Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2024. № 2
Vestnik of Astrakhan State Technical University.
Series: Management, computer science and informatics. 2024. N. 2
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)

КОМПЬЮТЕРНОЕ ОБЕСПЕЧЕНИЕ И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

COMPUTER ENGINEERING AND SOFTWARE

Научная статья
УДК 621.357
https://doi.org/10.24143/2072-9502-2024-2-77-84
EDN KYXVUS

Формализация процедуры выявления личностных характеристик потенциальной жертвы кибермошенничества

Игорь Владимирович Карпасюк✉, Александр Игоревич Карпасюк, Надежда Валерьевна Давидюк, Елена Витальевна Чертина

Астраханский государственный технический университет,
Астрахань, Россия, ikarpasyuk@mail.ru✉

Аннотация. Рассмотрено текущее состояние проблемы киберпреступности и выделены наиболее распространенные виды кибермошенничества. Описано понятие кибервиктимности как сочетание черт личности, характеризующее повышенный уровень склонности к тому, чтобы стать жертвой киберпреступления. Предложена процедура выявления личностных характеристик, присущих лицам с повышенной кибервиктимностью. Изучены подходы к исследованию взаимосвязи степени выраженности определенных черт характера с проявлением кибервиктимности. Рассмотрены методы психологической диагностики с целью выявления личностных качеств. Для определения количественных характеристик степени проявления черт характера с помощью 16-факторного личностного опросника Р. Кеттелла проведено тестирование выборки респондентов, в отношении которых были применены мошеннические действия в киберпространстве. Респонденты разбиты на две контрольные группы – поддавшихся действиям кибермошенников и сумевших им противостоять. Для каждого респондента получен набор стенов, описывающих степень проявления соответствующих черт характера. Поставлена задача выявления особенностей личности, наиболее характерных для респондентов каждой из контрольных групп, путем нахождения наибольшей вариации значений стенов по каждой из черт характера в разрезе рассматриваемых видов кибермошенничества. С помощью критерия Манна – Уитни проведена оценка различий в соответствующих выборках стенов, переведенных в ранговую шкалу. С помощью анализа асимптотической значимости различий в средних рангах выбраны черты характера, по которым достоверность различий максимальна, и получена матрица, позволяющая охарактеризовать склонность к подверженности определенному виду кибермошенничества наиболее выраженным проявлением именно этих черт характера. Проведено сравнение полученных результатов с опубликованными результатами исследований в данной области, выявлено их качественное соответствие. Сформировано множество личностных характеристик, значимых с точки зрения подверженности кибермошенничеству. Задано направление развития исследуемой темы.

Ключевые слова: кибермошенничество, кибервиктимность, фишинг, вишинг, степень выраженности черт характера, тест Кеттелла, критерий Манна – Уитни, подверженность кибермошенничеству

Для цитирования: *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. https://doi.org/10.24143/2072-9502-2024-2-77-84. EDN KYXVUS.

Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2024. № 2
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)
Компьютерное обеспечение и вычислительная техника

Original article

Formalising the procedure for identifying the personality characteristics of a potential cyber fraud victim

Igor V. Karpasyuk✉, Alexander I. Karpasyuk, Nadezhda V. Davidyuk, Elena V. Chertina

Astrakhan State Technical University,
Astrakhan, Russia, ikarpasyuk@mail.ru✉

Abstract. The current state of the problem of cybercrime is considered and the most common types of cyber fraud are highlighted. The concept of cybervictimisation is described as a combination of personality traits characterising an increased level of propensity to become a victim of cybercrime. A procedure for identifying personality characteristics of individuals with increased cybervictimisation is proposed. Approaches to researching the relationship between the degree of expression of certain character traits and the manifestation of cybervictimisation are studied. The methods of psychological diagnostics for the purpose of identifying personality traits are considered. To determine the quantitative characteristics of the degree of manifestation of character traits, the 16-factor personality questionnaire of R. Kettell was used to test a sample of respondents who were subjected to fraudulent actions in cyberspace. The respondents were divided into two control groups – those who succumbed to the actions of cyber fraudsters and those who managed to resist them. For each respondent, a set of walls describing the degree of manifestation of the relevant character traits was obtained. The task was to identify the personality traits most characteristic of the respondents in each of the control groups by finding the greatest variation in the wall values for each of the character traits across the types of cyberfraud under consideration. The Mann-Whitney criterion was used to evaluate the differences in the respective samples of walls translated into a ranking scale. Using the analysis of asymptotic significance of differences in the average ranks, the character traits for which the reliability of differences is maximum were selected, and a matrix was constructed that allows characterising the propensity to be exposed to a certain type of cyber fraud by the most pronounced manifestation of these character traits. The obtained results were compared with published research results in this area, and their qualitative correspondence was revealed. The set of personality characteristics significative in terms of exposure to cyber fraud is generated. The direction of development of the topic under study is set.

Keywords: cyber fraud, cyber victimhood, phishing, vishing, degree of expression of character traits, Kettell test, Mann-Whitney criterion, exposure to cyber fraud

For citation: 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.). https://doi.org/10.24143/2072-9502-2024-2-77-84. EDN KYXVUS.

Введение

В настоящее время формирование глобального киберпространства позволяет переводить различные виды человеческой деятельности в виртуальный формат, предоставляя возможность осуществлять взаимодействие посредством использования компьютерных коммуникаций. При этом вопросы обеспечения информационной безопасности приобретают особую актуальность. Вместе с бесспорными преимуществами цифровой эры возникают и новые угрозы, обобщаемые понятием киберпреступности как совокупности противоправных действий в киберпространстве.

Киберпреступность как в мире, так и в России демонстрирует высокие темпы роста. По статистике МВД РФ, за январь–сентябрь 2023 г. доля киберпреступлений в общей структуре и массиве преступности в РФ составила около 33 %, хотя за тот же период 2022 г. она составляла около 25 % [1]. При этом мошенничество является одним из наиболее часто совершаемых преступлений в киберпространстве. Согласно статистическим исследованиям, фишинг, вишинг и мошенничество в сфере онлайн-покупок относятся к числу наиболее популярных видов кибермошенничества. Так, на основе опроса интернет-пользователей, проведенного компанией «МТС Red», с начала 2023 г. с фишингом столкнулось больше половины россиян, причем треть опрошенных заявили, что получают фишинговые рассылки несколько раз в месяц [2]. По данным Сбербанка, в 2020 г. телефонные аферисты позвонили россиянам около 15 млн раз, каждый десятый звонок в России был мошенническим, при этом 80 % злоумышленников используют подмену номеров [3]. Согласно исследованиям компании Ozon, 66 % опрошенных становились жертвой мошенников при совершении онлайн-покупок, 44 % из них – один раз, а 4 % – более пяти раз [4].

Одной из наиболее серьезных угроз, вызванных явлением кибермошенничества, является вторжение киберпреступников в область личной безопасности. Оно может быть связано не только с хищением личных данных, нарушением прав и интересов в виртуальной среде, но и нанесением материального ущерба, что приводит к возникновению проблем за рам-

ками киберпространства. Поэтому вопросам кибербезопасности сейчас уделяется большое внимание.

Киберпреступники используют как техническую, так и социально-психологическую составляющие своей деятельности. И если попытки проникновения в защищенные информационные системы, предпринимаемые киберпреступниками с помощью программно-технических средств, все чаще оказываются сопряжены с непомерно большими усилиями и значительным риском обнаружения и блокирования, то воздействие на сотрудников организаций с целью получения необходимой конфиденциальной информации может принести желаемый результат со значительно меньшими затратами, и в организованной системе кибербезопасности зачастую именно человек представляется наиболее уязвимым звеном.

С помощью различных приемов искажения информации мошенник воздействует на интеллектуально-волевую сферу жертвы, тем самым манипулируя ею. Уязвимость к подобным манипуляциям в киберпространстве может быть описана понятием «кибервиктимность». Кибервиктимность представляет собой склонность индивида к тому, чтобы становиться жертвой компьютерных преступлений (кибержертвой) в силу психологических особенностей своей личности, выражаемых определенными чер тами характера. Поэтому актуальной задачей является выявление взаимосвязей между степенью выраженности черт характера и кибервиктимностью.

Проблемам кибервиктимности посвящен ряд современных исследований, выявляющих психологические аспекты кибервиктимности и специфические особенности личности, присущие жертвам киберпреступлений разного типа [5, 6]. Подобный подход позволяет развить идею качественного описания такой взаимосвязи в направлении формирования количественных критериев кибервиктимности в зависимости от уровня различий в средних показателях выраженности соответствующих личностных характеристик жертв киберпреступлений и лиц, сумевших успешно противостоять манипуляциям кибермошенников. Построение таких критериев должно основываться на статистической информации о психологических особенностях и чертах характера обеих категорий лиц, испытавших на себе воздействие киберпреступников.

Целью исследования является установление влияния личностных характеристик на склонность к проявлению кибервиктимности и определение наборов таких характеристик для конкретных видов кибермошенничества.

Для достижения указанной цели предлагается следующая процедура выявления личностных характеристик, присущих лицам с повышенной кибервиктимностью:

1. Сбор статистических данных, необходимых для формирования контрольных групп, посредством анкетирования респондентов, подвергшихся действиям кибермошенников.

1.1. Формирование выборки респондентов, которые подвергались тем или иным мошенническим действиям в киберпространстве.

1.2. Проведение тестирования респондентов на предмет выявления факта подверженности конкретному виду кибермошенничества $P = \{P_1, P_2, P_3\}$, где P_1 – фишинг, P_2 – вишинг, P_3 – мошенничество в сфере онлайн-покупок.

1.3. Проведение тестирования респондентов по методике Р. Кеттелла с целью выявления 16-и основных особенностей характера личности $C = \{C_1, ..., C_{16}\}$.

Результат:

– из числа респондентов сформированы 2 контрольные группы: $V = \{V_1, ..., V_N\}$ – респонденты, ставшие жертвами кибермошенничества; $R = \{R_1, ..., R_M\}$ – респонденты, которые смогли противостоять преступному воздействию;

– определены числовые характеристики, описывающие уровень проявления личностных характеристик каждого респондента.

2. Выявление зависимости между уровнями проявления личностных характеристик и видами кибермошенничества у респондентов 2-х групп.

Результат: получена матрица S, описывающая влияние личностных характеристик C_k, $k = 1, \ldots, 16$, на кибервиктимность по видам мошенничества P_i, $i = 1, 2, 3$.

3. Формирование множества личностных характеристик, значимых с точки зрения подверженности кибермошенничеству.

Практическая реализация процедуры выявления личностных характеристик, присущих лицам с повышенной кибервиктимностью

Получение статистических данных и формирование контрольных групп. Специфика диагностики личностных качеств заключается в выборе средств диагностики. С точки зрения выявления и анализа структуры личности в современной психологической диагностике наиболее распространенными являются две большие группы методов – проективные методики и опросники. Проективные методики основаны на анализе продуктов воображения и фантазии и направлены на раскрытие внутреннего мира личности, мира ее субъективных переживаний, мыслей, установок, ожиданий. Опросник – тип методик, задания в которых представлены в виде вопросов или утверждений, не имеющих правильного ответа и характеризующихся только их частотой и направленностью.

В рамках настоящего исследования целесообразно использовать личностные опросники, которые

представляют собой совокупность методических средств, применяемых для выявления и оценки индивидуальных свойств личности человека, определяющих его поступки. В качестве средства тестирования для определения уровней проявления черт личности был выбран 16-факторный личностный опросник Р. Кеттелла (форма А) [7]. Отличительной особенностью теста Кеттелла является его ориентация на выявление независимых факторов (первичных черт) личности. Многолетняя практика его успешного использования и достаточно высокий уровень надежности и валидности результатов позволяют считать тест Кеттелла адекватным инструментом измерения личностных характеристик, предоставляющим количественное описание проявления черт характера респондентов, необходимое для последующего анализа их кибервиктимности.

Методика Р. Кеттелла (методика 16PF) имеет стеновую стандартизацию, т. е. полученные в процессе опроса результаты с помощью ключей переводятся в стандартные баллы (стены). В тесте Кеттелла стены могут принимать целочисленные значения на отрезке от 1 до 10, где 1 соответствует минимальному проявлению соответствующего фактора (так называемый Полюс «–»), 10 – его максимальному проявлению (Полюс «+»). В качестве результатов диагностики можно получить качественную и количественную оценку особенностей характера человека.

В целях изучения вопроса влияния личностных характеристик на кибервиктимность была сделана выборка лиц (респондентов), которые подвергались тем или иным мошенническим действиям в киберпространстве. Объем такой выборки составил 106 человек. В число респондентов вошли лица, впервые однократно подвергавшиеся воздействию киберпреступников ровно по одному виду кибермошенничества из множества $P = \{P_1, P_2, P_3\}$.

Тестирование лиц, вошедших в данную выборку, проводилось в 2 этапа. На первом этапе респондентам предлагалось заполнить анонимную анкету, содержащую вопросы, связанные с подверженностью конкретному виду кибермошенничества. На втором этапе респонденты проходили тестирование по опроснику Кеттелла с целью выявления 16-и основных особенностей характера. Обозначим множество таких особенностей $C = \{C_1, ..., C_{16}\}$ (табл. 1).

Таблица 1

Table 1

Соответствие первичных факторов теста Кеттелла элементам множества *C*

The correspondence of the primary factors of the Kettell test to the elements of the set *C*

Элемент множества *C*	Обозначение первичного фактора	Полюс «–»	Полюс «+»
C_1	*A*	Замкнутость	Общительность
C_2	*B*	Низкая интеллектуальность	Высокая интеллектуальность
C_3	*C*	Эмоциональная нестабильность	Эмоциональная стабильность
C_4	*E*	Подчиненность	Доминантность
C_5	*F*	Сдержанность	Экспрессивность
C_6	*G*	Низкая нормативность поведения	Высокая нормативность поведения
C_7	*H*	Робость	Смелость
C_8	*I*	Жестокость	Чувствительность
C_9	*L*	Доверчивость	Подозрительность
C_{10}	*M*	Практичность	Мечтательность
C_{11}	*N*	Прямолинейность	Дипломатичность
C_{12}	*O*	Спокойствие	Тревожность
C_{13}	*Q*1	Консерватизм	Радикализм
C_{14}	*Q*2	Конформизм	Нонконформизм
C_{15}	*Q*3	Низкий самоконтроль	Высокий самоконтроль
C_{16}	*Q*4	Расслабленность	Напряженность

Тестирование по опроснику Кеттелла проводилось в электронном виде с помощью инструментов сайта psytests.org. Пример результата выполнения теста Кеттелла доступен на том же сайте [8]. Результаты тестирования были сохранены в обезличенном виде и агрегированы. На их основе были сформированы 2 группы респондентов (контрольные группы). Первую группу составили лица, которые пострадали от действий кибермошенников (жертвы). Во вторую группу вошли люди, сумевшие противостоять преступным действиям и не стать жертвами кибермошенничества (резистенты).

С учетом данных анонимных анкет респондентов была построена табл. 2.

Таблица 2

Table 2

Распределение количества респондентов по видам кибермошенничества, чел.

Distribution of the number of respondents by types of cyber fraud, person

Респонденты	Фишинг	Вишинг	Мошенничество в сфере онлайн-покупок
Жертвы	9	6	10
Резистенты	28	32	21

Постановка задачи. Имеются выборка жертв $V = \{V_1, ..., V_N\}$ объемом $N = 25$ и выборка резистентов $R = \{R_1, ..., R_M\}$ объемом $M = 81$. Каждому элементу V_g соответствует набор стенов v_{gk}, которые показывают выраженность черты характера C_k у жертвы V_g, $g = 1, \ldots, N$, $k = 1, \ldots, 16$. Каждому элементу R_h соответствует набор стенов r_{hk}, которые показывают выраженность черты характера C_k у резистента R_h, $h = 1, \ldots, M$, $k = 1, \ldots, 16$.

Необходимо оценить уровни вариации стенов, описывающих степень выраженности соответствующих черт характера (которые являются исследуемыми признаками) у респондентов, относящихся к разным контрольным группам – жертв и резистентов, а также провести редукцию числа признаков и выделение факторов (в соответствии с табл. 1), оказывающих доминирующее воздействие на вероятность попадания в одну из выборок – V или R.

Данная задача может быть формализована следующим образом. Заданы числовые характеристики значений ряда параметров в каждой из двух выборок. Следует определить, насколько влияние одного параметра выражено сильнее относительно влияния другого параметра при сравнении этих выборок.

Обработка полученных статистических данных. Для решения этой задачи был использован статистический метод сравнения выборок, построенный на основе непараметрического U-критерия Манна – Уитни [9]. В этом критерии выборки представляются в ранговой шкале и сравниваются не величины признаков, а их ранги. В отличие от других известных методов сравнения выборок, таких как корреляционный и дисперсионный анализ, регрессионные модели, факторный анализ, кластерный анализ и др., преимуществом критерия Манна – Уитни является возможность работы с выборками небольшого объема, причем содержащими разное количество элементов, что согласуется со спецификой проводимого исследования.

С целью выявления значимых черт характера, которые имеют основное влияние на подверженность соответствующим видам кибермошенничества, для каждого вида мошенничества P_i, $i = 1, 2, 3$, из элементов v_{gk} были составлены выборки $X_{ik} = \{X_{ik}^{(1)}, ..., X_{ik}^{(n)}\}$, содержащие стены, соответствующие определенной черте характера C_k, $k = 1, \ldots, 16$, у жертв $V_1, ..., V_n$ мошенничества P_i. Аналогичные выборки $Y_{ik} = \{Y_{ik}^{(1)}, ..., Y_{ik}^{(m)}\}$, содержащие стены по той же черте характера C_k, были составлены из элементов r_{hk} для резистентов $R_1, ..., R_m$ мошенничества P_i, причем в общем случае $m \neq n$. Для оценки различий между двумя независимыми и несвязанными малыми выборками X_{ik} и Y_{ik} по уровню количественной выраженности величины признака, описывающей проявление черты характера C_k в рамках вида мошенничества P_i, применен U-критерий Манна – Уитни.

Статистическая обработка полученных выборочных данных проводилась с помощью программы IBM SPSS Statistics, версия 27.0.1.0. По всем парам выборок X_{ik}, Y_{ik} были найдены средние ранги ν_{ik}, ρ_{ik} соответственно, а также асимптотическая значимость α_{ik} их различий, $i = 1, 2, 3$, $k = 1, \ldots, 16$. Пример вычисления данных показателей приведен на рисунке ниже.

Критерий Манна-Уитни

Ранги

	Группы	N	Средний ранг	Сумма рангов
Анкетируемые	1 группа	9	9,83	88,50
	2 группа	28	21,95	614,50
	Всего	37		

Статистические критерии[a]

	Анкетируемые
U Манна-Уитни	43,500
W Уилкоксона	88,500
Z	-2,959
Асимп. знач. (двухсторонняя)	,003
Точная знч. [2*(1-сторон. знач.)]	,002[b]

a. Группирующая переменная: Группы

b. Не скорректировано на наличие связей.

Результат расчета характеристик для $i = 1$, $k = 3$

The result of calculating the characteristics for $i = 1$, $k = 3$

Асимптотическая значимость характеризует достоверность различий в выборках данных: чем она ближе к нулю, тем достоверность выше.

Результаты и их обсуждение

Введем величину $\Delta_{ik} = \nu_{ik} - \rho_{ik}$, $i = 1, 2, 3$, $k = 1, \ldots, 16$, характеризующую величину разброса значений средних рангов в выборках жертв и резистентов. Ее знак определяет, какие значения стенов по черте характера C_k в среднем характерны для жертв мошенничества P_i. Так, низким значениям стенов

будут соответствовать отрицательные значения Δ_{ik}, высоким значениям стенов – положительные значения Δ_{ik}.

Приняв, что достоверные различия будут достигаться для тех показателей выборок (черт характера респондентов), у которых величина асимптотической значимости не превышает значение 0,01, на основании результатов расчетов из множества C были выделены черты характера, которые оказывают доминирующее влияние на подверженность каждому из видов киберпреступлений, входящих в множество P. Полученная взаимосвязь между такими чертами характера и видами кибермошенничества представлена в виде матрицы S:

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

В матрице S строки соответствуют видам мошенничества P_i, $i = 1, 2, 3$, столбцы – чертам характера C_k, $k = 1, \ldots, 16$. Элементы s_{ik} матрицы S находят по следующим правилам:

$$s_{ik} = \begin{cases} 0, \ \alpha_{ik} > 0,01; \\ -1, \ \alpha_{ik} \le 0,01, \ \Delta_{ik} < 0; \\ 1, \ \alpha_{ik} \le 0,01, \ \Delta_{ik} > 0. \end{cases}$$

Таким образом, ненулевой элемент s_{ik} матрицы S свидетельствует о том, что у жертв и резистентов кибермошенничества P_i выявлена наиболее значимая разница в средних уровнях проявления черты характера C_k. При этом условие $s_{ik} = 1$ обозначает, что жертвам данного кибермошенничества присуща сильная выраженность соответствующей черты характера, определяемая значениями стенов, близкими к их максимальному значению на Полюсе «+», а условие $s_{ik} = -1$ обозначает, наоборот, слабую выраженность этой черты характера со значениями стенов жертв, близкими к их минимальному значению на Полюсе «–».

Представленные в виде матрицы S итоговые данные, в агрегированной форме описывающие результаты выявления черт характера, которые имеют преобладающее влияние на подверженность рассмотренным видам кибермошенничества, свидетельствуют, что склонность к тому, чтобы стать жертвой фишинга, преимущественно обусловлена эмоциональной нестабильностью, преобладающей подчиненностью и низким самоконтролем; для вишинга такая склонность характеризуется эмоциональной нестабильностью, доверчивостью, тревожностью и высоким уровнем внутренней напряженности; для мошенничества в сфере онлайн-покупок – выраженной экспрессивностью, прямолинейностью характера и низким уровнем самоконтроля. Характерно, что низкий уровень проявления таких черт характера, как C_3 (эмоциональная стабильность) и C_{15} (самоконтроль) критичен для потенциальной подверженности их обладателя сразу нескольким видам киберпреступлений из числа указанных.

Результаты проведенного исследования в целом соответствуют качественной картине сопоставления различных видов мошеннических схем, применяемых в сфере информационных технологий, характерным чертам характера их жертв, приведенной в работе [10].

Исследование, проведенное в работе [11] с целью выявления психологических особенностей лиц, проявивших кибервиктимное поведение (без учета их рассмотрения в разрезе разных видов кибермошенничества) и основанное на сравнительном анализе результатов исследования контрольных групп, полученных с помощью методики 16PF Р. Кеттелла, тестов «Уровень субъективного контроля» и «Шкала реактивной и личностной тревожности», также подтверждает состоятельность описанного матрицей S соответствия: так, черты характера C_1, C_3, C_5, C_9, C_{11}, C_{12}, C_{15}, C_{16} выделены в работе [11] как те, по которым асимптотическая значимость различий соответствующих значений средних рангов в контрольных группах минимальна, что указывает на достоверность предположения о критичности соответствующих личностных характеристик в вопросе их влияния на кибервиктимность.

Заключение

Матрица S демонстрирует, какие типичные черты характера свойственны людям, наиболее подверженным воздействию указанных кибератак, однако она показывает только качественную картину подобных взаимосвязей. Полученные статистические данные, характеризующие числовые значения выраженности исследованных черт характера у респондентов контрольных групп в разрезе рассмотренных видов кибермошенничества, возможно использовать для определения количественных характеристик параметров, описывающих влияние соответствующих факторов на степень склонности к тому, чтобы стать жертвой того или иного киберпреступления. Эти количественные характеристики могут быть положены в основу математической модели выявления степени склонности к кибервиктимности, применяемой в рамках соответствующего тестирования.

Список источников

1. Состояние преступности в России за январь–сентябрь 2023 года. М.: ФКУ «ГИАЦ» МВД РФ. URL: https://media.mvd.ru/files/application/5011395 (дата обращения: 19.12.2023).

2. Более половины россиян столкнулись с мошенничеством в интернете с начала года. URL: https://www.vedomosti.ru/technology/articles/2023/08/02/988049-bolee-polovini-rossiyan-stolknulis-s-moshennichestvom-v-internete (дата обращения: 17.07.2023).

3. Вишинг стал самым популярным способом мошенничества. URL: https://rg.ru/2021/08/01/vishing-lidiruet-sredi-sposobov-moshennichestva.html (дата обращения: 17.07.2023).

4. Озон провела опрос-исследование по мошенничеству в сфере онлайн-покупок. URL: https://habr.com/ru/news/732354/ (дата обращения: 17.07.2023).

5. 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.

6. Ildirim E., Çalici C., Erdoğan B. Psychological Correlates of Cyberbullying and Cyber-Victimization // The International Journal of Human and Behavioral Science. 2017. V. 3. N. 2. P. 7–21.

7. Кудинов С. И., Кудинов С. С. Психодиагностика личности: учеб. пособие. Тольятти: Изд-во ТГУ, 2012. 270 с.

8. Тест Кеттелла, 16PF/A. URL: https://psytests.org/result?v=ctlA1S4whsl1T-dyg0IulTUD8K&pp=1 (дата обращения: 20.12.2023).

9. Сидоренко Е. В. Методы математической обработки в психологии. СПб.: Речь, 2010. 350 с.

10. 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.

11. Власова Н. В., Буслаева Е. Л. Психологические особенности лиц, склонных к кибервиктимному поведению // Психология и право. 2022. Т. 12. № 2. С. 194–206.

References

1. *Sostoianie prestupnosti v Rossii za ianvar'–sentiabr' 2023 goda* [The state of crime in Russia in January–September 2023]. Moscow, FKU «GIATs» MVD RF. Available at: https://media.mvd.ru/files/application/5011395 (accessed: 19.12.2023).

2. *Bolee poloviny rossiian stolknulis' s moshennichestvom v internete s nachala goda* [More than half of Russians have faced fraud on the Internet since the beginning of the year]. Available at: https://www.vedomosti.ru/technology/articles/2023/08/02/988049-bolee-polovini-rossiyan-stolknulis-s-moshennichestvom-v-internete (accessed: 17.07.2023).

3. *Vishing stal samym populiarnym sposobom moshennichestva* [Phishing has become the most popular method of fraud]. Available at: https://rg.ru/2021/08/01/vishing-lidiruet-sredi-sposobov-moshennichestva.html (accessed: 17.07.2023).

4. *Ozon provela opros-issledovanie po moshennichestvu v sfere onlain-pokupok* [Ozone conducted a survey on fraud in the field of online shopping]. Available at: https://habr.com/ru/news/732354/ (accessed: 17.07.2023).

5. Drozdikova-Zaripova A. R., Kalatskaia N. N., Valeeva R. A., Kostiunina N. Iu., Biktagirova G. F. Sotsial'no-psikhologicheskie osobennosti studentov, sklonnykh k viktimnomu povedeniiu v internet-prostranstve [Socio-psychological characteristics of students prone to victimized behavior in the Internet space]. *Sovremennye naukoemkie tekhnologii*, 2019, no. 12-1, pp. 159-166.

6. Ildirim E., Çalici C., Erdoğan B. Psychological Correlates of Cyberbullying and Cyber-Victimization. *The International Journal of Human and Behavioral Science*, 2017, vol. 3, no. 2, pp. 7-21.

7. Kudinov S. I., Kudinov S. S. *Psikhodiagnostika lichnosti: uchebnoe posobie* [Psychodiagnostics of personality: a textbook]. Tol'iatti, Izd-vo TGU, 2012. 270 p.

8. *Test Kettella, 16PF/A* [Kettell test, 16PF/A]. Available at: https://psytests.org/result?v=ctlA1S4whsl1T-dyg0IulTUD8K&pp=1 (accessed: 20.12.2023).

9. Sidorenko E. V. *Metody matematicheskoi obrabotki v psikhologii* [Methods of mathematical processing in psychology]. Saint Petersburg, Rech' Publ., 2010. 350 p.

10. Karpasiuk I. V., Karpasiuk A. I. Moshennichestvo v IB-sfere i psikhologiia zhertvy: osobennosti i vzaimosviazi [Fraud in the information security sphere and the psychology of the victim: features and relationships]. *Zashchita informatsii. Insaid*, 2022, no. 3 (105), pp. 41-49.

11. Vlasova N. V., Buslaeva E. L. Psikhologicheskie osobennosti lits, sklonnykh k kiberviktimnomu povedeniiu [Psychological characteristics of individuals prone to cyber victim behavior]. *Psikhologiia i pravo*, 2022, vol. 12, no. 2, pp. 194-206.

Статья поступила в редакцию 22.01.2024; одобрена после рецензирования 11.03.2024; принята к публикации 04.04.2024
The article was submitted 22.01.2024; approved after reviewing 11.03.2024; accepted for publication 04.04.2024

Информация об авторах / Information about the authors

Игорь Владимирович Карпасюк – кандидат физико-математических наук, доцент; доцент кафедры высшей и прикладной математики; Астраханский государственный технический университет; ikarpasyuk@mail.ru

Igor V. Karpasyuk – Candidate of Physico-Mathematical Sciences, Assistant Professor; Assistant Professor of the Department of Higher and Applied Mathematics; Astrakhan State Technical University; ikarpasyuk@mail.ru

Александр Игоревич Карпасюк – студент, направление обучения «Информационная безопасность»; Астраханский государственный технический университет; akarpasyuk@mail.ru

Надежда Валерьевна Давидюк – кандидат технических наук, доцент; заведующий кафедрой информационной безопасности; Астраханский государственный технический университет; davidyuknv@bk.ru

Елена Витальевна Чертина – кандидат технических наук, доцент; доцент кафедры высшей и прикладной математики; Астраханский государственный технический университет; saprikinae_1912@mail.ru

Alexander I. Karpasyuk – Student, training area "Information Security"; Astrakhan State Technical University; akarpasyuk@mail.ru

Nadezhda V. Davidyuk – Candidate of Technical Sciences, Assistant Professor; Head of the Department of Information Security; Astrakhan State Technical University; davidyuknv@bk.ru

Elena V. Chertina – Candidate of Technical Sciences, Assistant Professor; Assistant Professor of the Department of Higher and Applied Mathematics; Astrakhan State Technical University; saprikinae_1912@mail.ru