ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК [343.98:004.056] + 159.923 + 519.25

DOI: 10.21822/2073-6185-2026-53-1-86-95 Оригинальная статья/ Original article

Матричная модель определения уровня кибервиктимности

И.В. Карпасюк, А.И. Карпасюк
Астраханский государственный технический университет,
414056, г. Астрахань, ул. Татищева, 16, Россия

Резюме. Цель. Целью исследования является построение матричной модели определения уровня кибервиктимности**. Метод.** Представлена задача количественной оценки степени кибервиктимности на основе результатов прохождения теста Кеттела. Приведен алгоритм перевода математической модели определения степени склонности к подверженности киберпреступлению в матричную форму. **Результат.** Введено понятие комплексного критерия кибервиктимности. Разработана математическая модель выявления общего уровня склонности к кибервиктимности и представления результатов моделирования как в числовом, так и в качественном виде. Проведено тестовое моделирование, позволяющее проверить адекватность построенных моделей на разных видах исходных данных. **Вывод.** Подтверждена корректность матричной модели путем совпадения полученных результатов с результатами моделирования, проведенного по исходной модели. Описаны возможности программного продукта, разработанного на базе рассмотренных моделей. Предложены области применения программного продукта и пути его модернизации.

Ключевые слова: кибермошенничество, кибервиктимность, стены, тест Кеттела, черты характера, жертва, степень подверженности киберпреступлению, критерий кибервиктимности

Для цитирования: И.В. Карпасюк, А.И. Карпасюк. Матричная модель определения уровня кибервиктимности. Вестник Дагестанского государственного технического университета. Технические науки. 2026; 53(1):86-95. DOI:10.21822/2073-6185-2026-53-1-86-95.

Matrix model for determining the level of cybervictimization

I.V. Karpasyuk, A.I. Karpasyuk
Astrakhan State Technical University,
16 Tatishcheva St., Astrakhan 414056, Russia

Abstract. Objective. The aim of the study is to construct a matrix model for determining the level of cyber victimization. **Method.** The problem of quantitative assessment of cyber victimization based on the Cattell test is presented. An algorithm for converting the mathematical model for determining the degree of susceptibility to cybercrime into matrix form is provided. **Result.** The concept of a composite cybervictimization criterion is introduced. A mathematical model has been developed for identifying the level of propensity for cyber-victimization in both numerical and qualitative forms. Test modeling was conducted to verify the adequacy of the constructed models with different types of input data. **Conclusion.** The correctness of the matrix model was confirmed by the coincidence of the obtained results with the results of simulation conducted using the original model. The capabilities of the software application developed based on the considered models are described. Potential application areas for the software application and paths for its modernization are proposed.

Keywords: cyber fraud, cybervictimization, stens, Cattell test, character traits, victim, degree of exposure to cybercrime, cybervictimization criterion

For citation: I.V. Karpasyuk, A.I. Karpasyuk. Matrix model for determining the level of cybervictimization. Herald of Daghestan State Technical University. Technical Sciences. 2026;53(1):86-95. (In Russ) DOI:10.21822/2073-6185-2026-53-1-86-95.

Введение. В настоящее время неуклонно возрастает риск подвергнуться преступным воздействиям, совершаемым посредством информационно-телекоммуникационных технологий, как для физических лиц, так и для организаций, в том числе задействованных в сфере обеспечения функционирования критической инфраструктуры [1-3]. Поэтому в современном информационном обществе, где технологический прогресс и виртуальное взаимодействие становятся неотъемлемой частью повседневной жизни, особую актуальность приобретают вопросы, связанные с ужесточением требований в области кибербезопасности. Серьезную угрозу для информационной безопасности общества представляет кибермошенничество - наиболее распространенная форма киберпреступности, которая заключается в использовании компьютерных сетей и программного обеспечения для получения незаконной выгоды за счет обмана или нарушения доверия жертв.

Проведение кибератак не может быть осуществлено без использования технического оборудования. Однако, эксперты констатируют возрастание роли социальной инженерии при организации преступных схем, реализуемых в киберпространстве [4], в том числе с применением технологий искусственного интеллекта (фейковые новости, генерация дипфейков и др.) [5]. Такая тенденция обусловлена наличием определенных поведенческих паттернов, основанных на когнитивных искажениях, учитывая которые, кибермошенники добиваются своей цели с наибольшей эффективностью [6].

Паттерное поведение, являясь основой социальной инженерии как системы способов психологического манипулирования людьми в целях разглашения ими конфиденциальной информации либо совершения ожидаемых от них действий, существенно облегчает деятельность киберпреступников. Оно базируется на ряде психологических особенностей личности, которые особенно хорошо проявляются у людей, обладающих выраженным доминированием определенных черт характера [7]. Связь типичных черт характера, свойственных людям, которые подвергаются успешному воздействию кибермошенников, с видами мошеннических схем, описана в работе [8].

Постановка задачи. Совокупность психологических, социальных, поведенческих характеристик и факторов, которые повышают вероятность того, что индивид станет жертвой киберпреступления, определяется понятием личностной кибервиктимности [9]. Интерес исследователей к проблеме кибервиктимности постоянно возрастает, что подтверждается многочисленными публикациями по этой теме как в российских, так и в зарубежных источниках [10-13]. Однако, большая часть подобных исследований носит качественный характер.

В работах [14,15] на основании проведенных статистических расчетов выявлено, что склонность к кибервиктимному поведению может быть обусловлена наличием определенных психологических особенностей эмоционального и межличностного характера. Данный подход позволил связать значимость величины различий в числовых показателях, характеризующих определенные черты характера у респондентов проблемной и контрольной групп, с проявлением кибервиктимности. Но в данных работах обосновывается только наличие такой взаимосвязи без вычисления количественных показателей ее силы (степени).

Методы исследования. В работе [16] построена математическая модель определения уровня зависимости между подверженностью некоторого респондента конкретному киберпреступлению и степенью проявления его черт характера с помощью введенного числового показателя CV. Расчеты проводились на основе выявления значимых черт характера, имеющих наибольшее влияние на такую зависимость. В качестве инструмента получения необходимых статистических данных был выбран 16-факторный личностный опросник Р. Кеттелла [17, 18], позволяющий оценить величину выраженности каждой из 16-ти черт характера респондента целочисленным значением (стеном). Все, прошедшие тестирование, респонденты были разбиты на две контрольные группы - поддавшиеся действиям кибермошенников (жертвы) и сумевшие им противостоять (резистенты). Путем нахождения наибольшей вариации значений стенов по каждой из черт характера в разрезе рассматриваемых видов кибермошенничества были выявлены особенности личности,

наиболее характерные для респондентов каждой из контрольных групп. С помощью критерия Манна-Уитни [19, 20] проведена оценка различий в соответствующих выборках стенов, переведенных в ранговую шкалу, и выбраны черты характера, по которым достоверность различий максимальна. Полученные данные о чертах характера, оказывающих доминирующее влияние на склонность к подверженности наиболее распространенным видам кибермошенничества (P_1 - фишинг, P_2 - вишинг, P_3 - мошенничество в сфере онлайн-покупок), представлены в виде матрицы S_{3x16} [21]:

$$S = \begin{pmatrix} 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}. \quad (1)$$

Здесь строки соответствуют видам мошенничества, входящим в множество $P = \{P_i\}$, i = 1, 2, 3, столбцы — чертам характера C_k, k = 1, …, 16. Условие $s_{ik} = 1$ означает, что жертвам i -го кибермошенничества присуща сильная выраженность k -ой черты характера, условию $s_{ik} = -1$ соответствует ее слабая выраженность.

Матрица S описывает взаимосвязь между видами кибермошенничества и значимыми чертами характера жертв этих преступлений с качественной точки зрения. Количественные показатели такой взаимосвязи, характеризующие степень ее проявления, найдены в работе [16]. Используем эти данные, построив на основе матрицы S матричную модель, в агрегированной форме описывающую способ вычисления критериев CV по всем рассматриваемым видам кибермошенничества. Затем применим эту модель для определения комплексного показателя кибервиктимности, характеризующего общий уровень кибервиктимности произвольного респондента и вычисляемого по числовым значениям выраженности черт его характера, определенным с помощью теста Кеттела.

Построение матричной модели определения уровня кибервиктимности. Найденные в [16] значения весовых коэффициентов, характеризующих влияние значимых черт характера C_t, t = 1, …, T_i на подверженность преступлению P_i, опишем векторами $\boldsymbol{w}_i = (w_{i1}, \dots, w_{iT_i})$, i = 1, 2, 3, приведенными в формуле (2):

$$\begin{aligned} \boldsymbol{w_1} &= (0.320, 0.307, 0.374), \\ \boldsymbol{w_2} &= (0.218, 0.261, 0.274, 0.246), \\ \boldsymbol{w_3} &= (0.296, 0.344, 0.360). \end{aligned} \quad (2)$$

Матрица S визуализирует наборы наиболее характерных черт личности жертв преступлений P_i путем размещения в i-х строках ненулевых элементов на тех позициях, которые соответствуют этим чертам характера. Номера этих позиций в строке i опишем с помощью вектора $\boldsymbol{h}_i = (h_{i1}, \dots, h_{iT_i})$. Значения элементов векторов $\boldsymbol{h}_i$, i = 1, 2, 3, приведены в формуле (3):

$$\begin{aligned} \boldsymbol{h_1} &= (3, 4, 15), \\ \boldsymbol{h_2} &= (3, 9, 12, 16), \\ \boldsymbol{h_3} &= (5, 11, 15) \end{aligned} \quad (3)$$

Построим матрицу W_{3x16}, определив ее элементы W_{ik} по формуле:

$$W_{ik} = \begin{cases} w_{it}, & k = h_{it}, \\ 0, & k \neq h_{it}, \end{cases} \quad i = 1, 2, 3, \ k = 1, \dots, 16, \ t = 1, \dots, T_i. \quad (4)$$

Таким образом, матрица W получается из матрицы S заменой ненулевых элементов в i-х строках элементами w_{it} на позициях h_{it}. Аналогичным образом заменим ненулевые элементы матрицы S в каждой ее строке с номером i на позициях h_{it} значениями $\delta_t(r_t)$, описывающими степень выраженности черт характера респондента относительно его подверженности i-му кибермошенничеству и задаваемыми формулой:

$$\delta_t(r_t) = \begin{cases} f(r_t), & \Delta_t > 0, \\ g(r_t), & \Delta_t < 0, \end{cases} \quad t = 1, \dots, T_i, \quad (5)$$

где Δ_t - элемент вектора

$$\boldsymbol{\Delta} = \boldsymbol{\nu} - \boldsymbol{\rho}, \quad (6)$$

а функции f и g определяются формулами (7) и (8) соответственно:

$$f(x)=\begin{cases}0, & x<\rho_t,\\ \frac{x-\rho_t}{\nu_t-\rho_t}, & x\in[\rho_t,\nu_t],\\ 1, & x>\nu_t,\end{cases} \tag{7}$$

$$g(x)=\begin{cases}1, & x<\nu_t,\\ 1-\frac{x-\nu_t}{\rho_t-\nu_t}, & x\in[\nu_t,\rho_t],\\ 0, & x>\rho_t\end{cases} \tag{8}$$

(подробное описание формул (5)-(9) приведено в работе [16]). Транспонировав построенную таким образом матрицу, получим матрицу D_{16x3}, элементы которой D_{ki} задаются формулой:

$$D_{ki}=\begin{cases}\delta_{it}(r_{it}), & k=h_{it},\\ 0, & k\neq h_{it},\end{cases} \quad i=1,2,3,\ k=1,\dots,16,\ t=1,\dots,T_i. \tag{9}$$

Элементы векторов $\boldsymbol{r}_i=(r_{i1},\dots,r_{iT_i})$, используемые для проведения расчетов по формулам (5)-(9), равны значениям стенов по наиболее значимым чертам характера респондента, определяющим его подверженность преступлению P_i и найденным в процессе прохождения им теста Кеттела. Найдем квадратную матрицу 3-го порядка $V = W\cdot D$. Ее диагональные элементы в силу построения будут совпадать с критериями CV_i, характеризующими степень подверженности респондента преступлению P_i [16] и вычисляемыми по формуле:

$$CV_i=\sum\nolimits_{k\in\boldsymbol{h}_i} W_{ik}\cdot D_{ki}\,, \tag{10}$$

Составим из них вектор-столбец

$$\boldsymbol{CV}=\begin{pmatrix}CV_1\\ CV_2\\ CV_3\end{pmatrix}, \tag{11}$$

выделив диагональные элементы из матрицы V по формуле:

$$\boldsymbol{CV}=\sum\nolimits_{i=1}^{3} B_i\cdot V\cdot B_i\cdot U\,, \tag{12}$$

где

$$U=\begin{pmatrix}1\\ 1\\ 1\end{pmatrix}, \tag{13}$$

B_i - квадратные матрицы 3-го порядка, в которых элемент b_{ii} = 1, а все остальные элементы равны нулю.

Определение комплексного критерия кибервиктимности. В работе [21] для каждого вида кибермошенничества, принадлежащего множеству P, при проведении анкетирования были выявлены респонденты, являющиеся его жертвами, и респонденты, являющиеся его резистентами. Распределение количества респондентов-жертв и респондентов-резистентов по видам кибермошенничества приведено в [21, стр. 81, табл. 2]. Пусть общее количество респондентов в контрольной группе жертв равно N, общее количество респондентов в контрольной группе резистентов равно M, количество жертв преступления P_i равно n_i, количество резистентов преступления P_i равно m_i. Можно построить вектор $\boldsymbol{\varphi}=(\varphi_1,\varphi_2,\varphi_3)$ весовых коэффициентов, определяющих долю респондентов, подвергшихся попыткам кибермошенничества P_i, в общем количестве респондентов из контрольных групп жертв и резистентов, элементы которого задаются формулой:

$$\varphi_i=\frac{n_i+m_i}{N+M},\ \ i=1,2,3. \tag{14}$$

По построению $\varphi_i\in(0,1)$, $\sum_{i=1}^{3}\varphi_i=1$. Найденные значения элементов вектора $\boldsymbol{\varphi}$ приведены в формуле (15):

$$\boldsymbol{\varphi}=(0.349,0.358,0.292). \tag{15}$$

Используя аддитивную свертку [22, 23] критериев CV_i с весовыми коэффициентами φ_i, можно построить комплексный критерий кибервиктимности CVT, который определяется формулой:

$$CVT=\sum\nolimits_{i=1}^{3}\varphi_i\cdot CV_i\,. \tag{16}$$

Тогда обобщенная матричная модель определения комплексного критерия кибервиктимности будет иметь вид:

$$CVT = \boldsymbol{\varphi} \cdot \boldsymbol{CV} = \boldsymbol{\varphi} \cdot \sum_{i=1}^{3} B_i \cdot W \cdot D \cdot B_i \cdot U. \quad (17)$$

Обсуждение результатов. Комплексный критерий кибервиктимности характеризует общий уровень склонности к кибервиктимности произвольного респондента, то есть определяет, насколько проявление черт его характера делают его в среднем предрасположенным к тому, чтобы стать потенциальной жертвой киберпреступлений, входящих в множество *P*. Как и частные критерии CV_i, комплексный критерий *CVT* измеряется в долях единицы. Чем ближе его значение к единице, тем более уязвимым является респондент при совершении в отношении него киберпреступлений, и наоборот.

В предположении линейности изменения значений критерия *CVT* в зависимости от изменения стенов черт характера респондентов, для описания качественной характеристики степени общей кибервиктимности может быть предложена нечеткая переменная $\mu(CVT)$ с равномерными интервалами изменения значений критерия *CVT*, содержащая 5 возможных значений:

$$\mu(CVT) = \begin{cases} \text{"Кибервиктимность очень слабая"}, & CVT \leq 0.2; \\ \text{"Кибервиктимность достаточно слабая"}, & 0.2 < CVT \leq 0.4; \\ \text{"Кибервиктимность средняя"}, & 0.4 < CVT \leq 0.6; \\ \text{"Кибервиктимность достаточно сильная"}, & 0.6 < CVT \leq 0.8; \\ \text{"Кибервиктимность очень сильная"}, & CVT > 0.8. \end{cases} \quad (18)$$

Данная переменная позволяет перевести числовую характеристику степени уязвимости к кибератакам в наглядное словесное описание выявленного уровня кибервиктимности. Применим разработанную математическую модель для проведения контрольных оценок склонности к кибервиктимности. Подставим элементы векторов из формул (2) и (3) в формулу (1) с помощью формулы (4), получим матрицу *W*:

$$W = \begin{pmatrix} 0 & 0 & 0.32 & 0.307 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.374 & 0 \\ 0 & 0 & 0.218 & 0 & 0 & 0 & 0 & 0 & 0.261 & 0 & 0 & 0.274 & 0 & 0 & 0 & 0.246 \\ 0 & 0 & 0 & 0 & 0.296 & 0 & 0 & 0 & 0 & 0 & 0.344 & 0 & 0 & 0 & 0.36 & 0 \end{pmatrix}. \quad (19)$$

Расчет элементов матрицы *D* с помощью формул (5)-(9) проведем по стенам респондента, близким к средним стенам жертв рассмотренных видов кибермошенничества и использованным для моделирования в статье [16]. Они приведены в формуле (20):

$$\boldsymbol{r_1} = (3, 3, 4), \quad \boldsymbol{r_2} = (3, 4, 7, 6), \quad \boldsymbol{r_3} = (7, 3, 4). \quad (20)$$

Полученная при этом матрица *D* представлена формулой (21):

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.948 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0.947 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0.873 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0.907 \\ 0 & 0.746 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.847 & 0 & 0.796 \\ 0 & 0.599 & 0 \end{pmatrix} \quad (21)$$

Тогда матрица $V = W \cdot D$ будет иметь вид:

$$V = \begin{pmatrix} 0.926 & 0.32 & 0.298 \\ 0.207 & 0.799 & 0 \\ 0.305 & 0 & 0.879 \end{pmatrix}. \quad (22)$$

Сравнивая диагональные элементы V_{11}, V_{22}, V_{33} матрицы *V* с найденными в статье [16] значениями критериев CV_1, CV_2, CV_3, можно убедиться в их совпадении.

Используя матрицы

$$B_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \tag{23}$$

выделим диагональные элементы матрицы V по формуле (12) и подставим их в вектор-столбец $\boldsymbol{CV}$, получим:

$$\boldsymbol{CV} = \begin{pmatrix} 0.926 \\ 0.799 \\ 0.879 \end{pmatrix}. \tag{24}$$

Подставим вектор весовых коэффициентов (15) и вектор частных критериев кибервиктимности (24) в формулу (17), найдем комплексный критерий кибервиктимности респондента, рассчитанный по его стенам (20): $CVT = 0.867$. Найденное значение этого критерия в силу его близости к единице свидетельствует о высоком уровне кибервиктимности, что подтверждается значением нечеткой переменной $\mu(CVT)$:

$$\mu(0.867) = \text{«Кибервиктимность очень сильная»}. \tag{25}$$

Таким образом, исходное предположение о близости стенов респондента к стенам жертв соответствующих киберпреступлений подтверждается выводом о высокой степени его общей предрасположенности к тому, чтобы стать потенциальной жертвой кибермошенников в силу особенностей своего характера, который был получен в результате моделирования с использованием построенной матричной модели.

Выполнив аналогичным образом расчет комплексного критерия кибервиктимности для респондента, имеющего стены, характерные для резистентов соответствующих киберпреступлений

$$\boldsymbol{r_1} = (6, 7, 8), \quad \boldsymbol{r_2} = (6, 6, 3, 4), \quad \boldsymbol{r_3} = (4, 5, 6), \tag{26}$$

получим

$$\boldsymbol{CV} = \begin{pmatrix} 0.122 \\ 0.24 \\ 0.314 \end{pmatrix}, \tag{27}$$

$$CVT = 0.221, \ \ \mu(0.221) = \text{«Кибервиктимность достаточно слабая»}. \tag{28}$$

Элементы вектора $\boldsymbol{CV}$, представленного формулой (27), совпадают со значениями критериев CV_i, найденными в статье [16] для стенов респондента, совпадающих с элементами векторов (26). Полученное значение нечеткой переменной также подтверждает правильность интерпретации заданных формулой (26) стенов респондента как стенов лица, в целом устойчивого к преступным воздействиям со стороны кибермошенников.

Проведено моделирование для случаев «идеальной жертвы» и «идеального резистента», когда респондент обладает наивысшими или минимальными стенами в зависимости от того, увеличением или уменьшением стенов по соответствующим чертам характера обусловлено усиление кибервиктимности. Значение комплексного критерия кибервиктимности для «идеальной жертвы» получилось равным единице, а для «идеального резистента» - равным нулю. Данные, полученные в ходе проведенного моделирования, свидетельствуют о том, что построенная модель выдает правдоподобные результаты для входной информации, соответствующей разным уровням проявления кибервиктимности, в том числе и для экстремальных значений параметров.

Построенная математическая модель выявления склонности к кибервиктимности была положена в основу разработанного программного продукта «Анализатор уровня кибервиктимности». Данный программный продукт является инструментом, позволяющим рассчитывать комплексный показатель кибервиктимности, и может использоваться как в виде самостоятельного модуля, так и в составе комплексной системы поддержки принятия решений в процессе приема соискателей на работу, а также тестирования сотрудников.

Целью программного продукта является автоматизация процесса определения степени подверженности пользователей кибермошенничеству как в разрезе отдельных видов преступлений, так в целом. Входными данными являются стены по первичным факторам личности, полученные в ходе предварительного прохождения теста Кеттела 16PF/A [24].

В состав выходных данных входит отчет, получаемый на основе разработанной математической модели и содержащий как сведения о подверженности тестируемого конкретным видам мошенничества в процентном отношении, так и значение показателя общей склонности к тому, чтобы стать жертвой киберпреступления, представленное в числовом и качественном выражении.

К достоинствам программы следует отнести возможность получать отчетные данные по тестируемому в режиме реального времени при условии предварительного прохождения им теста Кеттела, что может способствовать оперативному выявлению степени склонности тестируемого к кибервиктимности, необходимому для принятия возможных управленческих решений. В область применения программы входит ее личное использование в целях самодиагностики, выявление потенциально ненадежных сотрудников, поддержка принятия кадровых решений. Порядок работы с программой «Анализатор уровня кибервиктимности» состоит из следующих этапов:

1. Пройти тест Кеттела и зафиксировать полученные стены по всем 16-ти исследуемым первичным факторам.
2. Внести полученные данные по стенам для каждого из первичных факторов путем выбора нужных числовых значений в выпадающих списках напротив соответствующих факторов.
3. Нажать на кнопку «Получить отчёт», чтобы вывести на экран результаты оценки уровня кибервиктимности, или на кнопку «Выгрузить отчёт», чтобы те же результаты сохранились в файле формата Word.

Вид главной формы программы «Анализатор уровня кибервиктимности» с выведенными отчетными данными, полученными по заданным значениям стенов для первичных факторов, приведен на рис. 1.

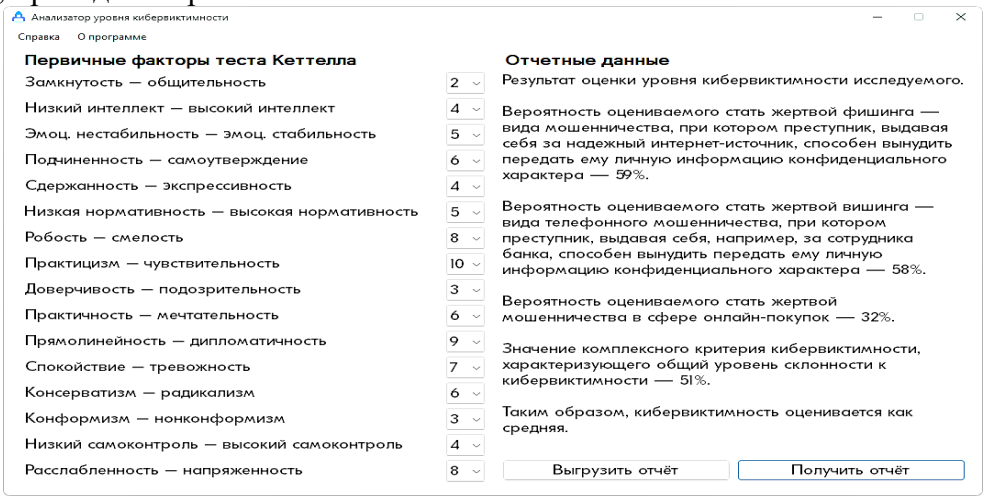

Рис. 1 - Интерфейс программы «Анализатор уровня кибервиктимности»
Fig. 1 - Interface of the Cyber Victimization Level Analyzer program

Для программы «Анализатор уровня кибервиктимности» получено свидетельство о государственной регистрации [25].

Вывод. Представление математической модели определения уровня кибервиктимности в матричном виде позволяет не только придать ей наглядную компактную форму, но и упростить ее компьютерную реализацию. Важным практическим аспектом ее использования является удобство ее масштабирования путем расширения видов рассматриваемых киберпреступлений. Полное совпадение результатов проведенного тестового моделирования с результатами тестирования на тех же исходных данных математической модели, оформленной без применения матричных структур, свидетельствует о корректности ее перевода в матричную форму записи.

К числу возможных направлений развития представленной модели и модернизации программы «Анализатор уровня кибервиктимности» можно отнести:

- наращивание статистической базы числовых показателей личностных характеристик представителей контрольных групп жертв и резистентов киберпреступлений;
- самообучение системы за счет учета в системе числовых показателей каждого нового тестируемого;
- построение матриц весовых коэффициентов для описания взаимосвязи уровня проявления черт характера с видами киберпреступлений в разрезе различных показателей (гендерный признак, возрастные группы, группы профессий и т.д.);
- внедрение дополнительных опций - возможность прохождения теста Кеттела в самой программе, формирование разнообразных отчетов, изменение интерфейса для разных категорий пользователей (кадровик, руководитель, сотрудник службы безопасности).

Библиографический список:

1. Состояние преступности в России за январь-июнь 2025 года. М.: ФКУ «ГИАЦ» МВД РФ. URL: https://media.mvd.ru/files/application/13467874 (дата обращения: 05.08.2025).
2. Попкова А.А., Парфенов К.В, Алборов А.Р. Угрозы информационной безопасности в государственном секторе России // Известия вузов. Социология. Экономика. Политика. 2024. № 4. С. 77-93. URL: http://www.sep-tyuiu.ru/ru/journal-item/80 (дата обращения: 05.08.2025).
3. Нурмаммедов А. Я., Дурдыев С. А., Хыдыров М. Г. Растущие угрозы кибератак на критическую инфраструктуру: вызовы и инновации // Вестник науки. 2024. № 5 (74). С. 1485-1487. URL: https://cyberleninka.ru/article/n/rastuschie-ugrozy-kiberatak-na-kriticheskuyu-infrastrukturu-vyzovy-i-innovatsii (дата обращения: 05.08.2025).
4. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. 2021. № 1 (42). С. 133-138. URL: https://sciup.org/socialnaja-inzhenerija-kak-sposob-sovershenija-kiberprestuplenij-140256700 (дата обращения: 05.08.2025).
5. URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (дата обращения: 05.08.2025). Информационная безопасность (тренды).
6. URL: https://press.psu.ru/index.php/philsoc/article/view/9671 (дата обращения: 05.08.2025). Игнатова Е.С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study // Вестник Пермского университета. Философия. Психология. Социология. 2024. № 3. С. 374-390.
7. URL:https://gpa.cfuv.ru/attachments/article/4051/Выпуск%2064%20часть%204,%202019%20год.pdf (дата обращения: 05.08.2025). Братусин А.Р., Власенко Е.Е. О характерных индивидуально-типологических особенностях и поведенческих паттернах личности типичных жертв финансового мошенничества // Проблемы современного педагогического образования. Сборник научных трудов / Ялта: РИО ГПА, 2019. Вып. 64. Ч. 4. С. 292-294.
8. Карпасюк И.В., Карпасюк А.И. Мошенничество в ИБ-сфере и психология жертвы: особенности и взаимосвязи // Защита информации. Инсайд. 2022. № 3(105). С. 41-49. URL: http://www.inside-zi.ru/pages/3_2022/41.html (дата обращения: 05.08.2025).
9. Жмуров Д.В. Личностная и корпоративная кибервиктимность // Виктимология. 2025. Т.12. № 2. С. 202-210. URL: https://www.victimolog.ru/index.php/victimo/article/view/692 (дата обращения: 05.08.2025).
10. URL: https://psyjournals.ru/journals/psylaw/archive/2023_n1/7 (дата обращения: 05.08.2025). Вихман А.А. Личностные предикторы кибервиктимности и кибербуллинга в юношеском возрасте // Психология и право. 2023. Т. 13. № 1. С. 94–106.
11. https://cyberleninka.ru/article/n/kiberviktimnost-kak-novaya-kategoriya-viktimologii-postmoderna (дата обращения: 05.08.2025). Жмуров Д.В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. №. 2. С. 113–122.
12. Griffith C., Tetzlaff-Bemiller M., Hunter L. Understanding the cyber-victimization of young people: A test of routine activities theory. Telematics and Informatics Reports. 2023;9. URL: https://www.sciencedirect.com/science/article/pii/S2772503023000026 (дата обращения: 05.08.2025).
13. Aparisi D., Delgado B., Bo R.M. Explanatory model of cyberbullying, cybervictimization, aggressiveness, social anxiety, and adaptation to university: a structural equation analysis // J. Comput. Educ. 2025. Vol 12. Pp. 217-238. https://link.springer.com/article/10.1007/s40692-023-00308-5 (дата обращения: 05.08.2025).
14. URL: https://psyjournals.ru/journals/psylaw/archive/2015_n4/Safuanov_Dokuchaeva (дата обращения: 05.08.2025).Сафуанов Ф.С., Докучаева Н.В. Особенности личности жертв противоправных посягательств в Интернете // Психология и право. 2015. Т. 5. № 4. С. 80-93.
15. URL: https://psyjournals.ru/journals/psylaw/archive/2022_n2/Vlasova_Buslaeva (дата обращения: 05.08.2025). Власова Н.В., Буслаева Е.Л. Психологические особенности лиц, склонных к кибервиктимному поведению // Психология и право. 2022. Т. 12. № 2. С. 194-206.

16. Карпасюк И.В., Карпасюк А.И. Математическая модель определения степени склонности к подверженности киберпреступлению // Вестник Дагестанского государственного технического университета. Технические науки. 2025. Т.52. №1. С.87-96. URL: https://vestnik.dgtu.ru/jour/article/view/1702 (дата обращения: 05.08.2025).
17. Истратова О.Н., Эксакусто Т. В. Психодиагностика: коллекция лучших тестов. – Ростов-на-Дону: Феникс, 2006. – 375 с.
18. Капустина А.Н. Многофакторная личностная методика Р. Кеттелла. – СПб.: Речь, 2007. – 104 с.
19. Сидоренко Е.В. Методы математической обработки в психологии. – СПб: Речь, 2010. – 350 с.
20. https://astu.org/Uploads/files/izdatelstvo/Наука%20и%20практика%202023%20%20Техн%20науки(1).pdf (дата обращения: 05.08.2025) Карпасюк И.В. Оценка применимости методов математической статистики для определения уровня выраженности черт характера в задаче выявления склонности к кибервиктимности // Наука и практика – 2023. Всероссийская междисциплинарная научная конференция, Астрахань, 13-17 ноября 2023 г. [Электронный ресурс]: материалы / Астрахан. гос. техн. ун-т. –Астрахань: Изд-во АГТУ, 2024. С. 427-429.
21. Карпасюк И.В., Карпасюк А.И., Давидюк Н.В., Чертина Е.В. Формализация процедуры выявления личностных характеристик потенциальной жертвы кибермошенничества // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 2. С. 77-84. URL: https://vestnik.astu.org/ru/nauka/article/82549/view (дата обращения: 05.08.2025).
22. Штойер Р. Многокритериальная оптимизация. – М.: Радио и связь, 1992. – 504 с.
23. Черноруцкий И.Г. Методы оптимизации и принятия решений. – СПб.: Лань, 2001. – 384 с.
24. Тест Кеттелла, 16PF. URL: https://psytests.org/multi/cat16pfA.html (дата обращения: 05.08.2025).
25. Свидетельство о государственной регистрации программы для ЭВМ 2024614787 Российская Федерация. Анализатор уровня кибервиктимности: N 2024612910: заявл. 15.02.24; опубл. 28.02.24 / А.И. Карпасюк, Н.В. Давидюк; заявитель и правообладатель Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный технический университет» ФГБОУ ВО «АГТУ» – 1 с.

References:

1. The State of Crime in Russia in January-August 2024. FSI «MIAC», Ministry of Internal Affairs, Russia. (In Russ) URL: https://media.mvd.ru/files/application/7206717 (accessed 05.08.2025).
2. Popkova A.A., Parfenov K.V., Alborov A.R. Threats to Information Security in the Russian Public Sector. *Proceedings of Higher Educational Institutions. Sociology. Economy. Politics*. 2024; 4: 77-93. (In Russ) URL: http://www.sep-tyuiu.ru/ru/journal-item/80 (accessed 05.08.2025).
3. Nurmammedov A.Ya., Durdyev S.A., Khydyrov M.G. Growing Threats of Cyber Attacks on Critical Infrastructure: Challenges and Innovations. *Herald of Science*. 2024; 5(74): 1485-1487. (In Russ) URL: https://cyberleninka.ru/article/n/rastuschie-ugrozy-kiberatak-na-kriticheskuyu-infrastrukturu-vyzovy-i-innovatsii (accessed 05.08.2025).
4. Yangaeva M.O. Social Engineering as a Way of Committing Cyber Crimes. *Vestnik of Siberian Law Institute of the MIA of Russia*. 2021; 1(42): 133-138. (In Russ) URL: https://sciup.org/socialnaja-inzhenerija-kak-sposob-sovershenija-kiberprestuplenij-140256700 (accessed 05.08.2025).
5. URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (accessed 05.08.2025). Information Security (trends). (In Russ)
6. Ignatova E.S. Manipulation of Emotional Security by Cybercriminals Using Social Engineering Technologies: a Case Study. *Perm University Herald. Philosophy. Psychology. Sociology*, 2024; 3: 374-390. (In Russ) URL: https://press.psu.ru/index.php/philsoc/article/view/9671 (accessed 05.08.2025).
7. URL:https://gpa.cfuv.ru/attachments/article/4051/Выпуск%2064%20часть%204,%202019%20год.pdf (accessed 05.08.2025). Bratusin A.R., Vlasenko E.E. On the Characteristic Individual Typological Features and Behavioral Patterns of the Personality of Typical Victims of Financial Fraud. *Problems of Modern Pedagogical Education*. 2019; 64(4): 292-294. (In Russ)
8. Karpasyuk I.V., Karpasyuk A.I. Information Security Fraud and Victim Psychology: Features and Relationships. *Zaŝita informacii. Inside*. 2022; 3(105): 41-49. (In Russ.) URL: http://www.inside-zi.ru/pages/3_2022/41.html (accessed 05.08.2025).
9. Zhmurov D. V. Personal and Corporate Cybervictimization. *Victimology*. 2025; 12(2): 202–210. (In Russ) URL: https://www.victimolog.ru/index.php/victimo/article/view/692 (accessed 05.08.2025).
10. URL: https://psyjournals.ru/journals/psylaw/archive/2023_n1/7 (accessed 05.08.2025). Vikhman A.A. Personality Predictors of Cyber-Victimization and Cyber-Bullying in Adolescence. *Psychology and Law*. 2023; 13(1): 94–106. (In Russ)
11. Zhmurov D. V. Cyber-victimhood as a new category of postmodern victimology. *PACIFIC RIM: Economics, Politics, Law*. 2021; 2: 113–122. (In Russ) URL: https://cyberleninka.ru/article/n/kiberviktimnost-kak-novaya-kategoriya-viktimologii-postmoderna (accessed 05.08.2025).

12. Griffith C., Tetzlaff-Bemiller M., Hunter L. Understanding the Cyber-Victimization of Young People: A Test of Routine Activities Theory. *Telematics and Informatics Reports*. 2023; 9. URL: https://www.sciencedirect.com/science/article/pii/S2772503023000026 (accessed 05.08.2025).
13. Aparisi D., Delgado B., Bo R.M. Explanatory Model of Cyberbullying, Cybervictimization, Aggressiveness, Social Anxiety, and Adaptation to University: A Structural Equation Analysis. *J. Comput. Educ*. 2025;12:217-238. https://link.springer.com/article/10.1007/s40692-023-00308-5 (accessed 05.08.2025).
14. https://psyjournals.ru/journals/psylaw/archive/2015_n4/Safuanov_Dokuchaeva (accessed 05.08.2025). Safuanov F.S., Dokuchaeva N.V. Personality Characteristics of Victims of Illegal Attacks on the Internet. *Psychology and Law*. 2015; 5(4): 80-93. (In Russ)
15. URL: https://psyjournals.ru/journals/psylaw/archive/2022_n2/Vlasova_Buslaeva (accessed 05.08.2025). Vlasova N.V., Buslaeva E.L. Psychological Features of Individuals Prone to Cyber Victimization. *Psychology and Law*. 2022; 12(2): 194-206. (In Russ)
16. Karpasyuk I.V., Karpasyuk A.I. Mathematical Model for Determining the Degree of Propensity to Be Exposed to Cybercrime. *Herald of Daghestan State Technical University. Technical Sciences*. 2025; 52(1): 87-96. (In Russ). URL: https://vestnik.dgtu.ru/jour/article/view/1702 (accessed 05.08.2025).
17. Istratova O.N., Exacusto T.V. Psychodiagnostics: A Collection of the Best Tests. Rostov-Na-Donu: Phoenix, 2006; 375. (In Russ.)
18. Kapustina A.N. Multifactorial Personality Methodology of R.Cattell. SPb: Language, 2007; 104. (In Russ)
19. Sidorenko E.V. Methods of Mathematical Processing in Psychology. SPb: Language, 2010; 350. (In Russ)
20. https://astu.org/Uploads/files/izdatelstvo/Наука%20и%20практика%202023%20%20Техн%20науки(1).pdf (accessed 05.08.2025).Karpasyuk I.V. Assessing the Applicability of Mathematical Statistics Methods for Determining the Degree of Manifestation of Character Traits in the Task of Identifying Susceptibility to Cybervictimization. / Science and Practice – 2023. All-Russian Interdisciplinary Scientific Conference. Astrakhan, November 13-17. Electronic Materials. Astrakhan State Technical University. Astrakhan: ASTU, 2024; 427-429. (In Russ).
21. Karpasyuk I.V., Karpasyuk A.I., Davidyuk N.V., Chertina E.V. Formalising the Procedure for Identifying the Personality Characteristics of a Potential Cyber Fraud Victim. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2024; 2: 77-84. (In Russ). URL: https://vestnik.astu.org/ru/nauka/article/82549/view (accessed 05.08.2025).
22. Shtoyer R. Multicriterial Optimization. M.: Radio and Telecommunications, 1992; 504. (In Russ)
23. Chernorutskiy I.G. Optimization and Decision Making Methods. SPb: Lan, 2001; 384. (In Russ)
24. Cattell Test, 16PF. URL: https://psytests.org/multi/cat16pfA.html (accessed 05.08.2025). (In Russ)
25. Certificate of State Registration of Computer Program 2024614787, Russian Federation. Cybervictimization Level Analyzer: Registration No. 2024612910; filed 15.02.2024; publ. 28.02.24 / A.I. Karpasyuk, N.V. Davidyuk; Applicant and Rights Holder: Federal State Budget Educational Institution of Higher Education "Astrakhan State Technical University" FSBEI HE «ASTU». (In Russ)

Сведения об авторах:

Карпасюк Игорь Владимирович, кандидат физико-математических наук, доцент, доцент, кафедравысшей и прикладной математики; ikarpasyuk@mail.ru

Карпасюк Александр Игоревич, магистрант, кафедра высшей и прикладной математики; akarpasyuk@mail.ru

Information about authors:

Igor V. Karpasyuk, Cand. Sci. (Physics and Mathematics), Assoc. Prof., Assoc. Prof., Department of Higherand Applied Mathematics; ikarpasyuk@mail.ru

Alexander I. Karpasyuk, Master's Student, Department of Higher and Applied Mathematics; akarpasyuk@mail.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 07.09.2025.

Одобрена после рецензирования/Reviced 29.10.2025.

Принята в печать/Accepted for publication 26.12.2025.