УДК 159.9

Психологическая структура кибервиктимности как угроза безопасности личности и государству

Екатерина Ивановна Ильянкова[1]✉, Светлана Николаевна Реховская[2], Елена Алексеевна Варфоломеева[3]
[1]Санкт-Петербургский университет МВД России, Санкт-Петербург, Россия
[2,3]Санкт-Петербургская академия Следственного комитета, Санкт-Петербург, Россия,
[1]ekaterinapogodina@yandex.ru✉, SPIN-код: 2490-5023
[2]svetrex@gmail.com, SPIN-код: 9497-7942
[3]velena_ea@mail.ru, SPIN-код: 2593-6905

Аннотация. Приведены результаты эмпирического исследования с участием 166 обследуемых. Предметом исследования выступили личностные особенности обследуемых с высоким уровнем кибервиктимности. Авторами выявлена трехкомпонентная психологическая структура кибервиктимности. Ее личностными предикторами являются склонность к импульсивным поступкам, открытость к новым контактам, стремление к взаимодействию, желание установить дружескую связь, подкрепленное доброжелательностью. В когнитивно-поведенческий компонент вошли особенности восприятия и реагирования на потенциальные угрозы: недооценивание рисков, уверенность в собственной неуязвимости, сниженный социальный интеллект. К межличностно-ситуативным факторам относятся излишняя открытость, доверительность, стремление поделиться личной информацией, доброжелательность, которыми могут воспользоваться злоумышленники (межличностный уровень), а также выбор платформ и онлайн-игр, особенности общения, степени погруженности в контент (ситуативный уровень).

Ключевые слова: кибервиктимность, личностные предикторы, психологическая структура кибервиктимности, добросовестность, социальный интеллект, импульсивность

Для цитирования: Ильянкова Е.И., Реховская С.Н., Варфоломеева Е.А. Психологическая структура кибервиктимности как угроза безопасности личности и государству // Правда и закон. 2025. № 4(34). С. 76–84.

The psychological structure of cybercrime as a threat to the security of the individual and the State

Ekaterina I. Ilyankova[1]✉, Svetlana N. Rekhovskaya[2], Elena A. Varfolomeeva[3]
[1]Saint Petersburg university of the Ministry of internal affairs of Russia, St. Petersburg, Russia
[2,3]SK RF SPb Academy, St. Petersburg, Russia
[1]ekaterinapogodina@yandex.ru✉, SPIN: 2490-5023
[2]svetrex@gmail.com, SPIN: 9497-7942
[3]velena_ea@mail.ru, SPIN: 2593-6905

Abstract. The results of an empirical study involving 166 subjects are presented. The subject of the study was the personal characteristics of the subjects with a high level of cyber-vulnerability. The authors have identified a three-component psychological structure of cybervictimity. Her personal predictors are a tendency to impulsive actions, openness to new contacts, a desire for interaction, and a desire to establish a friendly relationship, supported by benevolence. The cognitive-behavioral component includes the features of perception and response to potential threats: underestimation of risks, confidence in one's own invulnerability, reduced social intelligence. Interpersonal and

© Ильянкова Е.И., Реховская С.Н., Варфоломеева Е.А., 2025

situational factors include excessive openness, trust, the desire to share personal information, goodwill, which can be exploited by intruders (interpersonal level) and the choice of platforms, online games, communication features, degree of immersion in content (situational level).

Keywords: cybervictimity, personal predictors, psychological structure of cybervictimity, conscientiousness, social intelligence, impulsivity

For citation: Ilyankova E.I., Rekhovskaya S.N., Varfolomeeva E.A. The psychological structure of cybercrime as a threat to the security of the individual and the State // Truth and law. 2025. № 4(34). P. 76–84.

В сфере киберпреступности наблюдаются существенные изменения в укладе взаимодействия сторон криминального действия, которые все больше выходят за пределы традиционных отношений «преступник–жертва». Открытая агрессия и прямое столкновение уступают место более сложным формам. Ключевой становится «философия умиротворения» – отказ от прямого воздействия на потерпевшего, стремление максимально замаскировать свои действия. Это обусловлено несколькими причинами.

Во-первых, прямое воздействие в киберпространстве легче отслеживается и вызывает быстрые ответные меры. Во-вторых, маскировка действий позволяет достичь более широкого охвата и минимизировать риск разоблачения. Отсутствие явной угрозы и иллюзия безопасности создают «идеальные» условия для противоправных посягательств. Анонимность снижает чувство ответственности, повышает безнаказанность преступника, а отсутствие прямого контакта провоцирует ощущение беспомощности у потерпевшего.

Кибервиктимность рассматривается не только как пассивное состояние жертвы, но и как потенциально активный процесс преодоления. При кибервоздействии естественной реакцией становится желание ответить агрессией, отомстить обидчику. Однако, если не справиться с этим порывом, он втягивает жертву в цикл эскалации конфликта и разрушает ее эмоциональное равновесие. Кибервиктимность – состояние, при котором негативные последствия деструктивного кибервоздействия усиливаются. Обида, желание отомстить, страдания, чувство злости, тревоги, снижение самооценки и депрессии, как ни парадоксально, являются факторами, способствующими повторению деструктивного онлайн-воздействия [1].

Значимыми предикторами кибервиктимности называют повышенный нейротизм, тревожность, эмоциональную неустойчивость и негативные переживания в сочетании с направленностью на новый опыт и добросовестностью. Жертвы киберпосягательств эмоционально уязвимые, зависимые от стороннего мнения, склонные к поиску впечатлений, открытые для онлайн-взаимодействия и менее организованные [2]. Карпасюк И.В., Карпасюк А.И. обращают внимание на роль в кибервиктимности повышенного нейротизма и тревожности; склонности к переживанию негативных эмоций; страха; неуверенности; низкой доброжелательности; склонности к враждебности, цинизму и недоверию к другим, излишней подозрительности, ожидания худшего; высокой открытости новому опыту; потребности в одобрении; низкой самооценки и неуверенности в себе [3].

Wong R.Y.M., Cheung C.L.K., Xiao B. предложили модель трех «I» для изучения кибервиктимности при совершении онлайн-преступлений сексуального характера, охватывающую компоненты:

1) «подстрекательство» (провокационные сообщения, негативные комментарии, размещение личной информации и пр.);

2) «имплементация» (описывает механизмы перехода к реальному действию);

3) «торможение» (включает факторы, снижающие вероятность или интенсивность киберпреследования – индивидуальные моральные принципы, эмпатия, чувство ответственности, страх, социальные и правовые нормы и т.д.) [4].

Рассматривая кибервиктимность через призму концепции рефлексивности, можно предположить, что лица с пониженной личностной самооценкой и метарефлексией более склонны к кибервиктимизации [5]. Недостаточная самооценка и трудности с адекватной оценкой рисков, характерные для сниженной рефлексивности, приводят к неосознанному поиску внешнего подтверждения своей ценности в интернете, затрудняют понимание поведения и намерений злоумышленников.

В эмпирическом исследовании приняли участие 166 обследуемых в возрасте от 22 до 55 лет. Психодиагностический инструментарий:

– шкала кибервиктимизации Д.В. Жмурова [6];

– методика «Рефлексивная оценка потенциальной индивидуальной виктимности» И.А. Дмитриевой, И.А. Кибальченко;

– опросник по шестифакторной модели личности K. Lee, M. Ashton;

– Франкфуртские шкалы самооценки M. Deusinger;

– опросник «Способы совладающего поведения» R. Lazarus, S. Folkman.

Для выявления значимых связей и закономерностей применены дескриптивный, кластерный, сравнительный (U-критерий Манна-Уитни), корреляционный (r-критерий Спирмена) виды анализа.

В ходе кластерного анализа (табл. 1) результатов обследования при помощи Шкалы кибервиктимизации сформированы две группы респондентов:

1) с умеренной и высокой кибервиктимностью (n = 86; возраст: 48,28 ± 2,19);

2) с низкой кибервиктимностью (n = 80; возраст: 48,07 ± 8,30).

Таблица 1

Данные кластерного анализа

Начальные центры кластеров		
	Кластер	
Название показателя	Респонденты с умеренной и высокой кибервиктимностью (n = 86)	Респонденты с низкой кибервиктимностью (n = 80)
Кибервиктимизация	83	43
Конечные центры кластеров		
Кибервиктимизация	70,64 ± 5,46	56,55 ± 10,58

Психологический портрет личности при умеренной или высокой кибервиктимности характеризуется сочетанием провоцирующего поведения и недостаточных защитных механизмов. Они раскрывают личную информацию, участвуют в рискованных онлайн-акциях, высказывают провокационные суждения и реагируют на определенный контент. Их защитные стратегии не обеспечивают эффективное противостояние вероятным угрозам (рис. 1).



Рис. 1. Соотношение показателей кибервиктимности, выделенных в группах респондентов с высокой и низкой кибервиктимностью

Для выявления специфических особенностей лиц с высокой кибервиктимностью применен сравнительный анализ с использованием непараметрического критерия Манна-Уитни (табл. 2).

Таблица 2

Данные сравнительного анализа показателей кибервиктимности

№	Название показателя	Группа 1		Группа 2		Uэмп	p
		M	Sd	M	Sd		
1	Провоцирующее поведение	27,75	4,19	21,94	4,75	112,500	0,001*
2	Защитные стратегии	16,69	2,90	13,42	3,19	203,000	0,001*
3	Цифровая погруженность	12,58	1,30	10,94	2,05	220,500	0,001*
4	Опыт предыдущей кибервиктимизации	13,61	2,05	10,39	2,26	78,500	0,001*
5	Шкала кибервиктимизации	70,64	5,49	56,55	10,58	10,000	0,001*

Склонность к провоцирующему поведению вызывает ответное поведение со стороны других пользователей ($U = 112{,}50$, $p \leq 0{,}01$). Сниженная осторожность в высказываниях и действиях в сети повышает уязвимость и способствует включению в онлайн-конфликты ($U = 203{,}00$, $p \leq 0{,}01$). Высокая цифровая погруженность, большее количество контактов с другими пользователями и личной информации, доступной в сети, создает значительное число возможностей для преступного посягательства ($U = 220{,}50$, $p \leq 0{,}01$). Активное использование социальных сетей, онлайн-игр и иных онлайн-сервисов увеличивает вероятность столкнуться с нарушением прав ($U = 78{,}50$, $p \leq 0{,}01$). Выраженное использование защитных стратегий указывает на повышенную тревожность и озабоченность вопросами безопасности в сети ($U = 10{,}00$, $p \leq 0{,}01$).

Для изучения значимых взаимосвязей применен корреляционный анализ (табл. 3).

Таблица 3

Значимые корреляционные связи показателей кибервиктимности, потенциальной виктимности, личностных свойств, самооценки и копинг-стратегий, выделенных в группе респондентов с высокой кибервиктимностью

	Провоц. поведение	Защит. стратегии	Цифр. погружен.	Опыт пред. кибер-виктими-зации	Шкала кибер-виктими-зации
	Потенциальная виктимность				
Индивидуальная потенциальная виктимность	,343*				0,441**
	Личностные особенности				
Честность/ Скромность	-,381*				
Эмоциональность	,479**	,341*			
Экстраверсия	,417*				
Доброжелательность	,353*				
Добросовестность				,369*	
Открытость опыту			-,451**		
Уверенность в собственных решения					-,416*
Общая самоценность					-,437**
Настроение и впечатлительность		,341*			
Контактность и общительность		,341*			
Чувства и отношение к другим	-,525**	,445**			
	Копинг-стратегии				
Дистанцирование					,362*
Самоконтроль			,366*		

Положительная корреляция индивидуальной потенциальной виктимности с общим уровнем кибервиктимности (r = 0,441**) свидетельствует о ее переносе из реальной в онлайн-среду. Потенциальная виктимность положительно связана с провоцирующим поведением (r = 0,343*). Отсутствие значимых связей с защитными стратегиями и цифровой погруженностью при умеренной корреляции с опытом предыдущей кибервиктимизации подчеркивает, что сама по себе потенциальная виктимность не гарантирует использования адекватных защитных мер.

Личностные качества играют важную роль в формировании кибервиктимности. Более эмоциональные (r = 0,479) и общительные (r = 0,417) чаще проявляют рискованное поведение в сети. Доброжелательность (r = 0,353) положительно связана с провоцирующим поведением, указывая на стремление к установлению контактов, выходящее за нормативные рамки. Честность/скромность (r = 0,381) выступают в качестве защитных факторов, снижающих риск провоцирования преступного посягательства. Открытость опыту (r = -0,451)

отрицательно коррелирует с погруженностью в цифровые технологии, а уверенность в собственных решениях (r = -0,416) и общая самоценность (r = -0,437) отрицательно связаны с опытом предыдущей кибервиктимизации. Настроение и впечатлительность, а также контактность и общительность положительно коррелируют с эмоциональностью (r = 0,341*), указывая на связь между этими личностными аспектами и общей склонностью к эмоциональным реакциям и взаимодействию, которые могут влиять на кибервиктимность. Чувства и отношение к другим отрицательно коррелируют с провоцирующим поведением (r = -0,525) и положительно – с защитными стратегиями (r = 0,445): эмпатия и позитивное отношение к другим способствуют безопасному и продуманному поведению в сети.

Люди, пережившие киберпосягательство, начинают дистанцироваться от онлайн-взаимодействия (r = 0,362). Самоконтроль положительно коррелирует с погруженностью в цифровые технологии (r = 0,366). Косвенное влияние защитных стратегий подтверждается их связью с чувствами и отношением к другим (r = 0,445).

Психологическая структура кибервиктимности объединяет личностную уязвимость, ситуативные факторы и особенности взаимодействия с цифровой средой (рис. 2).



Рис. 2. Психологическая структура кибервиктимности

К личностным предикторам кибервиктимности следует отнести склонность к импульсивным поступкам, открытость к новым контактам, стремление к взаимодействию, желание установить дружескую связь, подкрепленное доброжелательностью. В этом проявляется склонность к провоцирующему поведению. Высокий социальный интеллект, эмпатия являются ценными качествами, которые проявляются в более продуманном и безопасном поведении в сети. Они способствуют не только осторожности, но и активному использованию средств защиты. Интересно, что даже опыт пережитой кибератаки становится катализатором поведенческих

изменений. Такие люди зачастую начинают избегать онлайн-взаимодействия, что является естественной реакцией на негативный опыт и своеобразной формой защиты, хоть и ограничивающей.

Когнитивно-поведенческий компонент определяет особенности восприятия и реагирования на потенциальные угрозы. Именно восприятие рисков, их осознание и оценка, становится первым «фильтром», через который проходит информация об опасностях в цифровом мире. Недооценивание рисков, уверенность в собственной неуязвимости, сниженный социальный интеллект определяют излишнюю открытость к опасным ситуациям [7]. Активные стратегии совладания проявляются в стремлении к поиску способов укрепления своей безопасности, анализу прошлого опыта и прогнозированию возможных сценариев развития событий в сети. Активная позиция определяет готовность к когнитивным усилиям, связанным с пониманием угроз, и устойчивость к соблазнам, которые могут подорвать безопасность (например, желание поделиться информацией ради вознаграждения или одобрения).

С другой стороны, осторожное избегание, основанное на интуитивном или осознанном снижении вероятности столкновения с риском, выражается в личной осторожности, предпочтении более безопасных форм взаимодействия. Такая стратегия обусловлена опытом прошлых неудач, склонностью к предусмотрительности и осознанием собственной уязвимости.

Индивидуальная виктимность проецируется из реального мира в онлайн-среду, определяя межличностную и ситуационную проекцию рисков. Поведенческие модели, невербальные сигналы и общая восприимчивость к манипуляциям, определяющие уязвимость в реальной жизни, становятся активными в онлайн-ситуациях. Данный компонент проявляется в поведении, которое способно привлечь внимание злоумышленников [8]. На межличностном уровне это излишняя открытость, доверительность, стремление поделиться личной информацией, доброжелательность, которыми могут воспользоваться злоумышленники. На ситуативном уровне такое поведение проявляется в выборе платформ, онлайн-игр, особенностях общения, степени погруженности в контент, которые сами по себе могут создавать благоприятные условия для кибервоздействия.

Таким образом, в психологической структуре кибервиктимности личностные особенности демонстрируют закономерную связь с подверженностью деструктивному онлайн-воздействию. Личностные черты (открытость опыту, уверенность в собственной неуязвимости, сниженный социальный интеллект, эмоциональность, доброжелательность, общительность и др.), индивидуальные стратегии совладания формируют психологический профиль, предопределяющий предрасположенность к кибервиктимизации. Противоречия в полученных эмпирических результатах различных исследователей о выявленных личностных предикторах кибервиктимности требуют дальнейшего детального изучения поднятой проблемы.

Многоуровневая система внутренних и внешних факторов, обусловливающих повышенную уязвимость личности в киберпространстве, формирует комплексную угрозу для безопасности как личности, так и государства. Понимание и нейтрализация психологических предпосылок кибервиктимности на уровне личности становятся необходимым условием повышения устойчивости государства к современным киберугрозам.

Список источников

1. Галиев Д.З., Беловол Е.В. Онлайн-активность и рискованное поведение как факторы кибервиктимности подростков // Живая психология. 2025. Т. 12. № 4(60). С. 12–19.

2. Вихман А.А., Волкова Е.Н., Скитневская Л.В. Традиционные и цифровые возможности профилактики кибербуллинга // Вестник Мининского университета. 2021. Т. 9. № 4. С. 10.

3. Карпасюк И.В., Карпасюк А.И. Математическая модель определения степени склонности к подверженности киберпреступлению // Вестник Дагестанского государственного технического университета. Технические науки. 2025. № 52(1). С. 87–96.

4. Won R.Y.M., Cheung C.L.K., Xiao B. Does gender matter in cyberbullying perpetration? An empirical investigation // Computers in Human Behavior. 2018. № 79. P. 247–257.

5. Карпов А.В. Рефлексивность как психическое свойство и методика ее диагностики // Психологический журнал. 2003. Т. 24. № 5. С. 45–57.

6. Жмуров Д.В. Кибервиктимность как новая категория виктимологии постмодерна // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 2. С. 113–122.

7. Вахнина В.В. Информационно-психологическая безопасность как условие формирования правового сознания, профилактики девиантного и противоправного поведения // Вестник Санкт-Петербургской академии Следственного комитета. 2024. № 1. С. 65–70.

8. Ефимова И.В. Девиантные формы поведения, реализуемые в цифровом пространстве // Вестник Санкт-Петербургской академии Следственного комитета. 2024. № 2. С. 39–44.

References

1. Galiev D.Z., Belovol E.V. Onlajn-aktivnost' i riskovannoe povedenie kak faktory kiberviktimnosti podrostkov // Zhivaya psihologiya. 2025. T. 12. № 4(60). S. 12–19.

2. Vihman A.A., Volkova E.N., Skitnevskaya L.V. Tradicionnye i cifrovye vozmozhnosti profilaktiki kiberbullinga // Vestnik Mininskogo universiteta. 2021. T. 9. № 4. S. 10.

3. Karpasyuk I.V., Karpasyuk A.I. Matematicheskaya model' opredeleniya stepeni sklonnosti k podverzhennosti kiberprestupleniyu // Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki. 2025. № 52(1). S. 87–96.

4. Won R.Y.M., Cheung C.L.K., Xiao B. Does gender matter in cyberbullying perpetration? An empirical investigation // Computers in Human Behavior. 2018. № 79. R. 247–257.

5. Karpov A.V. Refleksivnost' kak psihicheskoe svojstvo i metodika ee diagnostiki // Psihologicheskij zhurnal. 2003. T. 24. № 5. S. 45–57.

6. Zhmurov D.V. Kiberviktimnost' kak novaya kategoriya viktimologii postmoderna // Aziatsko-Tihookeanskij region: ekonomika, politika, pravo. 2021. № 2. S. 113–122.

7. Vahnina V.V. Informacionno-psihologicheskaya bezopasnost' kak uslovie formirovaniya pravovogo soznaniya, profilaktiki deviantnogo i protivopravnogo povedeniya // Vestnik Sankt-Peterburgskoj akademii Sledstvennogo komiteta. 2024. № 1. S. 65–70.

8. Efimova I.V. Deviantnye formy povedeniya, realizuemye v cifrovom prostranstve // Vestnik Sankt-Peterburgskoj akademii Sledstvennogo komiteta. 2024. № 2. S. 39–44.

Статья поступила в редакцию 02.11.2025; одобрена после рецензирования 05.12.2025; принята к публикации 08.12.2025.
The article was submitted 02.11.2025; approved after reviewing 05.12.2025; accepted for publication 08.12.2025.

Информация об авторах
Е.И. Ильянкова – кандидат психологических наук, преподаватель кафедры юридической психологии Санкт-Петербургского университета МВД России (Россия, 198206, г. Санкт-Петербург, ул. Летчика Пилютова, 1);
С.Н. Реховская – кандидат психологических наук, доцент кафедры юридической психологии и педагогики Санкт-Петербургской академии Следственного комитета (190000, г. Санкт-Петербург, наб. р. Мойки, 96);
Е.А. Варфоломеева – кандидат психологических наук, доцент кафедры юридической психологии и педагогики Санкт-Петербургской академии Следственного комитета (190000, г. Санкт-Петербург, наб. р. Мойки, 96).

Information about the authors
E.I. Ilyankova – Candidate of Psychological Sciences, Lecturer at the Department of Legal Psychology of the St. Petersburg University of the Ministry of Internal Affairs of Russia (Russia, 198206, St. Petersburg, St. Pilyutova Pilot, 1);
S.N. Rekhovskaya – Candidate of Psychological Sciences, Associate Professor of the Department of Legal Psychology and Pedagogy of the SK RF SPb Academy (Russia, 190000, St. Petersburg, nab. r. Moika, 96);
E.A. Varfolomeeva – Candidate of Psychological Sciences, Associate Professor of the Department of Legal Psychology and Pedagogy of the SK RF SPb Academy (Russia, 190000, St. Petersburg, nab. r. Moika, 96).