Научный сетевой журнал
МЕДИЦИНСКАЯ ПСИХОЛОГИЯ В РОССИИ

ОСОБЕННОСТИ ВОСПРИЯТИЯ ИНФОРМАЦИОННЫХ УГРОЗ ПРИ ПАРАНОИДНОЙ ШИЗОФРЕНИИ

***Цыганкова П.В.*[1], *Бурняшева А.М.*[2]**

[1] *Цыганкова Полина Васильевна*

кандидат психологических наук, доцент кафедры клинической психологии психолого-социального факультета; федеральное государственное автономное образовательное учреждение высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации, ул. Островитянова, 1, Москва, 117997, Россия. Тел.: 8 (495) 434-54-29.

E-mail: polina_tsy@mail.ru

2 *Бурняшева Анастасия Михайловна*

клинический психолог.

E-mail: contact.cycle@yandex.ru

Аннотация. Целью исследования является изучение особенностей восприятия информационных угроз при параноидной шизофрении. Актуальность исследования обоснована увеличением разнообразия и распространенности в современном обществе информационных угроз, сходством содержания и механизмов реализации информационных угроз с симптоматикой параноидной шизофрении и недостаточной изученностью влияния современных технологических изменений на протекание психических расстройств. Клиническую группу составили 30 больных параноидной шизофренией вне острого состояния, без когнитивного дефекта (15 мужчин, 31,8 ± 5,6 лет), контрольную группу — 30 психически здоровых испытуемых (15 мужчин, 31,3 ± 6,9 лет). В исследовании использована авторская методика «Восприятие информационных угроз», состоящая из 5 видеороликов, созданных на материале художественных фильмов и демонстрирующих ситуации информационных угроз (кража и подмена персональных данных, слежка через персональные устройства злоумышленником/госструктурами, трансляция личной жизни в Интернете), а также структурированное интервью. Проведен качественный анализ ответов. Для выявления межгрупповых различий в частотах ответов использован критерий хи-квадрат Пирсона. Выявлены значимые межгрупповые различия в восприятии информационных угроз: больные параноидной шизофренией значимо чаще, чем психически здоровые люди, игнорируют наличие угрозы и злонамеренность показанных действий; чаще прогнозируют однозначный исход событий; недооценивают риск информационных угроз в реальной жизни и не склонны предпринимать меры по защите от них. Обосновывается необходимость разработки и применения программ психологического просвещения больных параноидной шизофренией, тренингов навыков обеспечения личной информационной безопасности.

Ключевые слова: параноидная шизофрения; информационные угрозы; киберугрозы; информационная безопасность; восприятие информационных угроз.

УДК 159.937.3:616.895.8

Библиографическая ссылка

Цыганкова П.В., Бурняшева А.М. Особенности восприятия информационных угроз при параноидной шизофрении // Медицинская психология в России. – 2021. – Т. 13, № 1. – С. 8. doi: 10.24412/2219-8245-2021-1-8

Поступила в редакцию: 17.01.2021 Прошла рецензирование: 17.02.2021 Опубликована: 20.03.2021

Введение

В современном информационном обществе жизненное пространство человека виртуализируется, всё большую роль в его жизнедеятельности играют киберресурсы и процессы виртуальной социальной коммуникации [1]. Формируется «всеобъемлющая цифровая реальность» [9], оформляется пространство нового типа — киберпространство, к которому на сегодняшний день с помощью электронных устройств имеет доступ большая часть человечества [1; 9]. Д.Е. Добринская (2018) называет киберпространство «новой средой обитания современного человека» и отмечает такие его качества, как глобальность, повсеместность, сетевая структура, децентрация, а также подвижность, изменчивость, размытость границ. Автор указывает, что каждый индивид является частью этой среды независимо от своей воли и желания [9].

Способы поступательного внедрения информационно-коммуникационных технологий в обыденную жизнь и профессиональную деятельность человека многочисленны и разнообразны: от гипертекстуализации городской среды (мобильные карты и путеводители, приложения, облегчающие пользование общественным и личным транспортом, онлайн-бронирование различных услуг) до оценки состояния физического здоровья с помощью гаджетов, от онлайн-покупок до дистанционного образования, от возможности делиться со всем миром своими впечатлениями и мыслями в режиме реального времени до адресной рекламы и возможности индивидуализации информационного контента в соответствии с личной системой убеждений и предпочтений [14].

В киберпространстве закономерно трансформируется самопрезентация и самореализация личности. Ученые активно обсуждают содержание таких понятий, как «сетевая идентичность», «виртуальная идентичность», «мобильная идентичность», «электронная идентичность», «цифровая идентичность», придерживаясь порой диаметрально противоположных взглядов. Хотя некоторые авторы считают, что виртуальное пространство способствует формированию стабильной идентичности, многие характеризуют ее как нестабильную, множественную, размытую, гибкую, фрагментированную, зыбкую, динамичную и мобильную [15].

Проблема информационных угроз в современном обществе

Помимо безграничных возможностей информационные технологии создают и разного рода информационные угрозы, средства защиты от которых как общества в целом, так и каждого конкретного индивида в частности оказываются недостаточными.

Исчерпывающий список информационных угроз составить невозможно в связи с крайне высокой скоростью развития технологий, за которыми не успевает научная мысль, однако попытки их систематизации существуют. Например, C.Y. Lee (2009) выделяет 10 специфических угроз, связанных с использованием киберпространства и виртуальными коммуникациями: нарушение конфиденциальности и вторжение в частную жизнь; кража идентичности; кража интеллектуальной собственности; кибербуллинг, киберхарассмент и сталкинг; преднамеренный обман (клевета); спам; вторжение в область финансовых транзакций онлайн; вредоносное компьютерное обеспечение и компьютерные вирусы; инвестиционные аферы и жульничество; виртуальные преступления (т.е. преступления в виртуальных мирах, например многопользовательских онлайн-играх) [29].

Классификация киберугроз психологической безопасности взрослого человека отечественного психолога Р.М. Айсиной (2019) включает в себя: 1) угрозы, связанные с веб-контентом (информация деструктивного характера, информация низкого качества и искаженная информация — «фейк»); 2) угрозы, связанные с виртуальными социальными коммуникациями (троллинг, кибербуллинг, киберсталкинг, дранкшейминг, попытки вовлечения в девиантную активность); 3) угрозы, связанные с избыточным присутствием в киберпространстве (проблемы саморегуляции при использовании киберресурсов, чрезмерная вовлеченность в ролевые игры с риском искажения идентичности, ослабление связи с реальностью) и 4) угрозы, связанные с незащи-

щенностью персональных данных пользователя (кэтфишинг, кража интеллектуальной собственности, взлом личного фото- и видеоархива) [1].

В.А. Емелин является современным отечественным философом, наиболее активно исследующим проблему «оборотной стороны» информационных технологий. Он полагает, что техника и технологии становятся продолжением человеческого сознания и тела, размывая границы его идентичности и формируя новые потребности. Технологии дают человеку новые формы контроля над миром, но при этом он сам контролируется с помощью тех же технологических расширений. Автор остро ставит проблему приватности, называя технологические устройства «точками входа» в личное пространство индивида, открывающими власти и корпорациям новые возможности для манипуляций и контроля на уровне его обыденной жизни. Человек оставляет в киберпространстве не только свой «цифровой след» (ту информацию, которую он размещает добровольно), но и «цифровую тень» — информацию, которая создается автоматически, без ведома самого человека. Выстраивается система тотального цифрового мониторинга, контроля и управления обществом, человек, пользующийся электронными гаджетами, оказывается помещенным в «глобальный паноптикум» [11].

Сочетание тотальности и незаметности цифрового контроля, по мнению В.А. Емелина, может привести человека в состояние постоянного страха, напряженности [10]. А.Е. Войскунский, один из ведущих российских исследователей психологии интернета, считает безопасность, в том числе безопасность в киберпространстве, фундаментальной человеческой потребностью, фрустрация которой может иметь значительные негативные последствия для психического развития и психологического здоровья индивидуума и социума. Автор подчеркивает важность развития «киберэтики» с целью решения ряда актуальных морально-нравственных проблем, порожденных развитием технологий, среди которых — меры противодействия порнографии, педофилии, сексуальным домогательствам посредством интернета, всем разновидностям плагиата, пиратства и нарушений авторского права, проявлениям хакерства, кибершантажа, киберпреследования и мн. др. [6].

В целом можно отметить, что проблемы информационной безопасности находятся в поле внимания современных отечественных философов [8; 13; 23], юристов [3; 16; 22], социологов [2; 17; 19; 21], однако являются предметом эмпирических исследований в психологии сравнительно редко.

Роль информационных технологий для больных шизофренией

С психологической точки зрения есть основания для проведения аналогии между ситуацией воздействия информационных угроз на индивида и симптоматикой, характерной для параноидной шизофрении.

Для параноидной шизофрении, находящейся в фокусе внимания данного исследования, типичными являются галлюцинаторно-параноидные и бредовые переживания с преобладанием бреда преследования, а также симптом открытости мыслей [18]. Психоанализ объясняет возникновение параноидных переживаний проекцией больным на внешние объекты своих собственных отрицаемых разрушительных импульсов [20]. Такая примитивная проекция возможна лишь при несформированности, слабости границ Я, о чем писал ещё в 1918 г. Виктор Тауск (Victor Tausk) в своей работе «О возникновении "аппарата влияния" при шизофрении», что в дальнейшем получило развитие, в частности, в работах П. Федерна и Б. Лэндиза [7].

В.А. Емелин проводит аналогию между нарушением границ идентичности вторгающимися в личное пространство человека современными технологиями и непрочностью границ идентичности при психотической личностной организации с риском возникновения психотических переживаний [10], однако эмпирические исследования влияния информационных угроз на психическое функционирование больных шизофренией отсутствуют. В 2004 г. B. Schmid-Siegel и колл. опубликовали статью под заголовком «Быть веб-камерой», в которой изложили клинический случай

молодой женщины, включившей Интернет в свою бредовую систему. Авторы описали симптом, названный ими «трансляцией восприятия» и имеющий более сложную структуру, чем симптом «открытости мыслей» [32]. Подобные случаи могут служить подтверждением предположения, что современные технологии могут влиять на протекание психических заболеваний.

Большинство эмпирических исследований, однако, посвящены позитивному влиянию информационных технологий, особенно социальных сетей, на состояние больных шизофренией, включая снижение социальной изоляции и совладание с симптомами [24; 26; 28; 31]. Лишь в единичных публикациях упоминаются потенциальные риски и недостаточность навыков использования интернета у больных шизофренией [27; 34].

Специфика восприятия угроз и оценки рисков при шизофрении

Данные о восприятии больными шизофренией угрожающих стимулов скудны и противоречивы, существуют свидетельства в пользу склонности больных как к переоценке, так и к недооценке опасности. Для пациентов с шизотипическим расстройством и ультравысоким риском психоза характерны предвзятые стили атрибуции — приписывание враждебного намерения невинным другим и возложение вины [25]. При восприятии неопределенного стимульного материала проективного теста Роршаха для больных с расстройствами шизофренического спектра характерны специфические механизмы парадоксального структурирования информации, аналогичные механизмам кристаллизации бреда, выполняющие роль компенсаторного разрешения эндогенной психотической тревоги, ее опредмечивания и канализации [12]. У подростков с шизофренией и шизотипическим расстройством выявлено повышение уровня субъективной опасности при восприятии фотографий потенциально опасных мест и ситуаций, в том числе с привнесением элементов фабулы бреда [4]. В исследовании зарубежных коллег J. Henry с соавт. также была выявлена склонность больных шизофренией приписывать ситуациям более высокий уровень опасности, чем в контрольной группе, однако не было выявлено различий между психически здоровыми и психически больными людьми по способности различать стимулы с высокой и низкой опасностью и в степени опасности, приписываемой выражениям лиц [33]. В то же время имеются нейрофизиологические данные об отсутствии у больных шизофренией адекватной реакции на значимую угрозу для благополучия и даже выживания [5], а также данные о том, что больным шизофренией в той же мере, что и психически здоровым людям, присущ нереалистичный оптимизм при оценке личного риска, т.е. склонность полагать, что вероятность неблагоприятных событий для них ниже, чем для других людей [30].

Таким образом, имеющихся данных недостаточно для того, чтобы оценить специфику восприятия больными шизофренией информационных угроз и степень адекватности реагирования на них, что обуславливает актуальность представленного исследования. Его целью стало изучение особенностей восприятия информационных угроз при параноидной шизофрении, которое предположительно имеет неадекватный, искаженный характер.

Материалы и методы

С целью исключения из выборки испытуемых с когнитивным дефектом было проведено патопсихологическое исследование с использованием методик «Исключение понятий», «Сравнение понятий», «Толкование пословиц».

Для выявления особенностей восприятия угроз, опосредованных использованием информационных технологий, разработана авторская методика «Восприятие информационных угроз». Методика включает в себя 5 видеороликов продолжительностью 7—10 минут каждый, созданных путем нарезки видеофрагментов художественных фильмов соответствующей тематики:

1) «Сеть» («The Net», реж. И. Уинклер, 1995). Показана ситуация кражи и подмены персональных данных героини через Интернет.
2) «Крыса» («Ratter», реж. Б. Крамер, 2015). Показана ситуация слежения за героиней с ее персональных информационных устройств (ноутбука, телефона, стационарного компьютера).
3) «Сфера» («The Circle», реж. Дж. Понсольдт, 2017). Показана ситуация добровольной круглосуточной трансляции личной жизни девушки широкой публике через Интернет.
4) серия «Заткнись и танцуй» («Shut Up and Dance»), 3-го сезона сериала «Черное зеркало» («Black Mirror») (реж. Дж. Уоткинс; 2016). Показана ситуация управления поведением молодого человека через мобильный телефон и компьютер посредством шантажа о разглашении личной информации, добытой незаконным путём.
5) «Сноуден» («Snowden», реж. О. Стоун, 2016). Показана ситуация отслеживания государственным служащим граждан через персональные информационные устройства с помощью специально разработанных программ с целью оказания давления и манипулирования.

Видеофрагменты предъявлялись в случайном порядке. После просмотра каждого ролика с участниками проводилось структурированное интервью, направленное на оценку понимания ими показанного сюжета и отношения к показанным событиям. Были заданы следующие вопросы:

1. Что произошло в показанном вам видео?
2. Как вы думаете, кто совершил показанные действия и с какой целью?
3. Как вы считаете, как будут развиваться события дальше? Чем всё кончится?
4. Как бы вы поступили на месте главного героя/героини, если бы оказались в его/ее положении?
5. Могут ли такие события произойти в реальности?
6. Можно ли было обезопасить себя от попадания в подобную ситуацию/ от показанной угрозы?

После завершения показа видеороликов проводилась вторая часть интервью, посвященная проблеме информационных угроз в реальной жизни, вне связи с сюжетами фильмов. Были заданы вопросы:

1. Существуют ли информационные угрозы в реальности? Представляют ли они реальную опасность?
2. Сталкивались ли вы лично или кто-то из вашего окружения с угрозами, исходящими от информационных технологии? Какие это были ситуации?
3. Как вы или знакомые вам люди выходили из этих ситуаций?
4. Известны ли вам способы защиты от информационных угроз? Какие?
5. Защищаетесь ли вы сейчас от информационных угроз? Как?

Для оценки ответов участников был проведен качественный анализ и разработана система категорий ответов по каждому вопросу. С целью выявления статистически значимых межгрупповых различий в частоте ответов каждой категории использовался статистический критерий хи-квадрат Пирсона.

Характеристика выборки

В исследовании приняли участие 60 человек, составивших 2 группы: клиническую и контрольную.

Клиническую выборку составили больные параноидной шизофренией (F 20.0, согласно МКБ-10) в количестве 30 человек (15 мужчин), 20—40 лет, средний возраст — 31,8 ± 5,6 лет. Критериями исключения из группы были острое психотическое состояние и наличие когнитивного дефекта. Клинической базой являлся ФГБНУ «Научный центр психического здоровья».

Контрольную группу составили 30 психически здоровых участников (15 мужчин), 21—40 лет, средний возраст — 31,3 ± 6,9лет.

Как в клиническую, так и в контрольную группу отбирались участники, не смотревшие ранее использованные для создания видеороликов фильмы.

Результаты исследования

Для проведения качественного и количественного анализа содержания ответов участников на вопросы структурированного интервью разработана система критериев. Ответы на каждый из вопросов отнесены к определенной категории, после чего осуществлен подсчет и статистическое сравнение их частот.

1. Правильность понимания сюжета

Ответы на вопрос *«Что произошло в показанном вам видео?»* оценивались на основе соответствия сюжету фильма и были разделены на три категории:

1. ***Верное понимание:*** участник понимает наличие намеренной и целенаправленной угрозы благополучию, статусу, физическому или психическому здоровью главного героя, опосредованной информационными технологиями, верно оценивает источник угрозы и способ ее реализации.
2. ***Частичное понимание:*** участник осознает факт наличия информационной угрозы в отношении главного героя, однако неправильно определяет ее источник, искаженно трактует намерения субъекта угрозы или вовсе отрицает намеренность действий, приписывая его не человеку, а техническому устройству.
3. ***Неверное понимание:*** участник отрицает наличие угрозы благополучию, статусу, физическому или психическому здоровью главного героя, опосредованной информационными технологиями, например, расценивает показанное как психопатологическую продукцию или как сон.

В таблице № 1 представлено распределение ответов испытуемых двух групп по описанным категориям.

Таблица 1

Распределение ответов по критерию правильности понимания сюжета

Правильность понимания	Клиническая группа	Группа нормы	Уровень значимости различий
Верное понимание	**119 79%**	**142 95%**	**x^2=17,56 p≤0,01**
Частичное понимание	22 15%	8 5%	Значимые различия не выявлены
Неверное понимание	9 6%	0	

Примечание. В таблице указано абсолютное количество ответов соответствующей категории и процентное соотношение ответов. Статистически значимые различия выделены полужирным шрифтом.

Больные шизофренией значимо реже понимали сюжет роликов верно по сравнению с испытуемыми группы нормы. Участники клинической группы чаще игнорировали наличие угрозы, опосредованной информационными технологиями, в частности утверждали, что главный герой психически болен, а всё происходящее — проявление его психопатологической симптоматики. Например, испытуемый М. Д., муж., 30 лет, объясняет содержание видеоролика по серии сериала «Черное зеркало» так: *«Парень морально неустойчив, пришло ему в голову, что за ним следят: слышит голоса, сообщения какие-то. Психическое расстройство у него»*. В других случаях больные лишь частично понимали смысл видеоролика, игнорируя злонамеренный характер и опосредованность демонстрируемых действий информационными технологиями. Например, испытуемая М. О., жен., 30 лет, следующим образом объясняет содержание видеоролика по фильму «Сеть»: *«Хотят посадить ее, обвиняют; ложные обвинения, в чем она не виновата»*, не обращая внимания на причину этих событий — намеренное изменение личных данных героини злоумышленником в электронной базе. Нередко больные не понимают, что за действиями частного лица стоит организация или государство или приписывают действия случайным событиям. Например, испытуемая Е. А, жен., 34 года, так объясняет события видеоролика по фильму «Крыса»: *«Какой-то сбой произошел у нее в компьютере и теперь ей приходят сообщения, звонки…»*.

2. Интерпретация цели показанных действий

Ответы участников на вопрос *«Как вы думаете, кто совершил показанные действия и с какой целью?»* разделены на четыре категории:

1. ***Злое намерение частного лица или группы лиц:*** личные мотивы (месть, зависть, стремление к власти, известности, забава, запугивание, самоутверждение) или корыстные мотивы (получение прибыли, проведение эксперимента).
2. ***Злое намерение организации или государства:*** терроризм, отслеживание со стороны государства с целью контроля над гражданами; политическое манипулирование; проведение социального эксперимента, испытание на людях новых технологий.
3. ***Конструктивные намерения:*** стремление субъекта воздействия помочь главному герою, исправить какую-либо ситуацию.
4. ***Отсутствие явного намерения:*** отказ от ответа («не знаю»); восприятие событий как случайных или ненамеренных; восприятие событий как психологической продукции главного героя.

В процессе статистической обработки ответы были сгруппированы в более крупные категории: «наличие злого умысла» и «отсутствие злого умысла». В таблице № 2 представлено распределение ответов испытуемых двух групп по описанным категориям.

Таблица 2

Распределение ответов по критерию интерпретации цели показанных действий

Интерпретация цели показанных действий	Клиническая группа	Группа нормы	Уровень значимости различий
Наличие злого умысла	103 68%	129 86%	$x^2=12,85$ $p\leq0,01$
Отсутствие злого умысла	47 32%	21 14%	

Примечание. В таблице указано абсолютное количество ответов соответствующей категории и процентное соотношение ответов.

Участники с параноидной шизофренией значимо чаще, чем психически здоровые люди, игнорировали злонамеренный характер показанных в видеороликах действий и утверждали, что цель их действий является благой или что определенный мотив их

совершения отсутствует. Например, испытуемая Т. А., жен., 25 лет, объясняет цель показанных в ролике по фильму «Сфера» действий так: *«Это новый гаджет, чтобы жить в современном мире»;* а пациентка П. К., жен., 35 лет высказывает мнение, что цель — *«общение, показать свою жизнь, делиться с окружающими».* Сравним с ответом участника контрольной группы А. Б., муж., 30 лет: *«Из нехорошего умысла это делают, может быть будут потом ее шантажировать собранной информацией».*

В случаях, когда субъектом действий выступало государство, больные шизофренией нередко приписывали ему конструктивные намерения: предотвращение преступности и терроризма, укрепление общественного благополучия и т.п., воспринимая государство в роли идеализированной родительской фигуры, в то время как психически здоровые участники могли сформулировать предположение о возможном злонамеренном характере соответствующих действий (участник В. Н., муж., 23 года, ролик по фильму «Сноуден»: *«Это вторжение в личное пространство; очень много данных для анализа людей и их действий, которые потом можно использовать для контроля над гражданами»).*

3. Прогнозирование исхода событий

Ответы участников на вопросы *«Как вы считаете, как будут развиваться события дальше? Чем всё кончится?»* разделены на три категории:

1. ***Позитивный исход:*** герой выйдет из ситуации самостоятельно или с чьей-то помощью, обстоятельства изменятся на благоприятные для героя.
2. ***Негативный исход:*** герой уступит воздействию, угрозы будут реализованы, герой погибнет, совершит суицид или сойдет с ума.
3. ***Неопределенный исход:*** перечисление нескольких возможных вариантов развития событий; утверждение, что дать однозначный прогноз развития событий невозможно.

В таблице № 3 представлено распределение ответов испытуемых двух групп по описанным категориям.

Таблица 3

Распределение ответов по критерию прогноза исхода событий

Прогнозируемый исход	Клиническая группа	Группа нормы	Уровень значимости различий
Положительный	71 47%	59 39%	Значимых различий не обнаружено
Отрицательный	56 37%	48 32%	
Неопределенный	**23 16%**	**43 29%**	**x^2=7,78 p≤0,01**

Примечание. В таблице указано абсолютное количество ответов соответствующей категории и процентное соотношение ответов. Статистически значимые различия выделены полужирным шрифтом.

Больные параноидной шизофренией значимо чаще формулировали определенный — положительный или отрицательный — исход событий, в то время как участники группы нормы значимо чаще склонялись к неопределенному, многоальтернативному исходу. Процитируем прогноз больного Л. Д., муж., 28 лет, относительно развития событий ролика по фильму «Сеть»: *«Как-то так повернется сюжет, появится человек или какая-то новая информация, которая поможет делу. Будет хэппи-энд».* Другой испытуемый Д. З., муж., 36 лет предполагает отрицательный исход событий в видеофрагменте по фильму «Крыса»: *«Думаю, нехорошо все кончится… она и дальше будет себя так накручивать, доведет себя, потом попадет в больницу».*

Можно предположить, что работа примитивного защитного механизма расщепления позволяет больным шизофренией создавать более простую и предсказуемую картину мира, что снижает тревогу. Для психически здоровых людей неопределенность оказывается более переносимой, что прослеживается в их ответах. В качестве примера приведем прогноз участника контрольной группы Н. С., муж., 26 лет, относительно развития событий ролика по фильму «Крыса»: *«Либо она захочет выйти с ним [преследователем] на контакт; либо он псих, который доведет ее до суицида; либо она найдет способ выйти из этой ситуации».*

4. Стратегии собственных действий в аналогичной ситуации

Ответы участников на вопрос *«Как бы вы поступили на месте главного героя, если бы оказались в его положении?»* были разделены на четыре категории:

1. ***Выход из ситуации:*** бегство, отключение всех информационных устройств.
2. ***Коммуникация:*** переговоры, обращение за помощью.
3. ***Противостояние:*** борьба, отстаивание своей правоты, защита себя и близких, поиск и устранение источника угрозы.
4. ***Пассивность в отношении угрозы:*** игнорировать угрозу, надеяться на то, что она исчезнет или что-то/кто-то поможет, молиться, подчиняться указаниям и инструкциям.

Статистический анализ не выявил межгрупповых различий в частоте ответов. В обеих группах наиболее частотными были ответы категории «выход из ситуации» и «пассивность». Следует, однако, учитывать, что фактор неверного понимания некоторыми больными шизофренией сюжетов показанных видеороликов оказывает искажающее влияние на их выбор ответных действий, что делает полученный нами результат не вполне показательным.

5. Оценка реальности событий

Ответы участников на вопрос «Могут ли такие события произойти в реальности?» разделены на три категории:

1. ***Да.***
2. ***Отчасти:*** станут возможны в ближайшем будущем; возможны в других странах; возможны лишь в отношении определенной группы людей.
3. ***Нет.***

В таблице № 4 представлено распределение ответов испытуемых двух групп по описанным категориям.

Таблица 4

Распределение ответов по критерию оценки возможности событий в реальности

Возможность события в реальности	Клиническая группа	Группа нормы	Уровень значимости различий
Вполне возможно	108 72%	121 81%	x^2=3,118 p≥0,05
Потенциально/ ограничено возможно	21 14%	20 13%	Значимых различий не обнаружено
Принципиально невозможно	**21** **14%**	**9** **6%**	**x^2=5,33** **p≤0,05**

Примечание. В таблице указано абсолютное количество ответов соответствующей категории и процентное соотношение ответов. Статистически значимые различия выделены полужирным шрифтом.

Участники клинической группы значимо чаще утверждали, что показанные действия не могут происходить в реальности. Они чаще ссылались на вымышленный характер сюжета видеоролика, чем психически здоровые испытуемые. Кроме того, следует отметить, что в случаях неверного понимания больными шизофренией показанного сюжета в качестве возможных в реальности событий они могли расценивать возникновение психопатологической продукции или развитие полезных для общества инновационных технологий.

6. Возможность защититься от информационных угроз

Ответы испытуемых на вопрос «Можно ли было обезопасить себя от попадания в подобную ситуацию/от показанной угрозы?» разделены на три категории:

1. ***Возможность защититься:*** с помощью правильного использования устройств (осторожность, избирательность, техническая грамотность); эффективной стратегии взаимодействия с субъектом угрозы (противостояние манипуляциям, самостоятельное критическое мышление, отстаивание своих границ, умение договариваться); обращения за помощью к компетентным людям; бегства или избавления от технических устройств.
2. ***Невозможность защититься:*** беззащитность перед угрозой, невозможность ей противостоять.
3. ***Отрицание наличия угрозы, от которой необходимо защищаться.***

В таблице № 5 представлено распределение ответов испытуемых двух групп по описанным категориям.

Таблица 5

Распределение ответов по критерию оценки возможности защититься от информационных угроз

Возможно ли защититься	Клиническая группа	Группа нормы	Уровень значимости различий
Да, защититься возможно	**89 59%**	**111 74%**	**x^2=7,26 p≤0,01**
Нет, защититься невозможно	18 12%	29 19%	Значимых различий не обнаружено
Отрицание угрозы	**43 29%**	**10 7%**	**x^2=24,95 p≤0,01**

Примечание. В таблице указано абсолютное количество ответов соответствующей категории и процентное соотношение ответов. Статистически значимые различия выделены полужирным шрифтом.

Участники с параноидной шизофренией значимо чаще отрицали наличие объективной угрозы в показанных им видеороликах, что обусловлено искаженным восприятием их сюжета. Психически здоровые участники значимо чаще признавали угрозу и считали, что от нее возможно защититься, приводя примеры различных способов защиты.

7. Личное отношение к информационным угрозам

Материалы второй части структурированного интервью были также подвергнуты качественному и количественному анализу. Ответы испытуемых анализировались по следующим параметрам: личная обеспокоенность возможностью информационных угроз; личный опыт столкновения с подобными угрозами; знание способов выхода из подобных ситуаций; защитные меры, предпринимаемые участником в настоящее время. Статистически значимые межгрупповые различия обнаружены по обеспокоенности возможностью информационных угроз и активности защиты от них.

Распределение ответов испытуемых двух групп по критерию обеспокоенности потенциальным риском информационных угроз наглядно представлено на диаграмме № 1.

Диаграмма 1

Обеспокоенность информационными угрозами

Были обнаружены следующие статистически значимые различия. В группе нормы ни один участник не отрицал объективное существование информационных угроз, тогда как среди больных шизофренией отрицание встречалось у 20% испытуемых (6 человек). Значение критерия хи-квадрат: $\chi^2 = 6,67$, уровень статисти-ческой значимости: $p \leq 0,01$.

Распределение ответов испытуемых двух групп по критерию активности защиты от информационных угроз представлено на диаграмме № 2.

Диаграмма 2

Активность защиты от информационных угроз

Примечание. Значение критерия хи-квадрат: $\chi^2 = 11,24$, уровень статистической значимости: $p \leq 0,01$.

Среди больных шизофренией предпринимают целенаправленные действия по защите от информационных угроз чуть более четверти участников (28%), тогда как среди психически здоровых людей — почти три четверти (73%), что может отражать не только разную степень озабоченности данной проблемой, но и разную степень сформированности навыков обеспечения личной информационной безопасности.

Обсуждение результатов

Проведенное исследование продемонстрировало, что больные параноидной шизофренией, в отличие от психически здоровых лиц, склонны к преуменьшению опасности при восприятии ситуаций информационных угроз, а в ряде случаев не распознают их вовсе и приписывают показанным ситуациям иное значение. Они чаще, чем здоровые люди, игнорируют информационные угрозы, не замечают злонамеренный характер показанных действий, оценивают их как благоприятные для общества или конкретного человека, верят в хороший конец и отказываются принимать их реальность.

Психически здоровые люди верно понимают сюжет показанных роликов и признают возможность продемонстрированных в них событий в реальности. Они чаще, чем психически больные участники, осознают, что показанные угрозы исходят от частного лица или государства и преследуют корыстные мотивы. Согласно самоотчетам, они чаще сталкивались в жизни с подобными ситуациями или слышали о них от знакомых и знают, что следует предпринимать в подобных ситуациях. Они признают активное влияние на современного человека гаджетов и цифровых технологий, осведомлены о слабости систем информационной безопасности и знают, какие меры можно предпринять, чтобы обезопасить себя от информационных угроз.

Выявленные межгрупповые различия могут иметь несколько объяснений. В основе характерных для больных шизофренией искажений восприятия угроз может лежать работа примитивных защитных механизмов (в частности, отрицания и расщепления), характерных для психотического уровня функционирования психики и позволяющих снизить уровень тревоги путем грубого искажения восприятия реальности. Можно предположить также, что в силу аутизации, снижения социальной направленности, погруженности в собственные психопатологические переживания пациенты с шизофренией не склонны идентифицировать себя с героем художественного фильма, сопереживать ему, если показанная ситуация не соответствует содержанию их психопатологической продукции, в результате чего события оцениваются как нереальные и тревога не возникает. Наконец, свой вклад может вносить низкая вовлеченность больных представленной выборки в использование информационных устройств, дефицит соответствующих знаний и опыта. В любом случае больные параноидной шизофренией осознают риск нарушения собственной информационной безопасности в меньшей мере, чем здоровые люди, и не обладают достаточными навыками эффективного реагирования на подобные угрозы. А.Е. Войскунский [7] пишет о том, что невежество и неосведомленность могут лежать в основе неэтичного поведения в интернете и призывает специалистов проводить профилактическую работу с помощью специального обучения (тренинга). Мы полагаем, что неосведомленность и отсутствие соответствующих навыков обеспечения личной информационной безопасности могут лежать также в основе виктимного поведения.

В то же время отсутствие у больных реалистичных знаний об устройстве современных информационных технологий может выступать фактором провокации психотических срывов при столкновении с непривычным и непонятным для них опытом. Так, в клинической практике одного из авторов статьи был случай больного параноидной шизофренией, развившего острый параноидный психоз после посещения запрещенного интернет-сайта, неизбежным результатом чего он предполагал преследование со стороны спецслужб и тюремное заключение. В другом случае пациентка сформировала бредовое убеждение, что подвергается круглосуточной слежке и воздействию через популярный мессенджер, после того как получила несколько таргетированных рекламных сообщений.

На наш взгляд, исследование и обсуждение в профессиональном сообществе только компенсаторной роли информационных технологий при игнорировании их возможного патогенного потенциала для больных с расстройствами психотического уровня препятствует осуществлению своевременной психологической профилактики. В связи с выявленной недостаточной осведомленностью больных шизофренией о реально существующих информационных угрозах целесообразным представляется проведение с ними психопросветительской и тренинговой работы, направленной на формирование информационной грамотности, навыков безопасного обращения с гаджетами и эффективных способов выхода из угрожающих ситуаций.

Выводы

1. Выявлены значимые различия в восприятии информационных угроз больными шизофренией и психически здоровыми людьми: больные параноидной шизофренией значимо чаще игнорируют угрожающий характер показанных действий; интерпретируют угрожающие действия как преследующие благую цель или затрудняются определить конкретный мотив; отрицают реальную возможность показанных действий; прогнозируют положительный исход событий; в реальной жизни не предпринимают мер по защите от информационных угроз.
2. Обоснована необходимость разработки и применения программ психологического просвещения больных параноидной шизофренией, тренингов навыков предотвращения и эффективного выхода из ситуаций столкновения с информационными угрозами.

Литература

1. Айсина Р.М. Психологическая безопасность взрослых интернет-пользователей: анализ современных исследований // Вестник Омского университета. Серия: «Психология». – 2019. – № 1. – С. 28–38. DOI: 10.25513/2410-6364.2019.1.28-38

2. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. – 2012. – № 4. – С. 97–102.

3. Батурин Ю.М., Полубинская С.В. Что делает виртуальные преступления реальными // Труды Института государства и права РАН. – 2018. – Т. 13, № 2. – С. 9–35.

4. Вещикова М.И. Восприятие опасности подростками и его связь с личностными чертами у подростков в норме и при психической патологии // Вестник ЮУрГУ. Серия «Психология». – 2015. – Т. 8, № 1. – С. 56–62.

5. Влияние негативных эмоциональных стимулов на поздние этапы восприятия (300-400 мс) у больных параноидной шизофренией в имплицитной ситуации / А.Ю. Архипов, В.Ю. Новотоцкий-Власов, М.К. Нурбеков [и др.] // Журнал высшей нервной деятельности им. И.П. Павлова. – 2018. – Т. 68, № 1. – С. 28–40. DOI: 10.7868/S0044467718010033

6. Войскунский А.Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. — 2010. — № 1 (3). — С. 48–53.

7. Габбард Г., Лестер Э. Психоаналитические границы и их нарушения / пер. с англ. К. Немировского. – М.: Класс, 2014. – 272 с.

8. Дедюлина М.А. Компьютерная этика: философский анализ // Философские проблемы информационных технологий и киберпространства. – 2016. – № 1 (11). – С. 79–90. DOI: 10.17726/philIT.2016.11.1.130.20

9. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18: Социология и политология. – 2018. – Т. 24, № 1. – С. 52–70. DOI: 10.24290/1029-3736-2018-24-1-52-70

10. Емелин В.А. Утрата приватности: идентичность в условиях технологического контроля // Национальный психологический журнал. — 2014. — № 2(14). — С. 19–26. DOI: 10.11621/npj.2014.0203

11. Емелин В.А., Рассказова Е.И., Тхостов А.Ш. Психологические последствия развития информационных технологий // Национальный психологический журнал. – 2012. – № 1 (7). – С. 81–87.

12. Жданок Д.Н. Патологическая адаптация при психотической тревоге в контексте теории самоорганизующихся систем // Медицина и образование в Сибири. – 2012. – № 4. – С. 9.

13. Журавлев М.С. Философия информационной безопасности // Известия Тульского государственного университета. Гуманитарные науки. – 2014. – № 2. – С. 40–50.

14. Лукаш А.В. Информационно-коммуникационные технологии как фактор социо-культурных процессов современности // Общество: философия, история, культура. – 2017. – № 3. – С. 66–70. DOI: 10.24158/fik.2017.3.15

15. Лысак И.В., Косенчук Л.Ф. Формирование персональной идентичности в условиях сетевой культуры. – М.: Спутник+, 2016. – 147 с.

16. Марков А.А. Характеристики информационной безопасности на современном этапе развития общества // Управленческое консультирование. – 2011. – № 3. – С. 67–76.

17. Нарыков Н.В., Дементьев С.А. Формообразующие факторы и социальные условия информационной безопасности личности // Научный вестник Омской академии МВД России. – 2017. – № 3 (66). – С. 57–59.

18. Петрюк П.Т. К изучению клиники параноидной формы шизофрении (обзор литературы) // Журнал психиатрии и медицинской психологии. – 2010. – № 1-2. – С. 122–130.

19. Радионов М.В. Информационное общество и проблемы информационной безопасности: социологические проблемы исследования // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 6-1. – С. 186–190.

20. Райкрофт Ч. Критический словарь психоанализа / пер. с анг. Л. Топоровой, С. Воронина, И. Гвоздева. – СПб.: Восточно-Европейский Институт Психоанализа, 1995. – 260 с.

21. Тлий А.А. Источники угроз в контексте информационной безопасности: социологический аспект // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. – 2013. – № 4 (130). – С. 159–163.

22. Устинов Д. Сущность информационной безопасности // Международный журнал гуманитарных и естественных наук. – 2017. – № 12. – С. 146–151.

23. Философские аспекты проблемы информационной безопасности / К.И. Болотов, А.В. Семашко, А.В. Гуменникова [и др.] // Актуальные проблемы авиации и космонавтики. – 2012. – Т. 2, № 8. – С. 445–446.

24. Digital Technology Use Among Individuals with Schizophrenia: Results of an Online Survey / K. Gay, J. Torous, A. Joseph [et al.] // JMIR Mental Health. – 2016. – Vol. 3, № 2. – P. e15. DOI: 10.2196/mental.5379. – Available at: https://pubmed.ncbi. nlm.nih.gov/27146094/ (Accessed 20 June 2020).

25. Fragile Self and Malevolent Others: Biased Attribution Styles in Individuals at Ultra-High Risk for Psychosis / H.Y. Park, M. Bang, K.R. Kim [et al.] // Psychiatry Investigation. – 2018. – Vol. 15, № 8. – P. 796–804. DOI: 10.30773/pi.2018.05.08

26. How connected are people with schizophrenia? Cell phone, computer, email, and social media use / B.J. Miller, A. Stewart, J. Schrimsher [et al.] // Psychiatry Research. – 2015. – Vol. 225, № 3. – P. 458–463. DOI: 10.1016/j.psychres.2014.11.067

27. Internet use, eHealth literacy and attitudes toward computer/internet among people with schizophrenia spectrum disorders: a cross-sectional study in two distant European regions / C. Athanasopoulou, M. Välimäki, K. Koutra [et al.] // BMC Medical Informatics and Decision Making. – 2017. – Vol. 17, № 1. – P. 136. DOI: 10.1186/s129 11-017-0531-4. – Available at: https://pubmed.ncbi.nlm.nih.gov/28931385/ (Accessed 20 June 2020).

28. Internet Use for Social Interaction by People with Psychosis: A Systematic Review / A. Jakubowska, J. Kaselionyte, S. Priebe [et al.] // Cyberpsychology, Behavior, and Social Networking. – 2019. – Vol. 22, № 5. – P. 336–343. DOI: 10.1089/cyber. 2018.0554

29. Lee C.Y. Understanding Security threats in Virtual Worlds // AMCIS 2009 Proceedings. – California, 2009. – Paper 466.

30. Prentice K.J., Gold J.M., Carpenter W.T. Jr. Optimistic Bias in the Perception of Personal Risk: Patterns in Schizophrenia // The American Journal of Psychiatry. – 2005. – Vol. 162, № 3. – P. 507–512. DOI: 10.1176/appi.ajp.162.3.507

31. Rekhi G., Ang M.S., Lee J. Clinical determinants of social media use in individuals with schizophrenia // PLoS One. – 2019. – Vol. 14, № 11. – P. e0225370. DOI: 10.1371/journal. pone.0225370. – Available at: https://pubmed.ncbi.nlm.nih.gov/ 31747434/ (Accessed 20 June 2020).

32. Schmid-Siegel B., Stompe T., Ortwein-Swoboda G. Being a webcam // Psychopathology. – 2004. – Vol. 37, № 2. – P. 84–85. DOI: 10.1159/000077584

33. Threat perception in schizophrenia-spectrum disorders / J.D. Henry, C. von Hippel, T. Ruffman [et al.] // Journal of the International Neuropsychological Society. – 2010. – Vol. 16, № 5. – P. 805–812. DOI: 10.1017/S1355617710000640

34. Torous J., Keshavan M. The role of social media in schizophrenia: evaluating risks, benefits, and potential // Current Opinion in Psychiatry. – 2016. – Vol. 29, № 3. – P. 190–195. DOI: 10.1097/YCO.0000000000000246

Specifics of the perception of cyberthreats in paranoid schizophrenia

Tsygankova P.V.[1]
E-mail: polina_tsy@mail.ru

Burnyasheva A.M.
E-mail: contact.cycle@yandex.ru

[1] *Pirogov Russian National Research Medical University*
Ostrovitianov str. 1, Moscow, 117997, Russia
Phone: +7 (495) 434-54-29

Abstract. The objectives of the research were to study the specifics of the perception of information security threats in paranoid schizophrenia. The background of the research is grounded on the increase in diversity and prevalence of information security threats in modern society, on the similarity of the content and mechanisms of the implementation of cyberthreats with the symptomatology of paranoid schizophrenia and on insufficient state of knowledge of the impact of modern technological changes on the course of mental disorders. The clinical group consisted of 30 patients with paranoid schizophrenia outside exacerbation and without cognitive deficiency (15 men, 31.8 ± 5.6 years old), the control group consisted of 30 mentally healthy research subjects (15 men, 31.3 ± 6.9 years). In the research the author's method "Perception of information security threats" was used, it consists of 5 videos made up using the content of feature films and demonstrating cyberthreats (theft and substitution of personal data, surveillance through personal devices by an intruder/government agencies, streaming personal life on the Internet) in combination with structured interview. A qualitative analysis of the answers was conducted. The Pearson's chi-squared test was used to identify intergroup differences in response rates. Significant intergroup differences in the perception of cyberthreats were revealed: patients with paranoid schizophrenia significantly more often than mentally healthy people ignore the existence of a threat and the maliciousness of the actions shown; more often predict a single outcome; underestimate the risk of information security threats in real life and are undisposed to take protection measures against such threats. The necessity of developing and applying psychological education programs for patients with paranoid schizophrenia, training of personal information security skills is substantiated.

Key words: paranoid schizophrenia; information security threats; cyberthreats; informational security; perception of information security threats.

For citation
Tsygankova P.V., Burnyasheva A.M. Specifics of the perception of cyberthreats in paranoid schizophrenia. Med. psihol. Ross., 2021, vol. 13, no. 1, p. 8. doi: 10.24412/221 9-8245-2021-1-8 [in Russian, abstract in English].