

**ОТЗЫВ официального оппонента**  
**на диссертацию на соискание ученой степени кандидата**  
**социологических наук Швыряева Павла Сергеевича**  
**на тему: «Киберпреступность как социальная проблема: стратегии**  
**противодействия»**  
**по специальности 5.4.7. Социология управления**

Наравне с продвижением преимуществ цифровых технологий и интернета в современное общество нельзя не отметить растущие угрозы, получившие общее название «киберпреступность». Проблема киберпреступности наносит прямой и косвенный урон репутации, финансовому благополучию, реализации инноваций на основе цифровых технологий. Пострадавшими являются абсолютно все стороны социального взаимодействия: государство, реализующее стратегии цифровой трансформации, бизнес, внедряющий инновации, граждане, которые пользуются в повседневной жизни решениями, продуктами, приложениями на основе цифровых технологий.

Актуальность избранной темы обусловлена необходимостью разобраться в истоках и причинах проблем, вызванных явлением киберпреступности. Автор абсолютно справедливо видит в киберпреступности социальную проблему. Иными словами, автор в своем исследовании фокусируется на индивидууме как источнике или причине проблем, влекущих совершение киберпреступлений. Очевидно, что организационно-институциональные меры, включая изменение нормативно-правовой базы, формирование ответственных подразделений, ответственных за мониторинг и реагирование на киберпреступлений в государственных и коммерческих структурах, являются необходимыми, но недостаточными мерами для сокращения негативного эффекта от киберпреступлений. Поэтому рассмотрение киберпреступности как социальной проблемы позволяет понять важную размерность в причинах ее возникновения и механизмах противодействия. В фокусе остается социальное взаимодействие, интенции и мотивы различных социальных групп, причастных к киберпреступлениям, их ключевые социальные характеристики.

Поэтому поставленная автором цель в диссертационном исследовании, связанная с корректировкой стратегий борьбы с киберпреступностью как социальным явлением является крайне актуальной. Сформулированные задачи предполагают анализ и интерпретацию в понимании социальной размерности киберпреступности, выявление ее компонент, относящихся к социальной природе, выработку рекомендаций для борьбы с киберпреступностью в связке с целями устойчивого развития.

Без понимания социальной размерности для явления киберпреступности невозможна эффективная борьба с ней, чем и обусловлена актуальность выбранной темы.

Автор проделал большую работу и внес существенный вклад в понимание проблематики киберпреступности как социального феномена. В работе проанализировано большое количество релевантных источников, выбран метод анализа сложившейся нормативно-правовой базы по противодействию киберпреступности, собрана статистика совершения киберпреступлений. Отмечу отдельно заслуживающую внимания и поддержки попытку автора провести социальную интерпретацию понятия социальной киберпреступности на основе экспертного опроса с очень интересной и трудно доступной для анализа референтной группой следователей, расследовавших причины и последствия киберпреступлений.

Логичным видится переход автора к рассмотрению более всеобъемлющей концепции борьбы с киберпреступлениями на основе понятия «цифровой иммунитет» как состояния, в котором индивидуум менее уязвим к угрозам различного типа. В этой связи автор предлагает развивать чрезвычайно важные вопросы, связанные с повышением цифровой гигиены граждан, формированием цифровой культуры в государственных и коммерческих структурах, проведением аудита систем кибербезопасности. В используемой автором концепции устойчивого развития применительно к социальным аспектам киберпреступности представляется эффективным сочетать одновременно несколько подходов по пониманию и применению мер различной природы. В частности, опора на общественные ценности, международное сотрудничество, аудит уязвимостей, диалог государства и общества о координации усилий по преодолению киберугроз, усиление кадровой политики, в том числе в составе органов внутренних дел, специализирующихся на киберпреступлениях.

Положительно оценивая содержание диссертации в целом, имеются некоторые замечания и пожелания:

1. В качестве общего замечания хотелось бы выделить недостаточное внимание автора к имеющимся у проведенного исследования ограничениям. Пытаясь сформулировать общую стратегию борьбы с киберпреступностью, автор не охватывает ряд референтных групп, к которым относятся граждане – пользователи цифровых продуктов, бизнес – разработчики цифровых решений. Работу бы украсило обсуждение социальных проблем кибербезопасности с представителями государственных регуляторов, ценностных вопросов с представителями гражданского общества или киберактивистами, вопросов безопасной разработки цифровых продуктов с представителями бизнеса.

2. Отдельно хотелось бы отметить достаточно абстрактный, хоть и полезный для практиков уровень высказанных рекомендаций в работе. Не хватает некоторой субъектности в том смысле, что автор нечетко указывает, кто и на основе какого подхода должен менять нормативную базу, вести диалог в обществе, формировать, развивать и реализовывать стратегию кибербезопасности на основе целей устойчивого развития. Также не хватает

анализа автора по качеству имеющихся в России стратегических документов по кибербезопасности на предмет ответа на социальные вызовы.

3. Несмотря на полезность и новизну в части сбора статистики о киберпреступлениях и анализа работы следователей, важно было бы протестировать выявленные наработки на референтных группах граждан и понять их отношение к предлагаемым автором изменениям. Технократический оптимизм россиян, отмеченный автором, относится к вере в потенциал цифровых технологий. Однако, если затронуть тему цифрового доверия к государству, то картина может быть совсем иной. В этой связи требует более детального обоснования вопрос ключевых акторов, ответственных за реализацию изменений в борьбе с киберпреступностью.

4. При разработке инструмента экспертного интервью хотелось бы видеть более тесную связь вопросов с социальными теориями, рассмотренными автором в параграфе 1.2. Также автор не выделяет конкретных компонентов или элементов при применении вышеуказанных теорий к анализу цифровой социальной системы. Работу бы улучшило создание схемы структуры цифровой системы, таблицы киберугроз и соответствующих им социальных эффектов, таблицы обобщения данных, полученных от экспертов, таблицы отличий в свойствах «доцифровой» преступности и киберпреступности.

5. Работа бы выиграла от более четкого очерчивания периметра исследуемых объектов. Киберпреступность – настолько сложное явление, что следует указать более четко границы возникающего социального компонента. Например, речь может идти о защите всего периметра государственной инфраструктуры безопасности, о взаимодействии граждан с отдельными цифровыми продуктами и услугами, которые предоставляются бизнесом или государством. Анализ подобных кейсов также бы мог украсить работу.

6. С учетом разработки автором предложений по модификации стратегии борьбы с киберпреступностью было бы полезно сформулировать несколько стратегических показателей, достижение которых могло бы свидетельствовать об успехах в борьбе с киберпреступлениями. Иными словами, работу украсила бы разработка подходов к минимизации негативных социальных эффектов, которые способствуют высокой интенсивности киберпреступлений.

Вместе с тем, указанные замечания не умаляют значимости диссертационного исследования. Диссертация Швыряева П.С. представляет собой оригинальное, самостоятельное исследование, обладающее научной новизной и практической значимостью,

Содержание диссертации Швыряева П.С. соответствует специальности 5.4.7. Социология управления по социологическим наукам, а именно следующим ее направлениям:

П4. - Принципы и методы управления в современных условиях.



П6 - Механизмы социального регулирования: институциональные, социально-стратификационные, социокультурные, социально-организационные.

П7 - Процессы и структуры государственного и муниципального управления.

П.12 - Социальные технологии в системе управления.

П.22 - Социальные параметры использования цифровых технологий в управлении. Социальные процессы управления искусственным интеллектом.

Содержание диссертации соответствует также критериям, определенным пп. 2.1-2.5 Положения о присуждении ученых степеней в Московском государственном университете имени М.В.Ломоносова, диссертация оформлена согласно требованиям Положения о совете по защите диссертаций на соискание ученой степени кандидата наук Московского государственного университета имени М.В.Ломоносова.

Таким образом, соискатель Швыряев Павел Сергеевич заслуживает присуждения ученой степени кандидата социологических наук по специальности 5.4.7. Социология управления.

Официальный оппонент:

Кандидат социологических наук,  
Заведующий, Международная лаборатория цифровой трансформации в государственном управлении, НИУ ВШЭ

СТЫРИН Евгений Михайлович

03.06.2024

Контактные данные:

тел.: 7495 772 95 90\*12357,

Специальность, по которой  
защищена диссертация:

22.00.08 – «Социология управления»

Адрес места работы:

109028, г. Москва, Покровский бульвар 13/11,

НИУ ВШЭ, Международная лаборатория цифровой трансформации в государственном управлении

Тел.: +7495 772 95 90\*12357; e-mail: estyrin@hse.ru

Подпись соискателя  
удостоверяю:

Подпись заверяю

Специалист по персоналу  
Управления персоналом  
Азовцев Т.Д.

03.06.2024