Научная статья

УДК 378

МОДЕЛИ И МЕТОД ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ФОРМИРОВАНИЮ УЧЕБНЫХ ПРОГРАММ ДИСЦИПЛИН ВОЕННО-ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ

Андрей Юрьевич Кийко[1], Станислав Федорович Мазурин[2], Александр Вадимович Фетисов[3], Александр Михайлович Казимирович[4]
[1–4] Академия войск национальной гвардии, Санкт-Петербург, Россия
[1] kiikovich@mail.ru
[2] svyatoslav53@mail.ru
[3] Eletskaysveta@yandex.ru
[4] sps5401@mail.ru

Аннотация. Разработан методологический подход к построению моделей типовых задач поддержки принятия решений, формирующий содержание учебных программ дисциплин военно-профессиональной подготовки в условиях цифровой трансформации процесса подготовки специалистов в военных вузах. В качестве критерия оптимальности решений используется требование минимизация возможного ущерба от инцидентов кибербезопасности. Предложен общий метод оптимизации решений с учетом нелинейного характера целевых функций моделей. Модели и метод имеют универсальный характер и могут быть использованы при разработке конкретных методик обоснования состава систем кибербезопасности организаций с учетом особенностей возможных угроз.

Ключевые слова: цифровая трансформация производства, угрозы цифрового производства, система кибербезопасности организации, учебные программы, военная подготовка, метод оптимизации решений

Для цитирования: Кийко А.Ю., Мазурин С.Ф., Фетисов А.В., Казимирович А.М. Модели и метод поддержки принятия решений по формированию учебных программ дисциплин военно-профессиональной подготовки // Вестник Военной академии войск национальной гвардии. 2024. № 4 (29). С. 205–212. URL: https://vestnik-spvi.ru/2024/12/021.pdf.

Original article

MODELS AND METHOD OF DECISION SUPPORT FOR THE FORMATION OF CURRICULA FOR MILITARY PROFESSIONAL TRAINING DISCIPLINES

Andrej Yu. Kijko[1], Stanislav F. Mazurin[2], Aleksandr V. Fetisov[3], Alexander M. Kazimirovich[4]
[1–4] Academy of the National Guard Troops, Saint-Petersburg, Russia
[1] kiikovich@mail.ru
[2] svyatoslav53@mail.ru
[3] Eletskaysveta@yandex.ru
[4] sps5401@mail.ru

Abstract. A methodological approach has been developed to construct models of typical decision support tasks for the formation of the content of educational programs for military professional training disciplines in the conditions of digital transformation of the process of training specialists in military universities. The requirement to minimize possible damage from cybersecurity incidents is used as a criterion for the optimality of solutions. A general method for optimizing solutions is proposed, taking into account the nonlinear nature of the objective functions of the models. The models and method are universal in nature and can be used to develop specific methods for substantiating the composition of companies' cybersecurity systems, taking into account the characteristics of possible threats.

Keywords: digital transformation of production, threats to digital production, company cybersecurity system, training programs, military training, solution optimization method

For citation: Kijko A.Yu., Mazurin S.F., Fetisov A.V., Kazimirovich A.M. Models and method of decision support for the formation of curricula for military professional training disciplines. Vestnik Voennoj akademii vojsk nacional'noj gvardii. 2024;4(29): 205–212. (In Russ.). Available from: https://vestnik-spvi.ru/2024/12/021.pdf.

Введение

Одним из сопутствующих эффектов организаций, связанных с интенсивным внедрением информационных технологий в управление ими, является обострение проблем обеспечения их кибернетической безопасности [1–5]. Такие условия определяются тем, что включение управления технологическими и другими процессами (в том числе и образовательной деятельностью) в глобальное киберпространство значительно повысило вероятность внешнего деструктивного информационного воздействия – кибератак на результаты их функционирования [6–12]. В связи с этим разработка и внедрение систем кибербезопасности, способных предотвратить или минимизировать риски от воздействий извне, особенно для организаций, где функционирует секретная информация, является наиболее актуальной проблемой. Одной из задач в ходе разработки таких систем является оптимизация их состава с учетом возможных инцидентов кибербезопасности конкретной организации. Проблематика оптимизации системы, а также значительные по объему материальные убытки, появляющиеся вследствие ошибок при определении элементов, входящих в системы кибербезопасности, могут быть устранены только на основе разработки моделей оптимизации решений.

Исходя из такой проблемы, статья посвящена методам обоснования моделей типовых задач и обобщенного метода оптимизации решений по формированию элементарного состава системы кибербезопасности.

Материалы и методы

Предлагаемые типовые модели предназначены для определения состава системы кибербезопасности любой организации в ситуации, когда определены возможные угрозы и проведена оценка их последствий.

Для противодействия угрозам имеется совокупность частных проектов (элементов), каждый из которых может с некоторой долей вероятности обеспечить предотвращение (снижение) ущерба для определенного подмножества инцидентов, связанных с этими угрозами.

Оптимальный вариант системы кибербезопасности представляет собою комплекс частных проектов (элементов), позволяющих максимально снизить ущерб организации от возможных кибератак. При построении математических моделей типовых задач по формированию состава систем кибербезопасности, следует применить аппарат теории дискретного математического программирования [13–17]. Предлагаемый метод оптимизации учитывает нелинейный характер используемых в моделях целевых функций.

Результаты

В качестве типовых моделей, для решения задач поддержки принятия решений на формирование состава систем кибербезопасности, рассмотрим:

a) модель для формирования системы защиты от независимых деструктивных воздействий;

b) модель для формирования системы с учетом взаимосвязанности угроз;

c) модель для формирования состава системы с одновременным выбором способов реализации ее элементов.

Модель для формирования системы защиты от попыток несанкционированного доступа

Представим, что в киберпространстве циркулируют N типов угроз несанкционированного доступа в информационную систему организации, которые могут наносить существенный ущерб $R_j j = \overline{1,N}$ информационно управляющей системе. Для получения минимального риска на основе устранения угроз при функционировании системы необходимо использовать M типов средств защиты. При таком условии эффективность применения i-го средства с целью минимизации ущерба от угрозы j-го типа можно выразить как w_{ij} (то есть значением вероятности абсолютного исключения ее воздействия или значением математического ожидания относительного снижения ущерба при воздействии рассматриваемой угрозы). При встраивании в структуру системы $\delta = \|\delta_{ij}\|, i = \overline{1,M};\ \ j = \overline{1,N}$ множества l_j средств защиты от j-й угрозы, численное значение снижения ущерба можно определить по зависимости вида:

$$f_j(\delta) = R_j, \qquad (1)$$

Необходимо определить такой вариант состава системы кибербезопасности, при котором достигается максимальное снижение ущерба от возможных инцидентов.

Соответствующая модель формирования оптимального состава системы кибербезопасности принимает следующий вид.

Определить состав системы кибербезопасности

$$\delta = \|\delta_{ij}\|, i = \overline{1,M}, j = \overline{1,N} \quad (2)$$

такой что

$$F(\delta *) = \max_{\delta} \sum_{j=1}^{N} R_j \quad (3)$$

$$\sum_{j=1}^{N} \delta_{ij} = 1, \quad i = \overline{1,M},$$

при

$$\delta_{ij} \in \{0,1\}, 0 \le w_{ij} \le 1, \quad R_j \ge 0, i = \overline{1,M}; j = \overline{1,N}. \quad (4)$$

Модель формирования кибербезопасности с учетом взаимосвязанности угроз

Важным фактором для приложений обобщением модели (2) - (4) выступает учет взаимосвязанности возможных угроз системе. Один из возможных способов их учета проистекает из предположения о том, что, если в итогом проведения защитных мероприятий угроза *j*-го типа нейтрализована, то с вероятностью a_{jr}, $j = \overline{1,N}$, $r = \overline{1,N}$, исключается связанная с ней угроза *r*-го типа. Общая модель формирования элементов системы в таком случае получит следующий вид.

Определить вариант состава системы

$$\delta = \|\delta_{ij}\|, \quad i = \overline{1,M}; \quad j = \overline{1,N}, \quad (5)$$

такой, что

$$F(\delta) = \max_{\delta} \sum_{r=1}^{N} R_r, \quad (6)$$

при

$$\sum_{j=1}^{N} \delta_{ij} = 1, \quad i = \overline{1,M}, \quad R_r \ge 0, \quad (7)$$

$$\delta_{ij} \in \{0,1\}, \quad 0 \le \varepsilon_{ij} \le 1, \quad 0 \le \alpha_{jr} \le 1, \quad \alpha_{jj} = 1. \quad (8)$$

Модель формирования состава системы кибербезопасности с одновременным выбором способов реализации ее элементов

Рассмотренный подход к формализации моделей формирования состава системы кибербезопасности может быть обобщен для ситуации, когда наряду с выбором включаемых в состав системы элементов необходимо принимать решения о методах реализации этих элементов. В таких условиях модель формирования оптимального варианта состава системы кибербезопасности организации может быть описана следующим математическим выражением:

$$F(\delta^{*}) = \max_{\delta} \sum_{j=1}^{N} f_j(\delta), \quad (9)$$

при

$$\sum_{j=1}^{N} \sum_{k=1}^{K} \delta_{i_{jk}} = 1, \quad i = \overline{1,M}, \quad (10)$$

$$\delta_{ijk} \in \{0,1\}, \quad i = \overline{1,M}; \quad j = \overline{1,N}, \quad k = \overline{1,k}, \quad (11)$$

где *k* – идентификатор способа реализации элементов системы кибербезопасности.

Метод решения задач по оптимизации состава систем кибербезопасности

Рассмотренные в п. п. 3.1–3.3 модели задач оптимизации системы кибербезопасности могут быть обобщенно представлены в виде модели, составляющей процесс оптимизации функции «булевых» переменных (разработаны английским математиком Д. Булем в XIX веке) следующего типа.

Тогда вариант решения может быть определен следующим образом:

$$\delta = \|\delta_{ij}\|, \quad i = \overline{1,M}; \quad j = \overline{1,N}, \quad (12)$$

при этом,

$$F(\delta *) = \max_{\delta} \sum_{j=1}^{N} f_j(\delta), \quad (13)$$

$$\sum_{j=1}^{N} \delta_{ij} = 1, i = \overline{1,M}, \quad (14)$$

где

$$\delta = \|\delta_{ij}\|, \ \delta_{i_j} \in \{0,1\}, \ i = \overline{1,M}; \ j = \overline{1,N};$$

$f_j(\delta)$ – переменные, относящиеся к неубывающим; функции, имеющие облик выпуклых к верху;

N, M – выражаются только целыми положительными числами.

Методом, позволяющим определить решение задачи по оптимизации модели (12) – (14) с необходимой точностью, является применение вариантов метода ветвей и границ. В данных условиях можно также использовать динамическое программирование [18–20]. Но возможности каждого из этих методов ограничиваются максимальным размером матрицы ***δ***. Это обусловлено тем, что задача (12) – (14) относится к классу *NP* (является сложно решаемой) [21, 22]. Вместе с тем для таких задач на практике не требуется поиска оптимального решения. В таком случае применяются приближенные методы.

Поэтому в рассматриваемых условиях предлагается метод решения задачи оптимизации относительно моделей типа (12) – (14). Метод относится к градиентно-разносторонним. Его сущность состоит в квазиэквивалентном переходе от задачи оптимизации (12) – (14). Он заключается в выборе вектора $\delta = \|\delta_{ij}\|$ к ряду *M* последовательно решаемых задач по выбору одной переменной вида $\delta_{ij} = 1$.

Ее выбор при каждом последовательном *t*-м шаге ($t = \overline{1,M}$) происходит по следующему алгоритму

$$\delta_{i*j*}{}^{t=1}, \text{ если } \Delta f_{i*j*}{}^{t} = \max_{G(t)} \Delta f_{ij}^{t}, \ \delta_{ij}^{t} = 0,$$

если $\Delta f_{i*j*}{}^{t} \ne \max_{G(t)} \Delta f_{ij}^{t}$, (15)

где *G(t)* – подмножество переменных $\delta_{ij} = i = \overline{1,M}; j = \overline{1,N}$, из которых производится выбор;

Δf_{ij}^{t} – величина приращения функции (12) на *t*-м шаге $t = \overline{1,M}$, при условии $\delta_{ij} = 1$.

В подмножество $G(t)$ входят переменные δ_{ij}, со следующими характеристиками

$$\Delta f_{ij}^t, \max_{j=\overline{1,N}} \Delta f_{ij}^t, i \in I_t'; \Delta f_{ij}^t, \max_{i \in I_t} \Delta f_{ij}^t, i \in J_t', \quad (16)$$

где I_t — подмножество индексов i переменных вида δ_{ij}, с характеристиками $\delta_{ij}^{t-1} = 0, i = \overline{1,M}; j = \overline{1,N}$ (подмножество переменных, незакрепленных до -го шага);

I_t' – подмножество, состоящее из индексов i переменных $\delta_{ij}, i \in I_t; j = \overline{1,N}$, для которых $\max_i a_i^t = c^t, i \in I_t;$ (17)

J_t' – подмножество, состоящее из индексов j переменных $\delta_{ij}, i \in I_t; j = \overline{1,M}$,

характеризующихся следующим образом

$$\max_j B_j^t = c^t, j = \overline{1,N}; \quad (18)$$

$$C^t = \max\left\{\max_{i \in I_t} a_i^t; \max_{j=\overline{1,N}} B_j^t\right\}; \quad (19)$$

$$a_i^t = \min_{j=\overline{1,N}}\left(\max_{j=\overline{1,N}} \Delta f_{ij}^t - \Delta f_{ij}^t\right), i \in I_t; \quad (20)$$

$$B_j^t = \min_{i \in I_t}\left(\max_{i \in I_t} \Delta f_{ij}^t - \Delta f_{ij}^t\right), j = \overline{1,N}. \quad (21)$$

Физическое содержание соотношения (20), (21) представляет собой оценки потерь эффективности кибербезопасности в случаях невключения соответствующих элементов в состав системы на t-м шаге.

Условия, приведенные в (16) – (19), указывают на переменные, для которых при $\delta_{ij}^t = 0$ потери оцениваются как максимальные. При этом условие (15) характеризует вариант, обеспечивающий максимальное приращение функции (12).

По своей сущности решение задачи (15) – (21) при каждом шаге t (t=1,2,…,M) определяет выбор направления подъема для задачи, описанной моделью (12) – (14). Исходя из этого задачу (15) – (21) следует понимать в виде принципа выбора направления подъема (повышения эффективности системы). Последовательное применение дает возможность определить решение, близкое к оптимальному (12) – (14).

Исходя из изложенного материала, можно заключить, что оптимизация решения сводится к эквивалентности задач по оптимизации (12) – (14) и (15) – (21). Из приведенной информации, очевидно, что для однотипных средств защиты рассмотренные задачи эквивалентны, а их решение – оптимально. При этом полученное решение (15) – (21) является приближенным решением оптимизации для модели (12) – (14), но считается оптимальным, так как удовлетворяет необходимым условиям.

Алгоритм, применяемый при реализации метода для задач (12) – (14) при последовательном решении задач (15) – (21), состоит в определенной последовательностью решения частных задач:

1. Принять t=1, и полагать, что множество $I_t = \{1,2,\ldots,M\}$.
2. Установить элементы матрицы приращения $\|\Delta f_{ij}\|, \ i = \overline{1,M}; \ j = \overline{1,N}$.
3. Определить множество $G(t)$ из условий (16) – (21).
4. Из условия (15) определить $\delta_{i\ j}^t = 1$ и убрать индекс i из множества I_t.
5. Проверить условие $I_t = \emptyset$. Если соблюдается (да), то перейти к п.8, если не соблюдается (нет), то – к п.6.
6. Принять $t = t + 1$.
7. Пересчитать элемент j -го сечения матрицы приращений $\Delta f^t = \|\Delta f_{ij}^t\|$ при условии $\delta_{i\ j}^{t-1} = 1$, перейти к п.3.
8. Вычислить функцию $F(\delta)$.
9. Получить решение.

Особенности алгоритмов п. п. 3.1–3.3 типовых задач с применением метода оптимизации связаны с вычислением элементов матрицы приращений

$$\Delta f^t = \|\Delta f_{ij}^t\|, \ i = \overline{1,M}; \quad j = \overline{1,N}$$

Для модели (2) - (4) с учетом условия (1) получим $\Delta f_{ij}^t = R_j \prod_{k \in I_j^{t-1}} \varepsilon_{kj} w_{ij}, j = \overline{1,N};$ j $\in I_t$, (22)

где: $\varepsilon_{kj} = 1 - w_{kj}$,

I_j^{t-1} – множество элементов для противодействия угрозам j-го типа, ранее включенных в состав системы кибербезопасности.

Для модели (5) – (8) элементы матрицы приращений определяются по выражению:

$$\Delta f_{ij}^t = \sum_{r=1}^N R_r^{t-1} \frac{w_{ij} Q_j^{t-1} \alpha_{jr}}{1 - P_j^{t-1} \alpha_{jr}}, \quad j = \overline{1,N}, \quad i = \overline{1,M}, \quad (23)$$

где

$$R_r^t = R_r^{t-1} \frac{1 - P_j^t \alpha_{jr}}{1 - P_j^{t-1} \alpha_{jr}}; \quad P_j^t = 1 - \prod_{i=1}^{M} \varepsilon_{ij}^{\delta_{ij}^t};$$

$$Q_j^t = 1 - P_j^t, \quad r = \overline{1,N}, j = \overline{1,N}.$$

Для модели (12) – (14) правило выбора переменной для включения в решение на -ом шаге алгоритма формализовано выражением:

$$\delta_{i*j*k*} = \begin{cases} 1, \text{если } \Delta f_{i*j*k*}^{t} = \max_{G(t)} \Delta f_{ijk'}^t \end{cases} \quad (24)$$

Подмножество $G(t)$ включает переменные δ_{ijk}, для которых

$$\Delta f_{i'j'k'}^t = \max_{\substack{i=\overline{1,N} \\ k=\overline{1,K}}} \Delta f_{ijk}^t, \quad j \in J_t', \quad (25)$$

где I_t – подмножество индексов i, не включенных в состав рассматриваемой системы;

I_t' – подмножество индексов i переменных δ_{ijk}, $i \in I_t$, j = $\overline{1,N}$, $k = \overline{1,K}$,

для которых

$$\max_{i\in I_t}\ \min_{k=1,k}\ a_{ik}^t = c^t; \max_{j=1,N}\ \min_{k=1,k}\ B_{jk}^t = c; \quad (26)$$

$$c^t = \max\left\{\max_{i\in I_t}\min_{k=1,k} a_{ik}^t; \max_{i=1,N}\min_{k=1,K} B_{jk}^t\right\}; \quad (27)$$

$$a_{ik}^t = \min_{j=1,N}\left(\max_{i=1,N}\Delta f_{ijk}^t - \Delta f_{ijk}^t\right), i \in I_t; B_{jk}^t =$$

$$\min_{i\in I_t}\left(\max_{i\in I_t}\Delta f_{ijk}^t - \Delta f_{ijk}^t\right), j = \overline{1,N}; k = \overline{1,K}. \quad (28)$$

Дальнейшая конкретизация моделей и алгоритмов оптимизации опирается на явное задание вида функции зависимости $F(\delta)$ с учетом особенностей объекта защиты и характера угроз.

Обсуждение

Статистические данные свидетельствуют, что в мировой практике наблюдается рост числа хакерских атак. Составителями индекса киберрисков Trend Micro подсчитано, что только в 2020 году до четверти организаций мира не менее 7 раз каждая подвергались кибератакам преступников. В последующие годы ситуация будет ухудшаться. До 83 % опрошенных считают, что атаки с очень высокой вероятностью будут успешными [23]. Практический опыт 2024 года подтверждает приведенный прогноз.

По данным Center for Strategic and International Studies USA, с 2018 года убытки от кибератак в мире выросли на 50 %. Средний убыток от каждой из них исчисляется суммой более 0,5 млн долларов. Глобальные убытки при этом составляют до 1 % от мирового ВВП. В России число хакерских атак только на стратегические организации только за 2020 год увеличилось в два раза по сравнению с предыдущим [24].

Поэтому создание эффективных систем кибербезопасности организаций является наиболее актуальной задачей в условиях развития IT-технологий. Сложность решения задачи требует разработки научно-методического аппарата формирования рассмотренных систем. При построении математических моделей типовых задач поддержки принятия решений, по формированию состава систем кибербезопасности, целесообразно использовать математический аппарат теории дискретного математического программирования.

Заключение

Таким образом, в статье представлен методологический подход к построению моделей формирования оптимального состава систем кибербезопасности организаций. В качестве критерия оптимальности в моделях используется требование минимизация ущерба от инцидентов кибербезопасности. Для решения задач предлагается метод оптимизации решений с учетом нелинейного характера целевых функций.

Предлагаемый в статье подход основывается на общих характеристиках поставленной в статье задачи. Поэтому он может служить теоретической основой для построения конкретных методик обоснования элементарного состава систем кибербезопасности организаций.

Список источников

1. Супрун А. Ф. Проблема инновационного развития систем информационной безопасности в транспортной отрасли // Автоматическое управление и вычислительная техника. 2018. № 52(8). С. 1105–1110. DOI: 10.3103/S0146411618080035.

2. Сонькин М. А. Методология реализации функции контроля в рамках концепции электронного правительства // International Journal of Scientific and Technology Research. 2020. № 9(2). С. 6259–6262.

3. Мулюкина В. Е. Киберриски малого и среднего бизнеса / В. Е. Мулюкина, Е. О. Козисова // Информационные системы и технологии: управление и безопасность. 2016. № 4. С. 117–122.

4. Ястребов О. Цифровая трансформация и модели оптимизации в сфере логистики // Труды SHS Web of Conf. 2018. V. 44. 00009. DOI: https://doi.org/10.1051/shsconf/20184400009.

5. Присяжнюк С. П. Показатели эффективности защиты информации в системе информационного взаимодействия для управления сложными распределенными организационными объектами // Автоматическое управление и вычислительная техника. 2017. Т. 51. № 8. С. 824–828. DOI: 10.3103/S0146411617080053.

6. Лось В. П. Подход к оценке эффективности обеспечения информационной безопасности в системах управления // Автоматика и вычислительная техника. 2020. Т. 54. № 8. С. 864–870. DOI: 10.3103/S0146411620080362.

7. Зотова Е. А. Модели прогнозирования рисков деструктивного воздействия на информационные процессы в системах управления // Информационно-управляющие системы. 2019. № 5. С. 18–23. DOI: 10.31799/1684-8853-2019-5-18-23.

8. Бажин Д. А. Риск-ориентированный подход к организации управления подсистемами защиты безопасности информационных систем // Автоматическое управление и вычислительная техника. 2016. № 50(8). С. 717–721. DOI: 10.3103/S0146411616080289.

9. Зайченко И. М. Модели прогнозирования ущерба от аварий на энергетических объектах и в энергосистемах предприятий // E3S Web of Conferences. 2019. № 110.

10. Гращенко Н. Обоснование финансирования мероприятий по предупреждению аварий в энергосистемах: Международная научная конференция «Энергоменеджмент коммунальных объектов и устойчивые энергетические технологии». 2018. DOI: 978-3-030-19868-8_30.

11. Сауренко Т. Эффективность обеспечения живучести информационно-управляющих систем логистики // E3S Web of Conferences. 2020. Т. 217. 07025. DOI: https://doi.org/10.1051/e3sconf/202021707025.

12. Лось В. П. Модель оптимальной комплексификации мер по обеспечению информационной безопасности. Автоматическое управление и вычислительная техника. 2020. № 54(8). С. 930–936. DOI: 10.3103 /S0146411620080374.

13. Алексеев А. О. Использование двойственности для повышения эффективности метода ветвей и границ при решении задачи о ранце // ЖВМФ. 1985. № 25(11). С. 1666–1673. U.S.S.R. Comput. Math. Math. Phys. 1985). № 25(6). С. 50–54. DOI: https://doi.org/10.1016/0041-5553(85)90008-4.

14. Сонкин М. Метод оптимизации производительности нескольких взаимосвязанных операций с использованием ресурсов и времени // International Journal of Applied Engineering Research. 2015. № 10(17). С. 38127–38132.

15. Сауренко Т. Н. Модель и метод планирования оценки объема и ассортимента инновационной продукции на промышленном предприятии // J. Phys.: Conf. Ser. 2017. 803(1). 012006. DOI: 10.1088/1742-6596/803/1/012006.

16. Черныш А. Модель и алгоритм обоснования решений по организации проекта высотного строительства // E3S Web of Conferences. 2018. 03003. DOI: https://doi.org/10.1051/e3sconf/20183303003.

17. Сонкин М. А. Математическое моделирование адаптивного распределения дискретных ресурсов: труды конференции 2016 года «Информационные технологии в науке, управлении, социальной сфере и медицине» (ИТССМСМ – 2016). 2016. С. 282–285. DOI https://doi.org/10.2991/itsmssm-16.2016.57.

18. Анисимов В. Г. Алгоритм ветвей и границ для одного класса задач планирования / В. Г. Анисимов, Е. Г. Анисимов // ЖВМФ. 1992. № 32(12). 2000–2005. Comput. Math. Math. Phys. 1992. 32(12). С. 1827–1883.

19. Анисимов В. Г. Модификация метода для одного класса задач целочисленного программирования / В. Г. Анисимов, Е. Г. Анисимов // ЖВМФ. 1997. № 37(2). С. 179–183 // Comput. Math. Math. Phys. 1997. № 37(2). С. 175–179.

20. Анисимов В. Г. Метод решения одного класса задач целочисленного программирования // ЖВМФ. 1989. № 29(10). С. 1586–1590. U.S.S.R. Comput. Math. Math. Phys. 1989. № 29(5). С. 238–241.

21. Алексеев А. О. Применение цепей Маркова при оценке вычислительной сложности симплекс-метода // Советский журнал вычислительной техники и системных наук. 1988. № 5. С. 130–134.

22. Анисимов В. Г. Алгоритм оптимального распределения дискретных неоднородных ресурсов на сети // ЖВМФ. 1997. № 37(1). С. 54–60. Comput. Math. Math. Phys. 1997. № 37(1). С. 51–57.

23. Каждая четвертая компания в мире подверглась атакам более 7 раз в 2020 году. URL: https://safe.cnews.ru/news/top/2021-02-04_kazhduyu_chetvertuyu_kompaniyu (дата обращения: 10.07.2024).

24. Цифровая трансформация, телекоммуникации, вещание и новости ИТ. URL: https://www.comnews.ru/content/212181/2020-12-15/2020-w51/kiberprestupniki-vredyat-trillion (дата обращения: 10.07.2024).

References

1. Suprun A. F. // Avtomaticheskoe upravlenie i vychislitel'naya tekhnika. 2018;52(8): 1105–1110. DOI: 10.3103/S0146411618080035. (In Russ.).

2. Son'kin M. A. Methodology for the implementation of the control function within the framework of the e-government concept // International Journal of Scientific and Technology Research. 2020;9(2): 6259–6262. (In Russ.).

3. Mulyukina V. E. Cyber risks of small and medium-sized businesses / V. E. Mulyukina, E. O. Kozisova // Information systems and technologies: management and security. 2016;4: 117–122. (In Russ.).

4. YAstrebov O. Cifrovaya transformaciya i modeli optimizacii v sfere logistiki // Trudy SHS Web of Conf. 2018. V. 44. 00009. DOI: https://doi.org/10.1051/shsconf/20184400009. (In Russ.).

5. Prisyazhnyuk S. P. Indicators of the effectiveness of information protection in the system of information interaction for the management of complex distributed organizational objects // Automatic control and computer technology. 2017. T. 51;8: 824–828. DOI: 10.3103/S0146411617080053. (In Russ.).

6. Los' V. P. Approach to Assessing the Effectiveness of Information Security in Management Systems // Automation and computer technology. 2020. T. 54;8: 864–870. DOI: 10.3103/S0146411620080362. (In Russ.).

7. Zotova E. A. Models for Forecasting the Risks of Destructive Impact on Information Processes in Control Systems // Information management systems. 2019. № 5. S. 18–23. DOI: 10.31799/1684-8853-2019-5-18-23. (In Russ.).

8. Bazhin D. A. Risk-Based Approach to the Organization of Management of Information Systems Security Subsystems // Automatic control and computer technology. 2016;50(8): 717–721. DOI: 10.3103/S0146411616080289. (In Russ.).

9. Zajchenko I. M. Modeli prognozirovaniya ushcherba ot avarij na energeticheskih ob''ektah i v energosistemah predpriyatij. E3S Web of Conferences. 2019;110. (In Russ.).

10. Grashchenko N. Obosnovanie finansirovaniya meropriyatij po preduprezhdeniyu avarij v energosistemah: Mezhdunarodnaya nauchnaya konferenciya «Energomenedzhment kommunal'nyh ob''ektov i ustojchivye energeticheskie tekhnologii». 2018. DOI: 978-3-030-19868-8_30. (In Russ.).

11. Saurenko T. Effektivnost' obespecheniya zhivuchesti informacionno-upravlyayushchih sistem logistiki // E3S Web of Conferences. 2020. T. 217. 07025. DOI: https://doi.org/10.1051/e3sconf/202021707025. (In Russ.).

12. Los' V. P. Model' optimal'noj kompleksifikacii mer po obespecheniyu informacionnoj bezopasnosti. Avtomaticheskoe upravlenie i vychislitel'naya tekhnika. 2020. № 54(8). S. 930–936. DOI: 10.3103 /S0146411620080374. (In Russ.).

13. Alekseev A. O. Ispol'zovanie dvojstvennosti dlya povysheniya effektivnosti metoda vetvej i granic pri reshenii zadachi o rance // ZHVMF. 1985;25(11): 1666–1673. U.S.S.R. Comput. Math. Math. Phys. 1985);25(6).: 50–54. DOI: https://doi.org/10.1016/0041-5553(85)90008-4. (In Russ.).

14. Sonkin M. Metod optimizacii proizvoditel'nosti neskol'kih vzaimosvyazannyh operacij s ispol'zovaniem resursov i vremeni // International Journal of Applied Engineering Research. 2015. № 10(17). S. 38127–38132. (In Russ.).

15. Saurenko T. N. Model' i metod planirovaniya ocenki ob''ema i assortimenta innovacionnoj produkcii na promyshlennom predpriyatii // J. Phys.: Conf. Ser. 2017. 803(1). 012006. DOI: 10.1088/1742-6596/803/1/012006. (In Russ.).

16. CHernysh A. Model' i algoritm obosnovaniya reshenij po organizacii proekta vysotnogo stroitel'stva // E3S Web of Conferences. 2018. 03003. DOI: https://doi.org/10.1051/e3sconf/20183303003. (In Russ.).

17. Sonkin M. A. Matematicheskoe modelirovanie adaptivnogo raspredeleniya diskretnyh resursov: trudy konferencii 2016 goda «Informacionnye tekhnologii v nauke, upravlenii, social'noj sfere i medicine» (ITSSMSM – 2016). 2016. S. 282–285. DOI https://doi.org/10.2991/itsmssm-16.2016.57. (In Russ.).

18. Anisimov V. G. Branch and Boundary Algorithm for a Single Planning Task Class /

V. G. Anisimov, E. G. Anisimov // ZHVMF. 1992;32(12). 2000–2005. Comput. Math. Math. Phys. 1992. 32(12). S. 1827–1883. (In Russ.).

19. Anisimov V. G. Modifikaciya metoda dlya odnogo klassa zadach celochislennogo programmirovaniya / V. G. Anisimov, E. G. Anisimov // ZHVMF. 1997;37(2): 179–183 // Comput. Math. Math. Phys. 1997. № 37(2). S. 175–179. (In Russ.).

20. Anisimov V. G. A method for solving a class of integer programming problems // ZHVMF. 1989;29(10): 1586–1590. U.S.S.R. Comput. Math. Math. Phys. 1989;29(5): 238–241. (In Russ.).

21. Alekseev A. O. Application of Markov Circuits in Estimating the Computational Complexity of the Simplex Method // Soviet Journal of Computer Engineering and System Sciences. 1988;5: 130–134. (In Russ.).

22. Анисимов В. Г. Algorithm for optimal distribution of discrete heterogeneous resources on the network // ЖВМФ. 1997;37(1): 54–60. Comput. Math. Math. Phys. 1997. № 37(1). С. 51–57. (In Russ.).

23. Kazhdaya chetvertaya kompaniya v mire podverglas' atakam bolee 7 raz v 2020 godu. Available from: https://safe.cnews.ru/news/top/2021-02-04_kazhduyu_chetvertuyu_kompaniyu (data obrashcheniya: 10.07.2024). (In Russ.).

24. Cifrovaya transformaciya, telekommunikacii, veshchanie i novosti IT. Available from: https://www.comnews.ru/content/212181/2020-12-15/2020-w51/kiberprestupniki-vredyat-trillion (data obrashcheniya: 10.07.2024). (In Russ.).

Информация об авторах

А.Ю. Кийко *– кандидат юридических наук*
С. Ф. Мазурин *– кандидат юридических наук, доцент*
А. В. Фетисов *– кандидат военных наук, доцент*
А. М. Казимирович *– кандидат педагогических наук*

Information about the authors

A. Yu. Kijko *– Candidate of Sciences (Law)*
S. F. Mazurin *– Candidate of Sciences (Law), Docent*
A. V. Fetisov *– Candidate of Sciences (Military), Docent*
A. M. Kazimirovich – *Candidate of Sciences (Pedagogy)*

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 12.09.2024; одобрена после рецензирования 14.11.2024; принята к публикации 23.12.2024.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

The article was submitted 12.09.2024; approved after reviewing 14.11.2024; accepted for publication 23.12.2024.