ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК [343.98:004.056] + 159.923 + 519.25
DOI: 10.21822/2073-6185-2025-52-1-87-96

Оригинальная статья/ Original article

Математическая модель определения степени склонности к подверженности киберпреступлению

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

Резюме. **Цель.** Целью исследования является построение математической модели определения взаимосвязи кибервиктимности с чертами характера, присущими жертвам кибермошенничества. Описаны особенности современного кибермошенничества, базирующегося в первую очередь на психологических аспектах влияния на жертву. **Метод.** Исследование основано на статистических методах, связанных с определением взаимосвязи степени подверженности киберпреступлениям с уровнем проявления черт характера жертв, выявленных в виде соответствующих количественных характеристик по тесту Кеттела. **Результат.** Продемонстрирован способ определения коэффициентов, задающих относительные веса для степени проявления этих факторов в задаче выявления подверженности определенному киберпреступлению. Предложена математическая модель, которая позволяет оценить уровень кибервиктимности некоторого респондента по отношению к конкретному киберпреступлению в зависимости от величины числовых значений, описывающих его личностные характеристики, подвергаемые изучению с помощью теста Кеттела. В рамках данной модели вводится числовой показатель, определяющий критерий степени подверженности респондента рассматриваемому киберпреступлению. Проведены расчеты уровня кибервиктимности в разрезе таких видов кибермошенничества, как фишинг, вишинг, мошенничество в сфере онлайн-покупок, для респондентов, которых можно отнести к жертве и к резистенту соответствующих киберпреступлений по совокупности личностных характеристик. **Вывод.** По результатам проведенных расчетов продемонстрировано соответствие полученных числовых характеристик, описывающих уровень кибервиктимности респондента, его качественной принадлежности к числу жертв или резистентов по каждому из видов кибермошенничества.

Ключевые слова: кибермошенничество, кибервиктимность, фишинг, вишинг, стены, тест Кеттелла, черты характера, жертва, степень подверженности киберпреступлению

Для цитирования: И.В. Карпасюк, А.И. Карпасюк. Математическая модель определения степени склонности к подверженности киберпреступлению. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(1):87-96. DOI:10.21822/2073-6185-2025-52-1-87-96

Mathematical Model for Determining the Degree of Propensity to Be Exposed to Cybercrime

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 develop a mathematical model for determining the relationship between cyber victimhood and the character traits inherent in victims of cyber fraud. The article describes the features of cyber fraud based on the psychological aspects of influence on the victim. **Method.** The study is based on statistical methods related to determining the relationship between the degree of susceptibility to cyber crimes and the level of

manifestation of the character traits of victims identified in the form of corresponding quantitative characteristics according to the Cattell test. **Result.** A method is proposed for determining the coefficients that set the relative weights for the degree of manifestation of factors in the task of identifying susceptibility to a particular cyber crime. A mathematical model is proposed for assessing the level of cyber victimhood of a respondent in relation to a specific cyber crime depending on the magnitude of numerical values describing the personal characteristics studied using the Cattell test. The model introduces a numerical indicator that determines the criterion for the degree of susceptibility of the respondent to the cyber crime in question. Based on statistical data, the level of cyber victimization was calculated in terms of types of cyber fraud, such as phishing, vishing, online shopping fraud, for respondents who can be classified as victims and resistors of the relevant cyber crimes based on a set of personal characteristics. **Conclusion.** The correspondence of the obtained numerical characteristics describing the level of cyber victimization of the respondent, his qualitative belonging to the number of victims or resistors for each type of cyber fraud was demonstrated.

Keywords: cyber fraud, cybervictimization, phishing, vishing, stens, Kettell test, character traits, victim, degree of exposure to cybercrime.

For citation: I.V. Karpasyuk, A.I. Karpasyuk. 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). DOI:10.21822/2073-6185-2025-52-1-87-96

Введение. В настоящее время наблюдается значительный рост количества киберугроз [1, 2]. В 2024 году количество преступлений, совершенных в РФ с использованием информационно-телекоммуникационных технологий, увеличилось на 16,4% по сравнению с 2023 годом, их удельный вес в общем числе зарегистрированных преступлений составил 39,2% [3]. Большая часть таких преступлений совершается путем мошенничества. В современной России мошенничество — одно из самых часто совершаемых преступлений, а среди видов мошенничества лидирующие позиции занимают телефонное и Интернет-мошенничество. При этом раскрываемость таких преступлений составляет не более 23% [4]. Киберпреступность носит интеллектуально-информационный характер, используя как техническую, так и социально-психологическую составляющие актов правонарушений в виртуальной среде. Взаимодействие сторон киберпреступления - правонарушителя и жертвы - может проявляться в разных видах и характеризоваться как наличием двух одушевленных оппонентов, так и воздействием на жертву достаточно автономного вредоносного программного продукта [5].

Наиболее распространенными, постоянно видоизменяющимися и совершенствующимися формами психологического воздействия на сознание и поведение людей в рамках явления киберпреступности являются многочисленные схемы кибермошенничества, успех применения которых зависит от различных способов маскировки вредоносных воздействий. Практически беспроигрышной стратегией воздействия на сознание и волю человека является формирование условий и обстоятельств, приводящих к погружению жертвы в информационно-психологическое пространство, способствующее принятию с ее стороны определенных решений, которые максимально эффективно приведут к конкретному результату, необходимому преступнику. Совокупность приемов, методов и технологий создания такого пространства описывается понятием «социальная инженерия» [6-8].

Все техники информационно-психологического воздействия на жертву с целью вынуждения совершения определенных действий основаны на когнитивных искажениях [9]. Искаженное видение объективной реальности способствует снижению внимательности и адекватного восприятия истинных мотивов киберпреступников. Именно этими психологическими особенностями жертвы пользуются мошенники, применяя обман как информационное, интеллектуальное воздействие одного человека на сознание и волю

другого [10]. Практически во всех типах мошеннических схем, реализуемых в киберпространстве, задействованы психологические приемы и методы, что значительно увеличивает эффективность этих схем. Различные способы использования социальной инженерии при проведении кибератак укладываются в единый шаблон, который описывается схемой Шейнова [6, 10, 11]. В рамках данной схемы, на этапах сбора информации о жертве и обнаружения ее уязвимостей основной задачей мошенников при подготовке киберпреступления является исследование психофизических и личностных характеристик объекта воздействия с целью выбора наиболее подходящего способа такого воздействия, который может привести к поставленной цели с максимальными шансами на успех и минимальными рисками и затратами.

Существует множество исследований, посвященных изучению характеристик личности кибержертв (субъектов, подверженных воздействию киберпреступников) и феномена кибервиктимности (склонности к подобным воздействиям) [12-16]. Установлено, что жертвы киберпреступлений характеризуются выраженностью определенных черт характера [17, 18]. Для жертв разных видов киберпреступлений набор подобных черт характера может отличаться [19]. Однако, большинство работ связано с выявлением качественной взаимосвязи личностных характеристик жертв с их подверженностью определенным видам киберпреступлений. В работах [20, 21] проведена количественная оценка различий в уровнях проявления черт характера жертв кибермошенничества и лиц, сумевших противостоять преступному воздействию (резистентов), и выявлены наборы черт характера с наибольшей асимптотической значимостью таких различий, определяющих личностный профиль жертв, в том числе в разрезе различных видов кибермошенничества. Расчеты проводились на основе статистических данных, содержащих целочисленные значения (так называемые стены), описывающие по десятибалльной шкале степени выраженности черт характера (первичных факторов) жертв и резистентов, которые были получены в рамках тестирования респондентов с помощью теста Кеттела [22, 23].

Постановка задачи. В работе [21] построена матрица S, описывающая взаимосвязь между 16-ю чертами характера и рассмотренными видами кибермошенничества: P_1 - фишинг, P_2 - вишинг, P_3 - мошенничество в сфере онлайн-покупок. Матрица S демонстрирует, какие типичные черты характера свойственны людям, наиболее подверженным воздействию указанных кибератак. Однако, она показывает только качественную картину подобных взаимосвязей. Определим количественные характеристики параметров, описывающих влияние соответствующих первичных факторов на степень склонности к тому, чтобы стать жертвой того или иного киберпреступления.

Методы исследования. Построение математической модели зависимости уровня кибервиктимности от степени проявления черт характера жертвы проведем на примере некоторого вида кибермошенничества P^*.

Определение весовых коэффициентов для значимых черт характера. Пусть кибермошенничеству P^* соответствует множество черт характера C_t, $t = 1, \dots, T$, оказывающих преобладающее воздействие на склонность к подверженности данному кибермошенничеству, полученное после редукции числа первичных факторов теста Кеттела и выделения наиболее значимых из них (см. [21]). Для разных видов кибермошенничества значения T могут быть различны.

Составим вектор $\boldsymbol{\nu} = (\nu_1, \dots, \nu_T)$, элементы которого ν_t равны средним значениям стенов жертв преступления P^* по черте характера C_t. Аналогичный вектор $\boldsymbol{\rho} = (\rho_1, \dots, \rho_T)$ составим из средних значений ρ_t стенов резистентов преступления P^* по тем же чертам характера C_t. По построению, значения элементов векторов $\boldsymbol{\nu}$ и $\boldsymbol{\rho}$ принадлежат отрезку [1, 10]. Найдем вектор $\boldsymbol{\Delta} = (\Delta_1, \dots, \Delta_T)$ по формуле

$$\Delta = \nu - \rho. \qquad (1)$$

Большему абсолютному значению элемента Δ_t данного вектора будет соответствовать большее влияние черты характера C_t на склонность к подверженности преступлению

P^*. Знак элемента Δ_t показывает характер такого влияния: отрицательное значение Δ_t означает, что на усиление подверженности преступлению P^* влияет уменьшение значений стенов, описывающих черту характера C_t, тогда как положительное значение Δ_t свидетельствует об усилении подверженности преступлению P^* при увеличении значений этих стенов. Следует отметить, что элементы Δ_t не могут быть нулевыми в силу того, что чертам характера C_t соответствуют наиболее значимые различия соответствующих стенов жертв и резистентов. Степень доминирования одних черт характера над другими при определении их влияния на подверженность преступлению P^* опишем с помощью весовых коэффициентов w_t:

$$w_t = \frac{|\Delta_t|}{\sum_{j=1}^{T}|\Delta_j|}, \ \ t = 1, \dots, T. \tag{2}$$

По построению $\sum_{t=1}^{T} w_t = 1$. Таким образом, нормированные показатели w_t принимают значения на интервале (0, 1) (при $T > 1$) и описывают относительные веса влияния черт характера C_t на подверженность киберпреступлению P^*.

Построение математической модели определения степени подверженности киберпреступлению. Найденные весовые коэффициенты w_t можно применить для определения степени угрозы стать жертвой киберпреступления P^* для любого респондента, прошедшего анкетирование по 16-факторному личностному опроснику Кеттела и имеющего значения стенов для всех факторов. При этом в расчет будут браться только значения стенов по чертам характера C_t, $t = 1, \dots, T$, соответствующим данному преступлению P^*.

Пусть известен набор целочисленных значений стенов для каждой из 16-ти черт характера некоторого произвольного респондента Θ, определенных с помощью теста Кеттела и принадлежащих отрезку [1, 10]. Из данного набора выберем стены, соответствующие чертам характера C_t для преступления P^*, и составим из них вектор $\boldsymbol{r} = (r_1, \dots, r_T)$. Степень выраженности черты характера C_t респондента Θ относительно склонности к тому, чтобы стать жертвой киберпреступления P^*, обозначим δ_t. Будем считать, что $\delta_t \in [0, 1]$, и значению $r_t = \rho_t$, описывающему характерные значения стенов резистентов, соответствует минимальное значение $\delta_t = 0$, а значению $r_t = \nu_t$, описывающему характерные значения стенов жертв, соответствует максимальное значение $\delta_t = 1$. Зависимость δ_t от r_t будем предполагать линейной.

Примем во внимание, что если для черты характера C_t величина $\Delta_t > 0$ (что соответствует случаю $\nu_t > \rho_t$), а для соответствующего стена r_t респондента Θ выполняется условие $r_t < \rho_t$, то черта характера C_t никак не влияет на подверженность респондента Θ преступлению P^*, и наоборот, при выполнении условия $r_t > \nu_t$ влияние черты характера C_t респондента Θ на подверженность этому преступлению не вызывает сомнений.

Аналогично, если величина $\Delta_t < 0$ ($\nu_t < \rho_t$) и $r_t > \rho_t$, то влияние черты характера C_t на преступление P^* у респондента Θ не проявляется, а если $r_t < \nu_t$, то такое влияние бесспорно.

Построим функции, позволяющие определять значение показателя δ_t по значению r_t в соответствии с приведенным выше описанием.

Случай $\Delta_t > 0$ означает, что при увеличении значений стенов $r_t \in [\rho_t, \nu_t]$ кибервиктимность по преступлению P^* будет линейно возрастать от 0 до 1, для значений $r_t < \rho_t$ величина показателя δ_t будет равна нулю, а для значений $r_t > \nu_t$ показатель $\delta_t = 1$. Найдем уравнение прямой $y(x)$, проходящей через точки $(\rho_t, 0)$ и $(\nu_t, 1)$:

$$y = \frac{x - \rho_t}{\nu_t - \rho_t}. \tag{3}$$

Тогда функция $f(x)$, описывающая изменения показателя δ_t в случае, когда $\Delta_t > 0$, с учетом формулы (3) будет иметь вид:

$$f(x) = \begin{cases} 0, & x < \rho_t, \\ \dfrac{x - \rho_t}{\nu_t - \rho_t}, & x \in [\rho_t, \nu_t], \\ 1, & x > \nu_t. \end{cases} \quad (4)$$

Проведем аналогичные построения для случая $\Delta_t < 0$, когда с увеличением значений стенов r_t на отрезке $[\nu_t, \rho_t]$ значения δ_t будут линейно уменьшаться от 1 до 0, для значений $r_t < \nu_t$ величина показателя δ_t будет равна 1, а для значений $r_t > \rho_t$ значения δ_t будут равны нулю. Тогда уравнение соответствующей линейной функции примет вид:

$$y = 1 - \frac{x - \nu_t}{\rho_t - \nu_t}. \quad (5)$$

Используя формулу (5), построим функцию $g(x)$, описывающую изменения показателя δ_t в случае, когда $\Delta_t < 0$:

$$g(x) = \begin{cases} 1, & x < \nu_t, \\ 1 - \dfrac{x - \nu_t}{\rho_t - \nu_t}, & x \in [\nu_t, \rho_t], \\ 0, & x > \rho_t. \end{cases} \quad (6)$$

Кусочно-линейные функции $f(x)$ и $g(x)$ позволяют вычислить уровень подверженности некоторого респондента Θ киберпреступлению P^* по значениям стенов этого респондента в зависимости от того, увеличением или уменьшением значений стенов характеризуется подобная подверженность, что определяется знаком соответствующих элементов вектора **Δ**. Тогда формула, описывающая зависимость относительных значений такой выраженности δ_t от значений стенов r_t для соответствующих черт характера C_t произвольного респондента Θ, имеет вид:

$$\delta_t(r_t) = \begin{cases} f(r_t), & \Delta_t > 0, \\ g(r_t), & \Delta_t < 0, \end{cases} \quad t = 1, \dots, T, \quad (7)$$

где Δ_t — элемент вектора Δ, задаваемого формулой (1), а функции f и g определяются формулами (4) и (6) соответственно.

Для удобства восприятия и в целях представления входных и выходных данных в одних единицах измерения, масштабируем значения $\delta_t \in [0, 1]$ так, чтобы они принимали целые значения на отрезке [1, 10]. Воспользуемся известной формулой для перехода от величины $x \in [\alpha, \beta]$ к пропорциональной ей величине $y \in [a, b]$:

$$y = a + (b - a) \cdot \frac{x - \alpha}{\beta - \alpha}. \quad (8)$$

В нашем случае $\alpha = 0,\ \beta = 1,\ a = 1,\ b = 10$, отсюда

$$\delta_t^* = [1 + 9\delta_t], \qquad t = 1, \dots, T, \quad (9)$$

где функция $[x]$ округляет элемент *x* до ближайшего целого числа по правилам математического округления. Таким образом, вектор $\boldsymbol{\delta}^* = (\delta_1^*, \dots, \delta_T^*)$ будет представлять собой аналог набора стенов теста Кеттела, описывающих степень проявления черт характера числами от 1 до 10, но предназначенный для характеристики степени влияния черт характера C_t респондента Θ на его подверженность преступлению P^*. При этом так же, как и в тесте Кеттела, значение $\delta_t^* = 1$ означает минимальный уровень влияния, значение $\delta_t^* = 10$ — максимальный уровень влияния. Расчет показателя (критерия) CV степени подверженности респондента Θ преступлению P^* проведем с помощью аддитивной свертки [24] по формуле

$$CV = \sum_{t=1}^{T} w_t \cdot \delta_t, \quad (10)$$

представляющей собой скалярное произведение векторов $\boldsymbol{w} = (w_1, \dots, w_T)$ и $\boldsymbol{\delta} = (\delta_1, \dots, \delta_T)$, элементы которых вычисляют по формулам (2) и (7) соответственно. Критерий CV принимает значения на отрезке [0, 1].

Если $CV = 0$, то это означает отсутствие основания для признания респондента Θ потенциальной жертвой киберпреступления P^*. Если же $CV = 1$, то респондента Θ с уверенностью можно отнести к числу потенциальных кибержертв преступления P^*.

Обсуждение результатов. Применим разработанную математическую модель для расчета весовых коэффициентов черт характера и проведения с их помощью оценок склонности к кибервиктимности для разных видов киберпреступлений.

В соответствии с данными, приведенными в работе [21], на склонность к тому, чтобы стать жертвой кибермошенничества P_1 (фишинга), указывают низкие значения стенов для черт характера C_3 (эмоциональная стабильность), C_4 (уровень доминантности) и C_{15} (самоконтроль), то есть количество значимых признаков в этом случае $T = 3$.

Векторы $\boldsymbol{\nu}$ и $\boldsymbol{\rho}$, элементами которых являются средние стены жертв и резистентов преступления P_1 соответственно, вычисленные по полученным исходным данным анкетирования респондентов для черт характера C_3, C_4, C_{15}, имеют вид: $\boldsymbol{\nu} = (2.784, 3.576, 3.261)$, $\boldsymbol{\rho} = (6.928, 7.552, 8.103)$. Тогда вектор $\boldsymbol{\Delta}$, вычисленный по формуле (1), имеет координаты $\boldsymbol{\Delta} = (-4.144, -3.976, -4.842)$. Вычислим весовые коэффициенты по формуле (2), получим: $\boldsymbol{w} = (0.320, 0.307, 0.374)$. В данном случае, для всех элементов вектора $\boldsymbol{\Delta}$ выполняется условие

$$\Delta_t < 0, \quad t = 1, \dots, T. \tag{11}$$

Проведем демонстрацию процесса моделирования по построенной модели выявления склонности к подверженности киберпреступлению на примере гипотетических значений стенов по показателям теста Кеттела для абстрактного респондента Θ, которые будут близки к средним значениям стенов жертв по каждому из рассматриваемых видов кибермошенничества, то есть личностные характеристики этого респондента должны свидетельствовать о том, что он является скорее жертвой, чем резистентом.

Пусть для респондента Θ вектор $\boldsymbol{r}$ значений стенов для черт характера C_3, C_4, C_{15}, определяющих возможную склонность к фишингу P_1, имеет вид $\boldsymbol{r} = (3, 3, 4)$. В силу условия (11), значения параметров δ_t, вычисляемые по формуле (7) и характеризующие степень влияния черт характера респондента Θ на его подверженность данному преступлению, будут представлять собой значения функции $g(x)$, описываемой формулой (6). Найдя эти значения, получим вектор $\boldsymbol{\delta} = (0.948, 1, 0.847)$. Тогда вектор $\boldsymbol{\delta}^* = (10, 10, 9)$, его элементы найдены по формуле (9). Таким образом, степень влияния черт характера респондента Θ на подверженность фишингу очень высоки. Далее найдем величину критерия CV_1 степени подверженности респондента Θ фишингу P_1 по формуле (10), получим: $CV_1 = 0.926$. Аналогичные расчеты проведем для остальных рассмотренных в работе [21] видов кибермошенничества — P_2 (вишинг) и P_3 (мошенничество в сфере онлайн-покупок), результаты представим в виде таблиц 1 и 2 соответственно.

Таблица 1. Вычисление критерия CV_2 для вишинга
Table 1. Calculating the CV_2 criterion for vishing

Исходные данные для преступления P_2 (вишинг) Initial data for the crime
$T = 4$: C_3, C_9, C_{12}, C_{16} $\nu = (3.046, 3.350, 8.362, 7.935)$ $\rho = (7.329, 8.474, 2.991, 3.108)$
Вычисление весовых коэффициентов *w* Calculation of weighting coefficients
$\Delta = (-4.283, -5.124, 5.371, 4.827)$ $w = (0.218, 0.261, 0.274, 0.246)$
Вычисление критерия CV_2 Calculation of the criterion
$r = (3, 4, 7, 6)$ $\delta = (1, 0.873, 0.746, 0.599)$ $\delta^* = (10, 9, 8, 6)$ $CV_2 = 0.799$

Таким образом, для респондента Θ, стены которого близки к средним значениям стенов жертв по каждому из рассмотренных видов кибермошенничества, показатели степени его подверженности данным киберпреступлениям достаточно близки к единице,

что свидетельствует о высоком уровне потенциальной кибервиктимности этого респондента по отношению к данным угрозам.

Таблица 2. Вычисление критерия CV_3 для мошенничества в сфере онлайн-покупок
Table 2. Calculating the CV_3 criterion for fraud in online shopping

Исходные данные для преступления P_3 (мошенничество в сфере онлайн-покупок) Initial data for the crime
$T = 3$: C_5, C_{11}, C_{15} $v = (7.194, 2.605, 3.088)$ $\rho = (3.523, 6.871, 7.549)$
Вычисление весовых коэффициентов *w* Calculation of weighting coefficients
$\Delta = (3.671, -4.266, -4.461)$ $w = (0.296, 0.344, 0.360)$
Вычисление критерия CV_3 Calculation of the criterion
$r = (7, 3, 4)$ $\delta = (0.947, 0.907, 0.796)$ $\delta^* = (10, 9, 8)$ $CV_3 = 0.879$

По аналогичной схеме выполним расчет критериев CV_1, CV_2, CV_3 для респондента Θ, стены которого будут близки к средним значениям стенов резистентов по этим же видам кибермошенничества. Результаты оформим в виде таблицы 3.

Таблица 3. Вычисление критериев CV_1, CV_2, CV_3 для респондента — резистента
Table 3. Calculating criteria CV_1, CV_2, CV_3 for the resistant respondent

Преступление P_1 (фишинг) Crime phishing
$T = 3$: C_3, C_4, C_{15} $v = (2.784, 3.576, 3.261)$ $\rho = (6.928, 7.552, 8.103)$ $\Delta = (-4.144, -3.976, -4.842)$ $w = (0.320, 0.307, 0.374)$ $r = (6, 7, 8)$ $\delta = (0.224, 0.169, 0.021)$ $\delta^* = (3, 2, 1)$ $CV_1 = 0.122$
Преступление P_2 (вишинг) Crime vishing
$T = 4$: C_3, C_9, C_{12}, C_{16} $v = (3.046, 3.350, 8.362, 7.935)$ $\rho = (7.329, 8.474, 2.991, 3.108)$ $\Delta = (-4.283, -5.124, 5.371, 4.827)$ $w = (0.218, 0.261, 0.274, 0.246)$ $r = (6, 6, 3, 4)$ $\delta = (0.31, 0.483, 0.001, 0.185)$ $\delta^* = (4, 5, 1, 3)$ $CV_2 = 0.24$
Преступление P_3 (мошенничество в сфере онлайн-покупок) Crime online shopping fraud
$T = 3$: C_5, C_{11}, C_{15} $v = (7.194, 2.605, 3.088)$ $\rho = (3.523, 6.871, 7.549)$ $\Delta = (3.671, -4.266, -4.461)$ $w = (0.296, 0.344, 0.360)$ $r = (4, 5, 8)$ $\delta = (0.130, 0.439, 0)$ $\delta^* = (2, 5, 1)$ $CV_3 = 0.189$

Из приведенных в табл. 3 результатов расчета следует, что для респондента Θ, стены которого близки к средним значениям стенов резистентов соответствующих преступлений, критерии CV_1, CV_2, CV_3 достаточно близки к нулю, что подразумевает низкую кибервиктимность респондента. Таким образом, результаты моделирования демонстрируют соответствие рассчитанных показателей ожидаемым результатам, что подтверждает работоспособность модели.

Вывод. Разработанная математическая модель определения степени склонности к подверженности определенному киберпреступлению может стать основой для построе-

ния модели выявления общего уровня кибервиктимности респондента для произвольного множества рассматриваемых киберпреступлений по совокупности числовых показателей его черт характера, выявленных с помощью теста Кеттела. Эта модель может быть применена в практической деятельности специалистов, работающих с персоналом, для выявления потенциальных угроз, связанных с кибервиктимным поведением тестируемого контингента.

Библиографический список:

1. Кириленко В.П., Алексеев Г.В. Гармонизация российского уголовного законодательства о противодействии киберпреступности с правовыми стандартами Совета Европы // Всероссийский криминологический журнал. 2020. Т. 14. № 6. С. 898-913. URL: https://cj.bgu.ru/reader/article.aspx?id=24196 (дата обращения: 28.10.2024).
2. URL: nbpublish.com/e_lr/contents_2020_4.html#32627 (дата обращения: 28.10.2024). Комаров А.А. Исследование по вопросу определения объема генеральной совокупности жертв мошенничества, совершенного посредством глобальной компьютерной сети Интернет //Юридические исследования. 2020. № 4. С. 29-45
3. Состояние преступности в России за январь-август 2024 года. М.: ФКУ «ГИАЦ» МВД РФ. URL: https://media.mvd.ru/files/application/7206717 (дата обращения: 23.10.2024).
4. Красовская Н.Р., Гуляев А.А. К вопросу о кибермошенничестве // Вестник Удмуртского университета. Социология. Политология. Международные отношения. 2022. №1. С. 133-138. URL: https://journals.udsu.ru/sociology/article/view/6709 (дата обращения: 28.10.2024).
5. Жмуров Д.В. Модели реализации виктимности в цифровой среде // Защита жертв преступлений в современном обществе: материалы VI Международной научно-практической интернет-конференции (Челябинск, 21–22 февраля 2023 г.). — Челябинск:Эскуэла, 2023. — С. 88-93. URL: https://victimolog.ru/index.php/PVCMS/article/view/532 (дата обращения: 28.10.2024).
6. Кузнецов М.В., Симдянов И.В.Социальная инженерия и социальные хакеры.- СПб.:БХВ-Петербург, 2007. - 368 с.
7. Грей Дж. Социальная инженерия и этичный хакинг на практике. - М.:ДМК Пресс, 2023. - 226с.
8. 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: 28.10.2024).
9. Мозжухина Ю. Н. Когнитивные искажения как свойство поведенческих моделей // Проблемы педагогики. 2017. № 9 (32). С.22-25. URL: https://problemspedagogy.ru/images/PDF/2017/32/Problemy-pedagogiki-9-32.pdf (дата обращения: 28.10.2024).
10. Шейнов В. П. Психология обмана и мошенничества. - М.:АСТ, -Мн.:Харвест, 2010. - 464 с.
11. URL: https://socio.isu.ru/export/sites/socio/ru/media/news/2021/.galleries/docs/__2021-1.pdf (дата обращения: 28.10.2024) Цивелев А.С. Информационная безопасность контрактных систем в сфере закупок//Социальная реальность виртуального пространства. III Междунар. науч.-практ. конф.(Иркутск, 20 сентября 2021 г.):материалы докл. Иркутск:Изд-воИГУ, 2021.- С.274-279.
12. Жмуров Д.В. Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. 2021. № 3. С. 109–121. URL: http://www.prolaw38.ru/kiberviktimizacija-issledovatelskaja-matrica/ (дата обращения: 28.10.2024).
13. URL: https://shelly.kpfu.ru/e-ksu/docs/F_598192770/elibrary_Victimological_features_of_cybercrime.pdf (дата обращения: 28.10.2024).Айнутдинова К.А., Айнутдинова И.Н. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества//Наука, образование: современные цифровые технологии формирования экосреды инновационного развития региона в условиях системных преобразований: мат-лы национальной научно-практич. конференции в 2-х частях. Часть 1. Казань: Университет управления «ТИСБИ», 2022.- С.34-40.
14. Первушина О.Н., Федоров А.А. Личностные особенности жертв телефонного мошенничества // Вопросы психологии. 2022. Т. 68. № 3. С. 92-103. URL: http://www.voppsy.ru/cnew22N3.htm (дата обращения: 28.10.2024).
15. Ildirim E., Çalici C., Erdoğan B. Psychological Correlates of Cyberbullying and Cyber-Victimization // The International Journal of Human and Behavioral Science. 2017. Vol. 3. № 2. Pp. 7-21. URL: https://dergipark.org.tr/en/download/article-file/395312 (дата обращения: 28.10.2024).
16. Olenik-Shemesh D., Heiman T., Zuaretz-Hannan M. Cyber-victim1ization among Children: Prevalence, Characteristics, Gender Differences and Links to Social Difficulties // Journal of Child and Adolescent Behavior. 2017. Vol. 5. № 2. 11 p. URL: https://www.omicsonline.org/open-access-pdfs/cybervictimization-

among-children-prevalence-characteristics-genderdifferences-and-links-to-social-difficulties-2375-4494-1000339.pdf (дата обращения: 28.10.2024).
17. URL:https://gpa.cfuv.ru/attachments/article/4051/%D0%92%D1%8B%D0%BF%D1%83%D1%81%D0%BA%2064%20%D1%87%D0%B0%D1%81%D1%82%D1%8D%B4.pdf (дата обращения: 28.10.2024). Братусин А.Р., Власенко Е.Е. О характерных индивидуально-типологических особенностях и поведенческих паттернах личности типичных жертв финансового мошенничества // Проблемы современного педагогического образования. 2019. № 64 - 4. С. 292-294.
18. Дроздикова-Зарипова А.Р., Калацкая Н.Н., Валеева Р.А., Костюнина Н.Ю., Биктагирова Г.Ф. Социально-психологические особенности студентов, склонных к виктимному поведению в интернет-пространстве // Современные наукоемкие технологии. 2019. № 12-1. С. 159-166. URL: https://top-technologies.ru/ru/article/view?id=37852 (дата обращения: 28.10.2024).
19. 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: 28.10.2024).
20. URL: https://psyjournals.ru/journals/psylaw/archive/2022_n2/Vlasova_Buslaeva (дата обращения: 28.10.2024). Власова Н.В., Буслаева Е.Л. Психологические особенности лиц, склонных к кибервиктимному поведению // Психология и право. 2022. Т. 12. № 2. С. 194-206.
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: 23.10.2024).
22. Кудинов С.И., Кудинов С.С. Психодиагностика личности: учебн. пособие. — Тольятти: Изд-во ТГУ, 2012. — 270 с.
23. Акимова М.К., Горбачева Е.И., Зархин В.Г., Козлова В.Т., Ярошевская С.В. Психодиагностика. Теория и практика : учебник для вузов. — М. :Юрайт, 2024. — 609 с.
24. Минюк С.А., Ровба Е.А., Кузьмич К.К. Математические методы и модели в экономике: Учеб. пособие. -М.: ТетраСистемс, 2002. — 432с.

References:

1. Kirilenko V.P., Alekseev G.V. The Harmonization of Russian Criminal Legislation on Counteracting Cybercrime With the Legal Standards of the Council of Europe. *Russian Journal of Criminology*. 2020; 14(6): 898-913. (In Russ.) URL: https://cj.bgu.ru/reader/article.aspx?id=24196 (accessed 28.10.2024).
2. URL: nbpublish.com/e_lr/contents_2020_4.html#32627 (accessed 28.10.2024). Komarov A.A. Research on the Question of Determination of the Total Number of Fraud Victims Committed Via Internet. *Legal Research*. 2020; 4:29-45. (In Russ.)
3. 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 23.10.2024).
4. Krasovskaya N.R., Gulyaev A.A. On the Issue of Cyber Fraud. *Bulletin of Udmurt University. Sociology. Political Science. International Relations*. 2022; 6(1): 133–138. (In Russ.) URL: https://journals.udsu.ru/sociology/article/view/6709 (accessed 28.10.2024).
5. Zhmurov D. V. Models of Victimhood Implementation in the Digital Environment. / Protection of Victims of Crime in Modern Society (PVCMS 2023), VI International Scientific-Practical Internet-Conference, Chelyabinsk, Russia, February 21-22, 2023, Proceedings, Escuela Chelyabinsk, pp. 88-93. (In Russ.) URL: https://victimolog.ru/index.php/PVCMS/article/view/532 (accessed 28.10.2024).
6. Kuznetsov M.V., Simdyanov I.V. Social Engineering and Social Hackers. St.Petersburg: BHV- Petersburg, 2007; 368. (In Russ.)
7. Gray J. Practical Social Engineering:A Primer for the Ethical Hacker. M.:DMK-Press, 2023;226. (In Russ.)
8. 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 28.10.2024).
9. Mozzhukhina Yu.N. Cognitive Distortions as a Property of Behavioral Models. *Pedagogical Problems*. 2017; 9(32): 22-25. (In Russ.) URL: https://problemspedagogy.ru/images/PDF/2017/32/Problemy-pedagogiki-9-32.pdf (accessed 28.10.2024).
10. Sheynov V.P. The Psychology of Deception and Fraud. M.: AST, Minsk: Harvest, 2010; 464. (In Russ.)
11. URL: https://socio.isu.ru/export/sites/socio/ru/media/news/2021/.galleries/docs/__2021-1.pdf (accessed 28.10.2024) Tsivilev A.S. Information Security of Contract Systems in the Field of Procurement. / Social Reality of Virtual Space, III International Scientific-Practical Conference, Irkutsk, Russia, September 20, 2021, Proceedings, Irkutsk State University Publishing, pp. 274-279. (In Russ.)

12. Zhmurov D.V. Cybervictimization. Research Matrix. *Prologue: Law Journal*. 2021; 3: 109-121. (In Russ.) URL: http://www.prolaw38.ru/kiberviktimizacija-issledovatelskaja-matrica/ (accessed 28.10.2024).
13. URL: https://shelly.kpfu.ru/e-ksu/docs/F_598192770/elibrary_Victimological_features_of_cybercrime.pdf (accessed 28.10.2024). Ainoutdinova K.A., Ainoutdinova I.N. Victimological Features of Cybercrime in the Context of Digital Transformation of Society. / Science, education: modern digital technologies for the formation of the eco-environment of innovative development of the region in the context of system transformations, National Scientific-Practical Conference, Kazan, Russia, 2022, Proceedings in 2 parts, Part 1, Kazan University of Management «TISBI», pp. 34-40. (In Russ.)
14. Pervushina O.N., Fedorov A.A. Personal Characteristics of Vishing Victims. *Voprosy Psikhologii*. 2022; 68(3): 92-103. (In Russ.) URL: http://www.voppsy.ru/cnew22N3.htm (accessed 28.10.2024).
15. Ildirim E., Çalici C., Erdoğan B. Psychological Correlates of Cyberbullying and Cyber-Victimization // *The International Journal of Human and Behavioral Science*. 2017; 3(2): 7-21. URL: https://dergipark.org.tr/en/download/article-file/395312 (accessed 28.10.2024).
16. Olenik-Shemesh D., Heiman T., Zuaretz-Hannan M. Cyber-Victimization Among Children: Prevalence, Characteristics, Gender Differences and Links to Social Difficulties // *Journal of Child and Adolescent Behavior*. 2017; 5(2): 11 p. URL: https://www.omicsonline.org/open-access-pdfs/cybervictimization-among-children-prevalence-characteristics-genderdifferences-and-links-to-social-difficulties-2375-4494-1000339.pdf (accessed 28.10.2024).
17. URL:https://gpa.cfuv.ru/attachments/article/4051/%D0%92%D1%8B%D0%BF%D1%83%D1%81%D0%BA%2064%20%D1%87%D0%B0%D1%81%D1%82%D1%8C%204,%2%B4.pdf (accessed 28.10.2024). 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.)
18. Drozdikova-Zaripova A.R., Kalatskaya N.N., Valeeva R.A., Kostyunina N.Yu., Biktagirova G.F. Socio-Psychological Features of Students Inclined to Victim Behavior in the Internet. *Modern high technologies*. 2019;12-1:159-166 (In Russ.) URL: https://top-technologies.ru/ru/article/view?id=37852 (accessed 28.10.2024).
19. 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 28.10.2024).
20. URL: https://psyjournals.ru/journals/psylaw/archive/2022_n2/Vlasova_Buslaeva (accessed 28.10.2024). Vlasova N.V., Buslaeva E.L. Psychological Features of Individuals Prone to Cyber Victimization. *Psychology and Law*. 2022; 12(2): 194-206. (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 23.10.2024).
22. Kudinov S.I., Kudinov S.S. Psychodiagnostics of Personality. A Study Guide. Togliatti: Togliatti State University Publishing, 2012; 270. (In Russ.)
23. Akimova M.K., Gorbacheva E.I., Zarkhin V.G., Kozlova V.T., Yaroshevskaya S.V. Psychodiagnostics. Theory and Practice. Textbook for Universities. M.:Urait, 2024; 609. (In Russ.)
24. Minyuk S.A., Rovba E.A. Kuzmich K.K. Mathematical Methods and Models in Economics. A Study Guide. M.:TetraSystems, 2002; 432. (In Russ.)

Сведения об авторах:

Карпасюк Игорь Владимирович, кандидат физико-математических наук, доцент, доцент, кафедра высшей 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 Higher and 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 04.11.2024.

Одобрена после рецензирования / Reviced 20.12.2024.

Принята в печать /Accepted for publication 11.01.2025.