Философская мысль
Правильная ссылка на статью:
Кочеткова Н.П. Кибербезопасность и эволюция информационного пространства: феноменологический анализ взаимосвязи с метавселенной и фиджитал-миром // Философская мысль. 2024. № 7. DOI: 10.25136/2409-8728.2024.7.71055 EDN: UTGATW URL: https://nbpublish.com/library_read_article.php?id=71055

Кибербезопасность и эволюция информационного пространства: феноменологический анализ взаимосвязи с метавселенной и фиджитал-миром

Кочеткова Наталья Павловна

ассистент; кафедра философии и медиакоммуникации; Казанский Государственный Энергетический Университет

420066, Россия, республика Татарстан, г. Казань, ул. Красносельская, 51

kochetkova@mediayug.ru

Статья из рубрики "Социальная философия"

DOI:

10.25136/2409-8728.2024.7.71055

EDN:

UTGATW

Дата направления статьи в редакцию:

18-06-2024

Дата публикации:

08-07-2024

Аннотация: Предметом исследования является кибербезопасность, в рамках современных меняющихся условий информационного пространства, которое наполняется такими явлениями как метавселенная и фиджитал мир. Данные системы создают новые угрозы и проблемы в обработке, передаче, сохранении и соблюдении конфиденциальности данных. Предполагая, что пересечение кибербезопасности, цифровой трансформации (включая метавселенную и фиджитал-мир) и феноменологического анализа представляет собой важнейшую область исследования, в работе рассматриваются аспекты построения кибербезопасности в стране. Само слияние рассматривается как центробежное течение, которое невозможно остановить, но необходимо регулировать, что говорит о том, что решающее значение для разработки

эффективных стратегий по преодолению проблем, возникающих в условиях быстро меняющегося цифрового ландшафта играет преобразование подходов к организации кибербезопасности. Методы исследования основываются на сборе, анализе и синтезе данных, что выявило ключевые проблемы. Ключевой метод - феноменологический анализ происходящих изменений в информационной сфере, связанных с распространением явлений метавселенной и фиджитал-мира, что позволило отразить проблемы обработки информации и незащищённости от вредоносных атак и предложить новый подход к формированию системы кибербезопасности. Научная новизна статьи заключается в комплексном подходе к изучению взаимосвязи кибербезопасности, эволюции информационного пространства и таких новых концепций, как метавселенная и фиджитал мир. Переход на последние является следующим этапом развития информационного пространства, что прослеживается в постепенном разрастании экосистем и личных информационных платформ. Все это говорит о необходимости расширения системы обеспечения личной информации, а также данных, которые попадают в незащищенные информационные сети. В то же время, отечественные системы кибербезопасности подвергаются критике, что говорит о необходимости поиска новых решений. Одним из таких вариантов может стать феноменологический подход к изучению данных. В исследовании показано, как использование феноменологических методов исследования позволяет по-новому взглянуть на возможности отечественных разработчиков по усилению мер кибербезопасности и их адаптации в условиях быстро меняющихся цифровых ландшафтов.

Ключевые слова:

кибербезопасность, информационный ландшафт, метавселенная, уязвимость безопасности детей, технологии, фиджитал-мир, социометрия, феноменология, эволюция информационного пространства, конфиденциальность информации

Введение

В цифровом обществе человек все больше теряет контроль над происходящими вокруг него событиями. Это явление подтверждается наводнением информационными потоками, которые превышают когнитивные возможности критического анализа и размышления. Следовательно, этические последствия, связанные с использованием технологий, становятся все более очевидными и насущными. В первую очередь, компьютеры и роботизированные системы демонстрируют превосходство по сравнению с человеческими возможностями в выполнении точных и вычислимых задач, таких как игра в шахматы, логическое мышление, выявление закономерностей и выполнение математических расчетов и т. д.

В условиях все более оцифрованного общества у людей постепенно ослабевает чувство самостоятельности и контроля над событиями, происходящими в их ближайшем окружении.

Это приводит к тому, что люди оказываются не востребованными. Существуют опасения, что развитие технологий приведет к росту уровня безработицы. Во-вторых, ИИ (искусственный интеллект) становится частью социальной сферы, и его возможности по оказанию воздействия на человека не изучены до конца. В данном ключе не удивительно, что аналитики говорят об опасности, которую представляет собой ИИ и

киберпространство в целом [1. с.129-140]

Исследователи, которые в своих работах используют социометрический метод, указывают на то, что сегодня прослеживается такая тенденция, как поляризация общественного мнения, что позволяет философам, психологам и даже юристам понять, как формируется убеждения современного человека и какие факторы влияют на наше мировоззрение. Данная информация позволяет определить тактику работы с людьми, организации соответствующих работ по разработке алгоритмов, устанавливающих различные формы информационных атак [2. с.16-20].

Замыкание в информационном пузыре и информационном ландшафте создают иллюзию реальности и прозрачности, которую каждый человек может контролировать самостоятельно. Прозрачность алгоритмов, эмпирический и феноменологический метод исследования позволяют ученым понимать, как функционирует информационное пространство и как обезопасить современное человечество от спорных, вредоносных и проблемных тем, которые могут быть угрозой не только для сознания, но и для общества в целом. Так, больше 10 лет назад Эдвард Сноуден, рассматривая вопросы приватности и этики, указал на то, что возможности человечества повлиять на развитие технологий и распространение информации минимальны и заключаются только в тщательном анализе поступающей информации, что в целом иллюстрирует актуальное антропологическое и гносеологическое измерение данного вопроса. (*Эдвард Сноуден: десять лет после разоблачений //https://www.securitylab.ru/analytics/538861.php*)

В работе использован феноменологический метод, позволяющий изучить кибербезопасность в контексте семантической метавселенной – идеи о множестве параллельных миров, где каждый может иметь свои законы и правила. В этом контексте кибербезопасность представляет собой способ защиты информации и данных от внешних угроз и атак, а также гарантию их целостности и конфиденциальности.

Научная новизна статьи заключается в комплексном подходе к изучению сложной взаимосвязи между кибербезопасностью, эволюцией информационного пространства ИИ зарождающимися концепциями метавселенной и фиджитал. Основная проблема, рассматриваемая в статье, заключается в необходимости постоянного мониторинга и адаптации мер кибербезопасности в ответ на динамичную природу информационного пространства, особенно по мере его расширения в метавселенную и фиджитал сферы.

Целью проводимой работы является изучение особенностей эволюции информационного пространства с опорой на феноменологические методы исследования.

Автор выдвигает гипотезы о том, что:

1. Быстрая эволюция информационного пространства и таких технологий, как ИИ и метавселенная, требует динамичного и адаптивного подхода к кибербезопасности.

2 . Феноменологические методы исследования могут предложить ценные идеи для понимания и решения сложных проблем кибербезопасности в контексте цифрового и метаверсального миров.

В центре работы – идея о том, что пересечение кибербезопасности, цифровой трансформации (включая метавселенную и фиджитал-мир) и феноменологического анализа представляет собой важнейшую область исследования. Это слияние имеет решающее значение для разработки эффективных стратегий по преодолению проблем, возникающих в условиях быстро меняющегося цифрового ландшафта.

Результаты

Философский подход к информационному насыщению пространства довольно неоднозначен. С одной стороны, прослеживается вероятность нивелирования роли человека и превознесение машины и возможностей инноваций. С другой, человечество должно развиваться и стремиться к новым целям, достигать их, пересматривать существующие нормы и таким образом трансформироваться. Это и есть эволюция. Все больший вес в последнее десятилетие имеют такие феномены информационного пространства, как метавселенная и фиджитал. Метавселенная – это виртуальный трехмерный мир, в котором люди взаимодействуют посредством аватара для выполнения широкого спектра действий. Такая деятельность может варьироваться от досуга и игр до профессионального и коммерческого взаимодействия, финансовых операций или даже медицинских вмешательств, таких как хирургия. Хотя точные масштабы и влияние метавселенной на общество и экономику пока неизвестны, уже сейчас можно оценить ряд возможностей и рисков. Крупные технологические компании расширяют свою деятельность в метавселенной, в том числе за счет слияний и поглощений.

Ожидается, что бизнес в метавселенной будет опираться в основном на криптовалюту и не взаимозаменяемые токены, что поднимает ряд вопросов защиты информации и кибербезопасности (например, как получить согласие пользователя или защитить аватары от кражи личных данных). В среде метавселенной существует простор для широкого спектра незаконных и вредных действий и практик, например, вводящая в заблуждение реклама, хищение интеллектуальной собственности. Более того, цифровое погружение в метавселенную может иметь серьёзные негативные последствия для здоровья, особенно для уязвимых групп, таких как несовершеннолетние, которым может потребоваться особая защита. Наконец, доступность и инклюзивность метавселенной остаются областями, в которых еще предстоит добиться прогресса для создания среды равных возможностей [3. с.112-129].

С философской точки зрения метавселенная - это возможность человека выйти за границы собственных возможностей и получить доступ к новым мирам, системе восприятия и передачи различного рода информации. В данном ключе расширяется система познания себя и мира, с одной стороны, а с другой полностью уйти от реальности. И если говорить о феноменологическом анализе данного контекста, то выявляется, тенденция к обострению потребности в расширении кругозора, но, информационное пространство, чаще всего, насыщено непроверенным контентом и как следствие, необходимо его проверять и регулировать, а так же осмысливать с критической точки зрения, чему должны способствовать инструменты фильтрации поступающих данных. Но, контроль над информационным потоком может ограничить разработчиков в процессе перехода к новому уровня мира — фиджитал.

В контексте зарождающейся концепции фиджитал-мира, который представляет собой конвергенцию физической и цифровой сфер, изучение кибербезопасности и ее последствий для будущего взаимодействия человека с технологиями имеет первостепенное значение. Поскольку фиджитал мир продолжает развиваться и формировать наши культурные, общественные и философские ландшафты, крайне важно изучить роль современных технологий в создании безопасной цифровой среды. Хотя исследования в этой области все еще находятся на начальной стадии, философы уже определили, что главной целью кибербезопасности в фиджитал-мире должно быть не отключение информационных систем и искусственного интеллекта, а исследование уязвимостей, которые могут стать точками давления и впоследствии привести к негативным последствиям для человека. Исследователи, подчеркивающие важность

развития фиджитал-мира, также отмечают необходимость создания доступных мер безопасности для всех людей. В данном ключе безопасность цифровых сред для будущего общества заключается в создании безопасной среды для взаимодействия в этом новом пространстве. На данном этапе развития, и для разработчиков и для теоретиков, данная тема становится все более актуальной задачей, которая еще не нашла своего окончательного решения[4. с.11-13].

Рассматривая переход от метавселенной к фиджитал, можно отметить, что современное человеческое восприятие еще не готово к полному переходу на виртуальные системы. Следовательно, только через индивидуальное развитие, повышение общей национальной культуры и уровня восприятия можно предположить, что человечество подготовится к переходу к фиджитал. Одноко уже сегодня необходимо рассматривать вопросы безопасности, предупреждая наступление серьезных последствий перехода на фиджитал мир [5. с.50-59].

Именно поэтому важно понимать взаимосвязь между кибербезопасностью, информационным пространством, метавселенной и фиджитал-миром и разрабатывать соответствующие стратегии и меры по защите цифровой инфраструктуры. Только так можно обеспечить безопасность и стабильность в современном мире, где информация играет все более важную роль.

Феноменологический анализ взаимосвязи кибербезопасности с метавселенной и фиджитал-миром позволяет понять, как эти концепции взаимодействуют между собой и какие вызовы и возможности они представляют для человечества. Таким образом, феноменологический анализ взаимосвязи кибербезопасности с метавселенной и фиджитал-миром позволяет понять сложность и многоуровневость проблемы защиты информации в современном мире и разработать эффективные стратегии по обеспечению безопасности информационного пространства.

Феноменологический анализ взаимосвязи кибербезопасности и эволюционирующего информационного пространства выявляет обостряющуюся проблему распознавания целей преступных структур. По мере усиления необходимости постоянного усиления защиты информационных систем и данных, вызванного стремительным развитием технологий и появлением новых угроз, становится очевидным, что современные технологии сами по себе часто служат инструментом, которым оперируют преступные организации. Соответственно, правоохранительные органы и правительства оказываются не в состоянии эффективно противостоять этим злоумышленникам, что подчеркивает острую необходимость упреждающего и адаптивного подхода к кибербезопасности в условиях постоянно меняющегося ландшафта угроз. Следовательно, можно предположить, что дальнейший путь борьбы с киберпреступлениями заключается именно в информатизации систем феноменологического анализа, который станет основой для проверок информации поступающей в тот или иной сервис. Д. А. Камбулов отмечает, что уже сегодня борьба с киберпреступлениями многообразна и включает различные «инструменты, которые организации используют для защиты от угроз кибербезопасности» [6. с.1661-1667].

Безусловно, опирающиеся на феноменологию аналитики, регулярно выделяют важность понимания взаимосвязи процессов развития инноваций и их внедрения в повседневную жизнь с общей эволюцией информационного пространства и его влиянием на метавселенную и фиджитал-мир. Однако, как показывает современное положение, на данном этапе стоит идея распространения сути метавселенной и ее возможного перехода в фиджитал, что отражено на пропаганде составных элементов данной

искусственной системы.

Следовательно, достижение этапов формирования метавселенной и переход к фиджитал под влиянием технологий - увлекательный процесс развития и совершенствования и не удивительно, что он стал целью многих организаций и даже стран, однако, вопрос угроз, которые она несет, не учитывается.

В условиях современной России отказ от некоторых зарубежных инновационных продуктов привел к созданию отечественными разработчиками собственной метавселенной, примером которой может служить экосистема "Сбер". Эта экосистема не только стремится объединить реальный мир и виртуальное пространство, но и представляет практичную бизнес-модель, которая стремится защитить своих пользователей, признавая при этом свои ограничения, что свидетельствует о длительном пути к реализации фиджитал мира (рис. 2). В настоящее время только "Яндекс" может соперничать со "Сбером" в данной сфере. Причем, обе компании озадачены возможностями организации действенной системы безопасности своих клиентов.

Содержание и обслуживание этих пользовательских метавселенных, зависит от интересов клиента, охватывая широкий спектр областей - от развлечений и потребности во взаимодействии за пределами социальных сетей до создания иммерсивного опыта в конкретных пространствах, способствующих таким видам деятельности, как обучение и саморазвитие. Следовательно, можно предположить, что в будущем произойдет конвергенция экосистем "Яндекса", "Сбера", "Газпрома", "Mail.ru" и других в единый мета-обзор, характеризующийся атрибутами вымышленного мира, с фокусом на обучение, развитие и предоставление социальных сетей [7. с. 41-45].

Вопросы кибербезопасности стоят бескомпромиссно и открыто, что указывает на значимость данного аспекта для компании. Но, этот пример можно считать единичным, так как во многом в отечественной информационной системе прослеживается серьёзное отставание от мировых тенденций. Яркой иллюстрацией этого несоответствия является катастрофический провал СДЭК, известной курьерской организации, которая 26 мая 2024 года столкнулась с атакой вредоносного ПО и не смогла эффективно смягчить ее последствия. В связи с этим администрация объявила о недельной приостановке работы служб доставки, оставив клиентов в недоумении относительно связи между неполадками на сайте и физическим распределением товаров. В действительности деятельность СДЭК в значительной степени зависит от информационных систем, которые контролируют все процессы - от приема заказов до их доставки и выдачи. Это подчеркивает тревожно низкий уровень кибербезопасности и постепенный переход этих систем к инновационным цифровым формам.

Следует отметить , что усиление мер кибербезопасности можно трактовать как акт самоорганизации человека, знаменующий переход на более высокий эшелон культурного развития и создание системы, отвечающей индивидуальным интересам. Эта система будет структурирована за счет использования персональных социальных сетей, которые будут предоставлять доступ к уже существующему контенту, хотя и адаптированному к специфическим требованиям каждого пользователя. Если допустить точность феноменологического анализа, то можно предположить, что в грядущую эпоху человечество будет опираться на своего рода "федеральную сеть", доступ к которой будет осуществляться через индивидуальные социальные сети, включающие в себя ряд фильтров и ограничителей и одновременно определяющие потребности и запросы конкретного пользователя.

В то же время, в современном мире, подключённом к Интернету, защита кибербезопасности претерпела быстрое развитие. Благодаря широкому применению активно развивающихся технологий, таких как Интернет вещей и облачные вычисления, генерируются и собираются огромные объёмы данных. Хотя получаемую информацию обрабатывают и ее можно использовать для лучшего удовлетворения соответствующих потребностей бизнеса, она также создают большие проблемы для кибербезопасности и защиты конфиденциальности [8. с.29-63].

Феноменологический анализ позволяет исследовать вызовы и возможности, которые появляются в связи с метавселенной и фиджитал-миром и выявить ряд важных аспектов работы в области кибербезопасности.

Во-первых, современный мир становится все более зависимым от цифровых технологий и информационных систем. Однако растущее значение информационного пространства породило новые угрозы кибербезопасности, что требует критического подхода к информации и контенту, с которыми сталкиваются люди.

Во-вторых, все больше организаций и государств сталкиваются с кибератаками и киберпреступностями, что подчёркивает важность защиты информационных ресурсов. Тем не менее, правовые аспекты не соответствуют потребностям времени, что подчёркивает необходимость дальнейшего тесного взаимодействия со стороны человека, общества в целом и государства как законодателя и защитника.

В контексте трансформирующего влияния цифровой эпохи на ведение политической войны национальными государствами критическая феноменология предполагает заметный сдвиг в расстановке приоритетов в вопросах безопасности в демократических странах. Это требует обсуждения проблем, связанных с уровнем инноваций в самих государствах, а также способах работы над безопасностью всех заинтересованных лиц. Примерами использования киберпространства государственными и негосударственными субъектами могут служить вероятные атаки с последующим подрывом демократических выборов, поощрения распространения насилия и даже вызовы суверенитету и ценностям демократических государств, что имеет крайне дестабилизирующий эффект [9. с.17-23].

Успешные кампании политической войны также заставляют избирателей подвергать сомнению результаты демократических выборов и то, были ли особые интересы или иностранные державы решающим фактором в данном результате. Это наносит серьезный ущерб политической легитимности демократий, которая зависит от способности избирателей доверять избирательным процессам и результатам, свободным от вредоносного влияния – предполагаемого или реального [10. с.19-21]. При этом, высокая активность массмедиа и блогосферы, накладываясь на социальное напряжение в электоральный период, способны оказать влияние на процесс делегитимации политического режима [11. с.257].

В демократических обществах основополагающие принципы индивидуальной свободы и права на участие в политическом дискурсе создают серьезные препятствия для эффективного противодействия всепроникающей угрозе политической войны. В то же время современные правительства часто не уделяют первостепенного внимания неотложным задачам борьбы с кибер-угрозами, поскольку сами используют широкий спектр научно-технических достижений для реализации своих собственных планов. В результате обще-ственность оказывается уязвимой и вынуждено ориентироваться в неохраня-емом информационном пространстве, не имея достаточной подготовки для противостояния этой новой и грозной опасности. Проблемы, которые эта новая

политическая война с использованием цифровых технологий создает для демократий, будут возрастать с развитием машинного обучения и появлением цифровых инструментов, таких как «глубокие фейки». О чем пытаются сказать как отечественные [12. с.9-10], так и зарубежные исследователи [13. с. 250].

С феноменальной точки зрения, современные технологические достижения позволили людям взаимодействовать с метавселенной, погружаясь в цифровые сферы и виртуальные среды. Однако эти возможности одновременно открыли новые уязвимости и угрозы индивидуальной безопасности. Кибератаки, хакерство и кибершпионаж становятся все более распространенными в современном мире, при этом значительная часть населения считает, что эти вопросы находятся в компетенции правительства. Правительства же, напротив, воспринимают эти средства как важнейшие инструменты, с помощью которых они могут достичь желаемых целей.

По факту, интернет с каждым днём становится все более насыщенным информацией, а также становится основным средством обмена данными и коммуникаций, что не даёт гарантий в безопасности никому. И, в связи с тем что, каждый день идёт процесс совершенствования ИИ и ИС, растут возможности, которые предоставляет цифровое пространство, а это указывает на то, что возрастает и уровень угрозы кибербезопасности [14. с.30-37].

Приведенные факты свидетельствуют о том, что эволюция информационных систем и цифрового пространства оказывает повсеместное влияние на различные слои общества. Однако если все заинтересованные стороны не уделят приоритетного внимания интеграции мер кибербезопасности в рамках технологического прогресса и их развертыванию в различных облачных архитектурах, перспективы дальнейшего совершенствования социально-экономической структуры представляются мрачными. Это утверждение объясняется, прежде всего, двумя факторами: во-первых, подрывом доверия как к политическим институтам, так и к достоверности информационного контента; во-вторых, постоянными этическими дилеммами, которые, несмотря на то, что являются предметом постоянного обсуждения на различных уровнях, остаются нерешенными.

Обсуждение результатов

Аналитика кибербезопасности на основе ИИ была интегрирована в последние версии технологии межсетевых экранов. Эти передовые брандмауэры включают в себя автоматизированные системы для обнаружения сетевых вторжений, категоризации зашифрованного трафика данных, выявления вредоносного программного обеспечения и других функций безопасности. Включение искусственного интеллекта позволяет этим важнейшим мерам защиты работать с большей скоростью, точностью и адаптивностью по сравнению с традиционными брандмауэрами. В области криптографии решения на основе ИИ начинают помогать исследователям оптимизировать разработку алгоритмов и могут значительно сократить усилия по криптоанализу, такие как поиск дифференциальных следов, что имеет решающее значение в дифференциальном криптоанализе [15. с.2019-2043].

Недавно идея генеративной противоборствующей сети была применена для построения алгоритма автоматического шифрования, что делает первый шаг к созданию интеллектуального решения защиты без вмешательства человека [16. с.439-454]. Напротив, конфиденциальность человека находится под угрозой из-за систем на базе искусственного интеллекта. Ожидается, что рост кибератак с использованием ИИ

приведет к взрывному росту проникновений в сети, кражам личных данных и эпидемическому распространению интеллектуальных компьютерных вирусов [17. с.7029-7035].

Таким образом, еще одной будущей тенденцией является защита от атак с использованием современных технологий, используя методы, основанные на оболочных системах данных и интеллектуальных программах, что, возможно, приведет к гонке вооружений основанных на ИС и ИИ.

Решение безопасности на основе ИИ — одна из наиболее быстро развивающихся областей, которая объединяет исследователей из разных областей, таких как машинное обучение, статистика, анализ больших данных и криптография, для борьбы с современными угрозами кибербезопасности.

Однако, во многом все перечисленные направления определяют работу зарубежных разработчиков, что говорит о необходимости стимулирования отечественного ИИ-производства.

В данном ключе важно подчеркнуть, что уровень отечественных разработок уступает зарубежным, что соразмерно с уровнем внедрения россиян в киберпространство. Безусловно, сегодня молодое поколение испытывает большее влияние на восприятие мира со стороны социальных сетей, а также созданных новых форм виртуальной реальности. В то время как среднестатистический пенсионер с большим скепсисом относится к предложениям метавселенной СБЕР, молодежь и люди среднего возраста активно используют потенциальные возможности этих технологий. Социометрический анализ того как технологии меняют представления о метавселенной и взаимосвязи с ней показывает, что российское общество меняется медленно (по сравнению с европейским или азиатским), но и эти изменения отражают потребительский склад восприятия людей (рис.1). И это не смотря на то, что сегодня известны побочные действия со стороны использования достижений Интернета. И они касаются, как здоровья, так и окружающей среды.

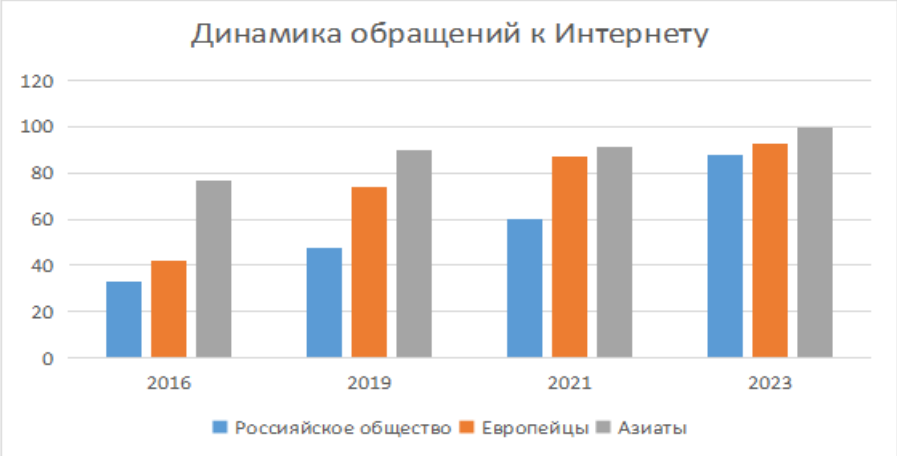

Рис.1 Результаты социометрического анализа о динамике использования информационного пространства

Как показано на рис.1, после 2019 года процесс обращения и применения информационных данных ускорился во всем мире и безусловно, страны, после пандемии столкнулись с новыми вызовами, такими как киберпреступления, мошенничества и новые способы мышления. В контексте продолжающейся эволюции киберпространства необходимо отметить согласованные усилия отечественных разработчиков в их

стремлении повысить производительность и безопасность. Однако критический анализ текущего ландшафта выявляет потенциальное несоответствие между достижениями этих разработчиков и изощренными методами, используемыми злоумышленниками, такими как мошенники и киберпреступники. Несмотря на значительные усилия, предпринятые российскими программистами в последние годы для повышения уровня кибербезопасности отечественных потребителей, о чем свидетельствуют данные, представленные в таблице 1, стремительный темп технического прогресса и адаптивный характер киберугроз требуют постоянного и проактивного подхода к обеспечению безопасности цифровой сферы.

Таблица 1

Деятельность компании кибербезопасности в РФ

Компании кибербезопасности	Период работы	Возможности продуктов
Лаборатория Касперского	На рынке с 1997	Более 20 ИБ-решений распространены на различные устройства и системы, защита развивается за счет функции интегративных решений. Инновации разрабатываемые компанией способны выявлять уязвимости систем и взаимодействовать между разными компонентами информационной инфраструктуры
Код Безопасности	На рынке с 1995	Специализируется на вопросах сетевой безопасности, работе в области криптографии и сохранения государственной тайны, что определяет область распространения на государственные учреждения
Security Vision	Появилась на рынке в 2010	Специализируется на работе с крупными финансовыми учреждениями (банками, коммерческими компаниями и прч.). специализируется на совершенствовании систем обеспечения безопасности в рамках происходящих в цифровом мире изменений
ИнфоТеКС	Образована в 1991 году	Разрабатывает систему криптографической защиты, а так же системы нацеленные на обнаружение угроз автоматическим системам

Д.А. Литвинов отмечает, что «За последние 10-15 лет участились кибератаки....», но в тоже время зарубежные агенты стремятся к «запрещению действия корпорации «Касперский»»[18. с.76-82] и это говорит о том, что российские разработки, в целом, могут выступать на международном уровне.

Индустрия кибербезопасности в России характеризуется дихотомией между компаниями, стремящимися соответствовать международным стандартам, и теми, кто сосредоточен на нишевых направлениях или не имеет широкого признания среди пользователей. Цены на системы безопасности, предлагаемые этими организациями, существенно различаются и

варьируются от нескольких тысяч до сотен миллионов рублей в зависимости от целевого сегмента потребителей. Такой разброс цен отражает воспринимаемую ценность и интерес к продуктам, представленным на рынке. С другой стороны, как показал пример со сбоем в работе СДЭК эффективность затрат на безопасность оправдываются наличием автоматической системы обновления, которая обычно обеспечивается облачными решениями. Таким образом, инвестиции в программы безопасности, разработанные отечественными специалистами, считаются оправданными, хотя опасения по поводу их эксплуатационной надежности и соответствия международным стандартам по-прежнему вызывают опасения у клиентов.

В то же время, ПО по кибербезопасности является лишь частью общей цифровизации, а это говорит о том, что оно воспринимается как неотъемлемая часть работы компьютерных систем, которые уже давно стали предметами общего потребления. А. Какаева, И. Какаев, О. Сахедова и Г. Корпяева указывают, что сегодня разработаны и активно переменяются такие системы как: «аналитика угроз, машинное обучение, поведенческий анализ и архитектура нулевого доверия» и данный перечень растет с каждым днем, но их применение зависят, в первую очередь от самих людей и принимаемых ими решений [19. с.1-8]

Если раньше потребительское отношение к миру и материальным благам рассматривалось как простой этап развития общества, то теперь этот вопрос стал одним из центральных в контексте воспитания молодого поколения с целью восстановления утраченных ценностей. Всепроникающее влияние цифровой среды на поведение и когнитивные процессы человека проявилось в негативном отношении к работе, реальной жизни и общественным ожиданиям. Одновременно возникли синтетические идеалы, пропагандирующие эгоизм, нарциссизм и различные формы самовыражения, что негативно сказывается на формировании законопослушных и ответственных граждан.

Нынешнее положение дел можно отчасти объяснить уменьшением государственного вмешательства в информационный поток. Российская Федерация служит ярким примером, иллюстрирующим преобразующее воздействие принятого в 2022 году закона, запрещающего распространение ложной информации в социальном киберпространстве. Таким образом, на смену преобладающим темам легкой финансовой наживы пришли понятия активного труда и личного развития. Более того, дискурс вокруг политических вопросов сменился статистическими анализами военных операций и распространением антироссийских настроений, которые зачастую лишены логической последовательности [20. с.200-212].

Такой способ воздействия на наполнение информационного ландшафта не просто повлиял на восприятие реальности, но и изменил отношение к правительству. А политика прозрачности информации, проводимая с учетом роли человека в современном информационном мире, позволила сформировать систему общенациональной поддержки как правительству, так и его политики.

И важно отметить, что созданные системы фильтрации информации, которые накладываются на социальные сети и системы взаимодействия могут быть использованы и в других направлениях, таких как защита приватных данных и сохранение безопасного пространства детей и молодежи.

Но, на данном этапе, это является частью проектов, которые могут оказаться в рамках государственных интересов.

Заключение

В заключение следует отметить, что необходимо постоянно отслеживать и адаптировать меры кибербезопасности в контексте постоянно развивающегося информационного пространства и технологий. Для достижения этой цели необходимо использовать следующие рычаги государственного управления.

1. Совершенствование законодательной базы в отношении киберпреступлений и атак.

2. Полноценное взаимодействие государственных программ и ИТ-компаний в области разработки доступных для населения систем безопасности.

3 . Финансирование разработок в области интернет-безопасности через конкурсы и соревнования среди студентов и школьников, которые могут предложить современные решения, исходя из своих потребностей.

4. Пропагандировать идеи критического подхода к осмыслению поступающей информации, а также идеи о необходимости фильтрации данных.

Учитывая ключевую роль кибербезопасности в современном информационном пространстве и способность феноменологического анализа изучать это явление в контексте метавселенной, данный подход может стать основой для более эффективной разработки новых систем кибербезопасности. Эти системы будут не только защищать информацию от внешних угроз и атак, но и обеспечивать ее целостность и конфиденциальность.

Последующий переход к системе фиджитал-мира также станет важным этапов в развитии цифровых систем и технологий, которые необходимо будет изучать с критической точки зрения, что требует феноменологического анализа и конкретизации вероятных угроз и негативных влияний.

Следовательно, перспективы дальнейших исследований в области кибербезопасности и эволюции информационного пространства распространяются на широкий спектр вопросов, которые охватывают, как идеи опережения преступных элементов, так и прогнозирования возможных направлений негативного влияния на сознание людей. Как следствие, данные темы должны исследоваться как с психологической, так и с философской точек зрения, что позволяет применять многогранный подход к их изучению.

Библиография

1. Sarker I.H. Cybersecurity and threat analysis based on artificial intelligence//Discover Artificial Intelligence. 2024. Volume 4, No.1. pp.129-140. DOI: 10.1007/s44163-024-00129-0
2. Аннаева А. Р., Аширов Г. Д., Атаев Г. Н., Бабаев Н. Б. Анализ актуальных киберугроз и методов защиты персональных данных в цифровом мире //IN SITU. 2023.№10. с.16-20
3. Синицын А., Ковалева Е. Тенденции и вызовы в области интернет-безопасности и защиты медицинских данных//Международный журнал Кибербезопасность и Криптография. 2019. № 7(4). с.112-129
4. Язгелдиев Ш., Керимов А., Бабаниязов Б. Интернет-безопасность и защита персональных данных: тенденции и вызовы в цифойров эпохе//IN SITU. 2023. №7. с. 11-13
5. Хорева Л. В., Кучумов А. В., Шраер А. В. Трансформация пути современного потребителя туристских услуг в фиджитал-среде // Профессорский журнал. Серия: Рекреация и туризм. 2023. №4 (20). с.50-59. DOI: 10.18572/2686-858X-2023-20-4-50-59
6. Камбулов Д. А. Решения для кибербезопасности// StudNet. 2021. №7. с. 1661-1667

7. Лукьянчикова А.С. Особенности продвижения модных брендов в метавселенных // Вопросы медиабизнеса. 2024. Т. 3. № 1. С. 41-45. DOI: 10.24412/3034-1930-2024-0050.
8. Clarke R., & Knake R. Cyber war: the next threat to national security and what to do about it//HarperCollins Publishers. 2010. №4. pp. 29-63. DOI:10.5860/selection.48-2963
9. Клокова У.Р. Основные направления укрепления кибербезопасности Российской Федерации//Российский университет дружбы народов (РУДН). 2022. №12. с.17-23
10. Аррыкова Г. К., Бегчаева Д. К., Бердиев К. Ч., Бердиев О. Ш. Обеспечение кибербезопасности в эпоху интернета вещей: вызовы и перспективы // IN SITU. 2023. №10. с. 19-21
11. Чурашова Е. А. Обвинительный дискурс как средство делегитимации (на примере республики Беларусь) //Философия и культура информационного общества: ВОСЬМАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ, Санкт-Петербург, 20–22 ноября 2020 года / Санкт-Петербургский государственный университет аэрокосмического приборостроения. 2020. с. 257-259
12. Дацева Э. Г., Куропятникова А. Ю. Приватность в эпоху больших данных//Молодой ученый.2022. № 4 (399). с. 9-10.
13. Rothrock R., & Clarke R. A. Digital resilience: Is your company ready for the next cyber threat. Nicholas Brealey Publishing, 2018.256p.
14. Литвиненко И. Л., Смирнов И. И. Основы цифровой экономики //AD ALTA: Журнал междисциплинарных исследований. 2019. Т. 9. №1 (7). с.30-37
15. Chen J., Su C.,& Yan Z. Cybersecurity analytics and privacy protection based on artificial intelligence//Security and Communication Networks. 2019. №185(91). pp. 2019-2043. doi:10.1155/2019/1859143
16. Patersonth Hanley L. Political Warfare in the Digital Age: Cyber-subversion, Information Operations and «deep fakes»//The Australian Journal of International Relations. 2020. №4 (74). pp. 439-454.
17. Raimundo R., & Rosario A. The impact of artificial intelligence on the security of data systems: a literature review//Sen sors. 2021. №21. pp. 7029-7035.
18. Литвинов Д.А. Оценка политики России в области кибербезопасности и возможные варианты ее совершенствования//Вестник науки и образования. 2019. №19-2 (73). с. 76-82
19. Какаева А., Какаев И., Сахедова О., Корпяева Г. Инновационные подходы к обеспечению кибербезопасности //Всемирный ученый. 2024. №24. с. 1-8
20. Буевич А.П., Буевич С.Ю., Варвус С.А., Сергеева А.Е., Карамова О.В. Влияние цифровизации на роль государства в современном мире: аналитический аспект//Достижения в области науки, технологий и инноваций. Спрингер. 2022. №4. с.200-212. doi:10.1007/978-3-030-90324-4_200

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования статьи «Кибербезопасность и эволюция информационного пространства: феноменологический анализ взаимосвязи с метавселенной и фиджитал-миром» выступает цифровой мир и его уязвимость. Цель своей работы автор определяет как изучение особенностей эволюции информационного пространства, что в значительной степени реализуется в тексте статьи.
Методология исследования является важной для автора темой. По его словам: «в работе использован феноменологический метод, позволяющий изучить

кибербезопасность в контексте семантической метавселенной». Важность феноменологического подхода для оценки потенциальных рисков в метавселенной и фиджитал-мире, подчеркивается на протяжении всей статьи. Однако ни методов, применяемых для этого в рамках феноменологического подхода, ни самого феноменологического подхода в тексте статьи, к сожалению, нет. Чтение текста не проясняет вопрос, как именно феноменологический подход может помочь осуществить эффективные меры кибербезопасности и, что, собственно говоря, имеет в виду автор под феноменологическим подходом. Реально в статье можно заметить сравнительно-описательный метод, исторический и критический анализ, поскольку автор делает акцент на изучении литературы, посвященной изучаемой проблеме и анализе фактов социальной реальности, связанных с распространением искусственного интеллекта и виртуальных и фиджитал миров.

Актуальность исследования объясняется важностью развития фиджитал-мира и необходимостью создания доступных мер безопасности для всех людей, которая еще не нашла своего окончательного решения.

Автор считает, что «научная новизна статьи заключается в комплексном подходе к изучению сложной взаимосвязи между кибербезопасностью, эволюцией информационного пространства ИИ зарождающимися концепциями метавселенной и фиджитал», однако каких-то принципиально новых идей в этой области автор не высказывает. Он считает необходимым подчеркнуть важность «постоянного мониторинга и адаптации мер кибербезопасности в ответ на динамичную природу информационного пространства, особенно по мере его расширения в метавселенную и фиджитал сферы», однако эта мысль представляется достаточно расхожим мнением, не обладающим на данный момент каким-либо эвристическим потенциалом. А действительно оригинальная идея о задействованности феноменологических методов в борьбе с киберпреступрлениями - автором не развивается.

Стиль статьи характерен для научных публикаций в области гуманитарных исследований. Автор стремится определить ключевые понятия исследования. Например, поясняет, что под метавселенной, он имеет в виду «виртуальный трехмерный мир, в котором люди взаимодействуют посредством аватара для выполнения широкого спектра действий», а фиджитал-мир «представляет собой конвергенцию физической и цифровой сфер». Кибербезопасность определяется как способ защиты информации и данных от внешних угроз и атак, а также гарантию их целостности и конфиденциальности.

К сожалению, при этом автор не поясняет, какие именно методы и приемы он имеет в виду, когда говорит о том что «феноменологические методы исследования могут предложить ценные идеи для понимания и решения сложных проблем кибербезопасности в контексте цифрового и метаверсального миров». Получается, что сама значительная составляющая именно философского аспекта исследования, не освящается должным образом в статье.

Структура и содержание работы соответствуют заявленной проблеме, однако не все ее аспекты оказываются в разной степени разработанными.

Не все выводы статьи вызывают однозначное согласие, например вывод о том, что в будущем человечество будет опираться на своего рода "федеральную сеть", доступ к которой будет осуществляться через индивидуальные социальные сети, включающие в себя ряд фильтров и ограничителей и одновременно определяющие потребности и запросы конкретного пользователя. История становления интернет-пространства однозначно свидетельствует о приоритете именно сетевого децентрализованного принципа развития. Говоря о кибербезопасности, автор делает акцент на «злоумышленников», преследующих преступные цели, не принимая во внимание, что как раз отечественные метавселенные «Яндекс» и «Сбер» демонстрируют поведение,

характерное для монополистического сговора, неоправданно повышая стоимость своих услуг, делая заведомо нефункциональные предложения (примером этого может служить облако Янекс-диска, бесплатный объем которого незначителен, а платны объем столь огромен, что не будет востребован). Предполагаемая автором конвергенция экосистем "Яндекса", "Сбера", "Газпрома", "Mail.ru" скорее усугубит проблемы с кибербезопасностью, чем решит их (вспомним, что каждая из этих платформ замечена в «сливании» данных своих клиентов).Таким образом, статья скорее полезна для полемики, чем с позиции предлагаемых в ней решений.

Библиография включает 20 наименований работ как отечественных, так и зарубежных исследователей, посвященных теме кибербезопасности.

Апелляция к оппонентам присутствует в виде отсылок к близким по тематике исследованиям,

Несмотря на замечания, статья может быть рекомендована к публикации и будет полезна для обсуждения важной темы.