA Interim Report IR-10-012. Laxenburg, Austria: Int. Inst. for Applied Systems Analysis, 2010. 34 p.

21. Hu J., Homem-de-Mello T., Mehrotra S. Risk-adjusted budget allocation models with application in homeland security. *IIE Transaction*s. 2011. Vol. 43, N 12. P. 819–839.

22. Ermoliev Y.M., Norkin V.I. Sample average approximation method for compound stochastic optimization problems. *SIAM Journal on Optimization*. 2013. Vol. 23, N 4. P. 2231–2263.

23. Armbruster B., Luedtke J. Models and formulations for multivariate dominance constrained stochastic programs. *IIE Transactions.* 2014. Vol. 45, Iss. 1. P. 1–14.

24. Cox A. Some limitations of "risk = threat × vulnerability × consequence" for risk analysis of terrorist attacks. *Risk Analysis*. 2008. Vol. 28, N 6. P. 1749–1761.

25. Cox A. What's wrong with hazard-ranking systems? An expository note. *Risk Analysis*. 2009. Vol. 29, N 7. P. 940–948.

26. Brown G.G., Cox L.A. Jr. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis*. 2011. Vol. 31, N 2. P. 196–204.

27. Bier V.M., Oliveros S., Samuelson L. Choosing what to protect: strategic defensive allocation against an unknown attacker. *J. Public Econ. Theory.* 2007. Vol. 9, N 4. P. 563–587.

28. Bier V.M., Haphuriwat N., Menoyo J., Zimmerman R., Culpen A. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Analysis*. 2008. Vol. 28, N 3. P. 763–770.

29. Данскин Дж.М. Теория максимина и ее приложение к задачам распределения вооружения. Москва: Сов. радио, 1970. 200 с.

30. Jenelius E., Westin J., Holmgren Å. J. Critical infrastructure protection under imperfect attacker perception. *International Journal of Critical Infrastructure Protection.* 2010. Vol. 3, Iss. 1. P. 16–26.

31. Dempe S. Foundations of bilevel programming. Dordrecht: Kluwer Academic Publishers, 2002. 306 p.

32. Dempe S., Zemkoho A.B. The bilevel programming problem: Reformulations, constraint qualications and optimality conditions. *Mathematical Programming*. 2013. Vol. 138, N 1. P. 447–473.

33. Scaparra M.P., Church R.L. A bilevel mixed-integer program for critical infrastructure protection planning. *Computers & Operations Research.* 2008. Vol. 35, N 6. P. 1905–1923.

34. Gaivoronski A.A., Werner A. Stochastic programming perspective on the agency problems under uncertainty. *Managing Safety of Heterogeneous Systems: Decisions under Uncertainties and Risks.* Ermoliev Y., Makowski M., Marti K. (Eds.). *Lecture Notes in Economics and Mathematical Systems.* 2012. Vol. 658. Berelin; Heidelberg: Springer-Verlag, 2012. P. 137–167.

35. Yanikoglu I., Kuhn D. Decision rule bounds for two-stage stochastic bilevel programs. *SIAM Journal on Optimization.* 2017. Vol. 28, N 1. DOI: 10.1137/16M1098486.

36. Ермольев Ю.М. Модели и методы стохастического программирования. Москва: Наука, 1976. 280 с.

37. Нурминский Е.А. Численные методы решения детерминированных и стохастических минимаксных задач. Киев: Наук. думка, 1979. 161 с.

38. Ермольев Ю.М., Норкин В.И. Методы решения невыпуклых негладких задач стохастической оптимизации. *Кибернетика и системный анализ.* 2003. № 5. С. 89–106.

39. Ushakov I.A. Optimal resource allocation with practical statistical applications and theory. Hoboken: Wiley, 2013. 238 p.

40. Azaiez M.N., Bier V.M. Optimal resource allocation for security in reliability systems. *European Journal of Operational Research*. 2007. Vol. 181, Iss. 2. P. 773–786.

41. Kuznetsov N.Yu. Fault trees — problems and the modern state of investigations. *Кибернетика и системный анализ.* 1994. № 3. С. 128–150.

42. Кузнецов Н.Ю., Михалевич К.В. Анализ надежности систем, описываемых деревьями отказа с эффективностями. *Кибернетика и системный анализ.* 2003. № 5. С. 142–151.

43. Волкович В.Л., Волошин А.Ф., Заславский В.А., Ушаков И.А. Модели и методы оптимизации надежности сложных систем. Михалевич В.С. (ред.). Киев: Наук. думка, 1993. 312 с.

44. Schneier B. Secrets and lies. Digital security in a networked world. Indianapolis, Indiana: Wiley Publishing, 2000. 414 p.

45. Ingoldsby T.R. Attack tree-based threat risk analysis. Calgary (Alberta, Canada): Amenaza Technologies Limited, 2013. 40 p.

46. Норкин В.И., Онищенко Б.О. Оптимизация надежности сложной системы стохастическим методом ветвей и границ. *Кибернетика и системный анализ.* 2008. № 3. С. 129–141.

47. Bertelè U., Brioschi F. Nonserial dynamic programming. New York; London: Academic Press, 1972. 236 p.

48. Бурков В.Н., Буркова И.В. Задачи дихотомической оптимизации. Москва: Радио и связь, 2003. 156 с.

49. Бурков В.Н., Буркова И.В., Попок М.В., Овчинникова Т.И. Метод сетевого программирования. *Пробл. управл.* 2005. Вып. 3. С. 23–29.

50. Обен Ж.-П., Экланд И. Прикладной нелинейный анализ. Москва: Мир, 1988. 512 с.

Надійшла до редакції 16.02.2018

В.І. Норкін, О.О. Гайворонський, В.А. Заславський, П.С. Кнопов

МОДЕЛІ ОПТИМАЛЬНОГО РОЗПОДІЛУ РЕСУРСІВ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. Розглянуто можливості застосування моделей і методів теорії дослідження операцій до планування захисту об'єктів критичної інфраструктури. Адаптація цих моделей враховує стохастичну, інформаційну та поведінкову невизначеності терористів. Зокрема розглянуто відповідні узагальнення задач антагоністичної гри нападу і захисту, раціонального розподілу захисних ресурсів та запропоновано методи розв'язання виниклих оптимізаційних задач.

Ключові слова: захист критичної інфраструктури, розподіл ресурсів, дворівневе стохастичне програмування, ієрархічне динамічне програмування.

V.I. Norkin, A.A. Gaivoronski, V.A. Zaslavsky, P.S. Knopov

MODELS OF THE OPTIMAL RESOURCES ALLOCATION FOR THE CRITICAL INFRASTRUCTURE PROTECTION

Abstract. Adaptation of the operations research models and methods to planning of the critical infrastructure protection is considered. The adaptation of these models consists in accounting for the stochastic, informational, and behavioral uncertainty of terrorists. In particular, relevant generalizations of the antagonistic attack–defense game, optimal allocation of protective resources, and methods to solve the appearing optimization problems are proposed.

Keywords: critical infrastructure protection, resource allocation, two-level stochastic programming, hierarchical dynamic programming.

Норкин Владимир Иванович,
доктор физ.-мат. наук, ведущий научный сотрудник Института кибернетики им. В.М. Глушкова НАН Украины, Киев; профессор кафедры Национального технического университета Украины «Киевский политехнический институт имени Игоря Сикорского»,
e-mail: vladimir.norkin@gmail.com.

Гайворонский Алексей Алексеевич,
профессор, Факультет индустриальной экономики и технологий, Норвежский университет науки и технологий, Трондхейм, Норвегия,
e-mail: alexei.gaivoronski@iot.ntnu.no.

Заславский Владимир Анатольевич,
доктор техн. наук, профессор кафедры Киевского национального университета имени Тараса Шевченко,
e-mail: zas.vlad@gmail.com.

Кнопов Павел Соломонович,
чл.-кор. НАН Украины, профессор, заведующий отделом Института кибернетики им. В.М. Глушкова НАН Украины, Киев,
e-mail: knopov1@yahoo.com.