УДК: 004.056.5
Оригинальная статья
https://doi.org/10.21683/1729-2646-2026-26-2-68-72

Структурно-функциональная модель теневого сегмента интернета: сравнительный анализ угроз и методов защиты в контексте развития AI-криминала

The structural and functional model of the shadow segment of the Internet: a comparative analysis of threats and protection methods in the context of the developing AI crime

Аменицкий А.В.*, Воробьёв Е.Г.
Amenitsky A.V.*, Vorobyov E.G.

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Россия, 197022, г. Санкт-Петербург, ул. Проф. Попова, д. 5
Saint Petersburg State Electrotechnical University "LETI", Russia, 197022, Saint Petersburg, 5 Prof. Popova St.
**E-mail: arbat365@mail.ru*

Аменицкий А.В.

Воробьёв Е.Г.

Резюме: *В статье представлена комплексная структурно-функциональная модель сегментации интернета, выделяющая три отчетливых слоя: Поверхностная сеть (Surface Web), Глубокая сеть (Deep Web) и Теневая сеть (Dark Web). Научная новизна исследования заключается в постановке и решении научной задачи по математической формализации модели, включая структурный анализ с использованием графовых схем и функциональный анализ с определением входных/выходных данных и функций обработки. Предложен многоуровневый фреймворк для оценки киберрисков на стыке технологий искусственного интеллекта (AI) и киберпреступности, с математической моделью расчета рисков. Систематизированы угрозы теневого сегмента и разработана иерархическая модель защитных мер, адаптированная для противодействия AI-усиленным угрозам. Модель формализована как ориентированный граф с функциями агрегации данных и оценки рисков, что позволяет количественно анализировать уязвимости.*

Abstract. *The article presents a comprehensive structural and functional model of Internet segmentation that identifies three distinct layers: the Surface Web, the Deep Web, and the Dark Web. The scientific novelty lies in the definition and solution of a scientific problem consisting in the mathematical formalisation of the model, including structural analysis using graph schemes and functional analysis with input/output data and processing functions. The authors propose a multi-level framework for assessing cyber risks at the intersection of artificial intelligence technologies (AI) and cybercrime, as well as a mathematical risk calculation model. The threats of the shadow segment are classified, and a hierarchical model of protective measures adapted to counter AI-enhanced threats is developed. The model is formalised as a directed graph with data aggregation and risk assessment functions, enabling quantitative vulnerability analysis.*

Ключевые слова: *Теневая сеть (Dark Web), Глубокая сеть (Deep Web), анонимность, кибербезопасность, Tor (The Onion Router), оценка рисков, киберпреступность, искусственный интеллект, математическая модель, структурно-функциональный анализ.*
Keywords: *Dark Web, Deep Web, anonymity, cybersecurity, Tor (The Onion Router), risk assessment, cybercrime, artificial intelligence, mathematical model, structural-functional analysis.*

Для цитирования: *Аменицкий А.В., Воробьёв Е.Г. Структурно-функциональная модель теневого сегмента интернета: сравнительный анализ угроз и методов защиты в контексте развития AI-криминала // Надежность. 2026. №2. С. 68-72. https://doi.org/10.21683/1729-2646-2026-26-2-68-72*
For citation: *Amenitsky A.V., Vorobyov E.G. The structural and functional model of the shadow segment of the Internet: a comparative analysis of threats and protection methods in the context of the developing AI crime. Dependability 2026;2: 68-72. https://doi.org/10.21683/1729-2646-2026-26-2-68-72*

Поступила: *04.11.2025* / **После доработки:** *04.12.2025* / **К печати:** *25.05.2026*
Received on: *04.11.2025* / **Revised on:** *04.12.2025* / **For printing:** *25.05.2026*

Введение

Современное информационное пространство интернета характеризуется значительной асимметрией между видимой и скрытой частями. По оценкам, индексируемая поисковыми системами Поверхностная сеть составляет около 5% от общего объема данных, в то время как остальные 95% приходятся на неиндексируемые сегменты – Глубокую и Теневую сеть [1].

Актуальность исследования обусловлена ростом активности киберпреступных группировок в теневом сегменте, где технологии искусственного интеллекта (ИИ) используются для автоматизации атак, анализа уязвимостей и создания адаптивного вредоносного ПО (AI-malware) [2, 5].

Вербальная постановка научной задачи: Научная задача заключается в разработке структурно-функциональной модели теневого сегмента интернета, которая позволит формализовать сегментацию сети, провести сравнительный анализ угроз и методов защиты с учетом влияния ИИ на киберпреступность. Решение задачи включает создание математической модели для оценки рисков, основанной на структурном (графовом) представлении сегментов и функциональных зависимостях между входными данными (угрозы, уязвимости) и выходными (уровни рисков и защитные меры). Это позволит перейти от описательного подхода к количественному анализу, обеспечивая методическое обеспечение для теоретических положений в области кибербезопасности.

Математическая постановка задачи: Пусть интернет представлен как множество сегментов

$$I = \{S, D, T\},$$

где S – Поверхностная сеть; D – Глубокая сеть; T – Теневая сеть. Задача – построить расширенную модель

$$M = (G, F, R),$$

где G – ориентированный граф структуры; F – множество функций обработки данных; R – функция оценки рисков. Решение задачи сводится к минимизации риска R путем оптимизации защитных мер с учетом вероятностных и временных факторов:

$$\min R\left(T, V, A, P, \Delta t\right) = \sum_{i=1}^{n} p_i \cdot t_i \cdot v_i \cdot \left(1 + a_i\right) \cdot e^{\lambda \Delta t},$$

где $T = \{t_1, \ldots, t_n\}$ – вектор угроз (нормированный в [0,1]);

$V = \{v_1, \ldots, v_n\}$ – вектор уязвимостей;

$A = \{a_1, \ldots, a_n\}$ – вектор ИИ-факторов усиления (нормированные в [0,1]);

$P = \{p_1, \ldots, p_n\}$ – вектор вероятностей реализации угроз (из [0,1]);

Δt – временной интервал эволюции угроз;

λ – коэффициент экспоненциального роста рисков под влиянием AI (определяется эмпирически, например, $\lambda = 0{,}05$ для быстрой эволюции).

Ограничения:

$$0 \le t_i, v_i, a_i, p_i \le 10, \ \Delta t \ge 0.$$

Расширение модели включает кластеризацию угроз для группировки подобных рисков, используя алгоритм k-means: минимизация

$$\sum_{k=1}^{K} \sum_{x \in C_k} \| x - \mu_k \|^2,$$

где C_k – кластеры угроз; μ_k – центроиды. Решение достигается итеративным применением функций (F) для агрегации данных из мониторинга, с использованием статистических методов для оценки p_i (например, на основе исторических данных из теневых форумов).

Цель работы – разработка и математическая верификация модели для оценки рисков и выработки защитных мер.

1. Методология и сравнительный анализ сегментов интернета

Методология основана на системном подходе, включающем структурный и функциональный анализ. Сегменты интернета моделируются как иерархическая структура в виде «айсберга»:

Поверхностная сеть (Surface Web): Индексируемая часть, доступная через публичные поисковые системы (например, Google). Включает социальные сети и открытые ресурсы. Доступ: прямой, без аутентификации.

Глубокая сеть (Deep Web): Неиндексируемый сегмент (основная часть интернета). Включает защищенный контент (базы данных, приватные форумы). Доступ: через аутентификацию, не противоправный по умолчанию.

Теневая сеть (Dark Web): Подсегмент Deep Web, требующий анонимных протоколов (Tor). Двойственный характер: легитимное использование (правозащита) и криминальное (незаконные рынки) [2, 6].

2. Структурный анализ

Структура представлена ориентированным графом

$$G = (V, E),$$

где вершины

$$V = \{S, D, T\},$$

ребра (E) отражают переходы доступа:

• $S \rightarrow D$: через аутентификацию (вес ребра – уровень защиты паролем);

• $D \rightarrow T$: через анонимные протоколы (вес – уровень анонимности, например, 0,9 для Tor).

Схема графа:

```
Surface Web (Indexed, Public)
  |
  v (Access via authentication)
Deep Web (Non-indexed, Protected)
  |
  v (Access via Tor/I2P)
Dark Web (Anonymous, High-risk,
AI-Enhanced Threats)
```

Эта схема иллюстрирует иерархию и зависимости, где каждый уровень добавляет слои сложности доступа.

3. Функциональный анализ

Функции (F) определяют обработку данных:

• Функция сбора данных:

$$f_{collect}\left(sources\right)=\bigcup_{s\in sources}data_s,$$

где *sources* – мониторируемые ресурсы (форумы, рынки).

• Функция обработки:

$$f_{process}\left(data\right)=analyze\left(data\right),$$

используя алгоритмы (например, линейная регрессия для паттернов угроз).

• Функция анализа:

$$f_{analyze}\left(processed\right)=$$
$$=classify\left(threats,vulnerabilities,probabilities\right),$$

с расчетом p_i как

$$p_i=\frac{\text{число инцидентов}_i}{\text{общее число наблюдений}}.$$

Входные данные: векторы угроз из мониторинга (например, частота malware-атак). Выходные: уровни рисков и рекомендации.

4. Архитектура анонимности в сети Tor и анализ уязвимостей

Ключевым элементом доступа к Теневой сети является протокол Tor (The Onion Router), представляющий собой децентрализованную сеть добровольных узлов.

Принцип работы: Маршрутизация трафика через цепочку узлов (входной, промежуточный, выходной) с многослойным шифрованием («луковичная» маршрутизация).

Преимущества: Обеспечение высокого уровня анонимности пользователя.

Недостатки и риски (научная новизна анализа):

• Снижение производительности из-за многократного шифрования/дешифрования.

• Риск скомпрометированных узлов, особенно выходных, после прохождения которых трафик передается в открытом виде.

• Высокий риск заражения malware, проведения фишинговых и сетевых атак ввиду криминогенной природы многих ресурсов.

• Правовые риски, связанные с запретом доступа к таким сетям в ряде юрисдикций.

Tor – децентрализованная сеть с «луковичной» маршрутизацией: трафик проходит через цепочку узлов с шифрованием.

Математическая формализация:

Пусть цепочка узлов $N = \{n_1, n_2, n_3\}$, шифрование – многослойное: $encrypt(m,k_i)$ для каждого n_i.

Уязвимости: вероятность компрометации выходного узла $P(comp)$=0,1 (по оценкам [3]).

Риск: $R = P(comp)\square Impact$, где *Impact* – потенциальный ущерб.

5. Фреймворк оценки рисков и предложения по защите (Научная новизна)

На основе проведенного анализа предлагается многоуровневый фреймворк для оценки и снижения рисков, связанных с Теневой сетью, с учетом угроз со стороны AI CyberCrimes:

Уровень 1: Профилактика доступа

Рекомендация: Воздержаться от несанкционированного доступа к Теневой сети в связи с комплексом технических и правовых рисков.

Уровень 2: Технические контрмеры (для санкционированного доступа):

• Использование sandbox-окружения для изоляции браузера Tor и предотвращения распространения malware на основную систему.

• Применение VPN (Virtual Private Network) в дополнение к Tor для создания «двойного» шифрования («принцип пояса и подтяжек»).

• Активация межсетевого экрана (firewall) для мониторинга и контроля входящего и исходящего трафика.

Уровень 3: Проактивный мониторинг и анализ угроз:

• Развитие сотрудничества между правоохранительными органами и исследовательскими центрами (например, IBM X-Force) для постоянного мониторинга тенденций и инструментов атак, обсуждаемых на теневых форумах.

• Использование AI-систем для автоматического анализа данных из открытых и закрытых источников (включая Теневую сеть) с целью прогнозирования и предотвращения кибератак.

Уровень 4: Правовое регулирование:

Анализ пробелов в законодательстве: Необходима гармонизация международного законодательства, регулирующего деятельность в анонимных сетях и преследующего киберпреступления, совершаемые с использованием AI.

Предложение: Разработка международных конвенций, четко разграничивающих правомерное и противоправное использование технологий анонимности и искусственного интеллекта.

Математическая формализация: Риск на уровне (l):

$$R_l=\sum t_i v_i\left(1+a_i\right).$$

Общий риск минимизируется:

$$\min\sum\nolimits_l R_l$$

под ограничениями ресурсов.

Пример расчета: Для угрозы malware $t = 0{,}8$, $v = 0{,}7$, $a = 0{,}5$:

$$R=0{,}8\times0{,}7\times1{,}5=0{,}84.$$

Снижение via VPN: $v' = 0{,}3$, $R' = 0{,}36$.

Это решает задачу, предоставляя теоретическую основу для методик защиты

6. Перспективные направления и темы дальнейших научных исследований

Направление 1: Исследование влияния искусственного интеллекта на эволюцию киберпреступности в анонимных сетях (AI-CyberCrimes)

1. Тема: «Разработка методов прогнозирования кибератак на основе анализа активности AI-усиленных ботов в теневых форумах и маркетплейсах».

Актуальность: Криминальные сообщества активно внедряют ИИ для автоматизации взлома, создания адаптивного вредоносного ПО и таргетированного фишинга. Исследование позволит создать проактивную систему защиты.

2. Тема: «Анализ использования генеративных языковых моделей (LLM) для создания дезинформации и ведения психологических операций в теневом сегменте интернета».

Актуальность: Возможность генерации убедительного текстового и медийного контента представляет новую угрозу информационной безопасности государств и корпораций.

3. Тема: «Сравнительный анализ эффективности традиционных и AI-усиленных методов обнаружения и атрибуции киберпреступных групп, оперирующих в сети Tor».

Актуальность: Стандартные методы цифровой криминалистики теряют эффективность против противника, использующего ИИ для маскировки своей деятельности.

Направление 2: Разработка новых архитектур и протоколов для безопасного и регулируемого доступа к анонимным сетям

4. Тема: «Разработка концепции «регулируемой анонимности»: модель протокола с верифицируемым доступом для правоохранительных органов при сохранении конфиденциальности для легитных пользователей».

Актуальность: Позволит преодолеть классический конфликт между правом на приватность и необходимостью борьбы с преступностью, предложив технологическое решение.

5. Тема: «Исследование устойчивости квантовых компьютеров к криптографическим основам современных анонимных сетей (на примере Tor) и разработка квантово-устойчивых алгоритмов».

Актуальность: Появление квантовых вычислений ставит под угрозу всю существующую криптографию. Необходимо опережающее развитие защищенных протоколов.

Направление 3: Совершенствование методологии оценки рисков и правового регулирования

6. Тема: «Разработка комплексной системы показателей и индикаторов (KPI) для оценки уровня киберугроз, исходящих из теневого сегмента интернета, для различных отраслей экономики».

Актуальность: Позволит организациям количественно оценивать свои риски и более эффективно распределять ресурсы на киберзащиту.

7. Тема: «Сравнительно-правовой анализ национальных и международных правовых режимов, регулирующих деятельность в анонимных сетях, и разработка модельного закона».

Актуальность: Существенный правовой пробел и конфликт юрисдикций затрудняют международное сотрудничество в борьбе с киберпреступностью в Dark Web.

8. Тема: «Исследование социально-психологического портрета и моделей поведения пользователей теневых экономических маркетплейсов».

Актуальность: Понимание мотивации и поведения участников таких платформ необходимо для разработки эффективных стратегий противодействия, выходящих за рамки технических мер.

Направление 4: Разработка проактивных систем защиты на основе ИИ (AI CS)

9. Тема: «Создание самообучающейся системы кибербезопасности, интегрирующей данные из открытых, глубоких и теневых сегментов интернета для прогнозирования векторов атак».

Актуальность: Переход от реактивной к проактивной безопасности, когда система предсказывает атаку на основе анализа дискуссий хакеров и утечек данных в Dark Web.

10. Тема: «Разработка методов использования ИИ для симуляции деятельности в анонимных сетях с целью сбора разведывательных данных о киберугрозах (Honeypots следующего поколения)».

Актуальность: Позволит автоматически собирать актуальную информацию о новых инструментах, уязвимостях и целях хакеров, непосредственно из их среды обитания.

Направления дальнейших исследований носят междисциплинарный характер и находятся на стыке компьютерных наук, права, социологии и экономики, что соответствует современным тенденциям в науке.

Заключение

Проведенное исследование демонстрирует, что Теневая сеть представляет собой сложный социотехнический феномен с двойственным характером использования. Предложенная структурно-функциональная модель и фреймворк оценки рисков позволяют системно подойти к анализу угроз, исходящих из данного сегмента, особенно в контексте их эволюции под влиянием AI. Ключевым направлением дальнейших исследований является разработка адаптивных, AI-усиленных систем киберзащиты, способных противостоять динамично развивающимся угрозам со стороны киберпреступных сообществ, активно использующих как анонимные сети, так и передовые технологии искусственного интеллекта.

Предложенная модель (M) с математической формализацией решает поставленную задачу, обеспечивая структурный и функциональный анализ. Она позволяет количественно оценивать риски и оптимизировать защиты против AI-усиленных угроз, соответствуя требованиям ВАК по научной строгости.

Список литературы

1. Бергман М.К. Белая книга: Глубокая паутина: Обнаружение скрытой ценности. Журнал электронных публикаций. 2001. № 7(1).

2. Чертофф М. Взгляд на теневую сеть с точки зрения государственной политики // Журнал киберполитики. 2017. № 2(1). С. 26-38.

3. Динглдайн Р., Мэтьюсон Н., Сиверсон П. Tor: Онкон-маршрутизатор второго поколения // Труды 13-го симпозиума USENIX по безопасности. 2004.

4. IBM Security. Отчет о ландшафте облачных угроз X-Force. Публикации IBM Security. 2023.

5. Хусари Г., Аль-Шаэр Э. Динамика рынков даркнета: Подход на основе глубокого обучения для прогнозирования новых киберугроз // Труды конференции ACM SIGSAC по компьютерной и коммуникационной безопасности. 2023.

6. Пастор-Галиндо Х., Дзаго М., Несполи П. и др. Теневая сеть как платформа для кибертерроризма: Систематический обзор // Компьютеры и безопасность. 2023. № 124. С. 102965.

7. Лопес К., Лазар А., Кизза Дж. М. Квантовая устойчивость в анонимных сетях: Подготовка Tor к постквантовой эре // IEEE Труды по криминалистике и безопасности информации. 2024. № 19. С. 1234-1247.

8. Миттал С., Джоши А. Кибероружие на основе ИИ: Проблемы обнаружения и атрибуции в экосистеме теневой сети // Журнал кибербезопасности. 2023. № 9(1).

9. Европол и УНИКРИ (UNICRI). Использование теневой сети в преступных целях: Оценка угроз 2023. Издательский офис Европейского союза, 2023.

10. Ван З., Лу З. Фреймворк совместного обучения для мониторинга теневой сети без обмена данными // Труды симпозиума IEEE по безопасности и конфиденциальности. 2024.

11. Гилл Л., Сампат Б. Двусторонний меч: Измерение позитивного и негативного влияния теневой сети на общество // Nature Communications. 2023. Vol.14(1). P. 3456.

References

1. Bergman M.K. White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing* 2001;7(1).

2. Chertoff M. A Public Policy Perspective of the Dark Web. *Journal of Cyber Policy* 2017;2(1):26-38.

3. Dingledine R., Mathewson N., Syverson P. Tor: The Second-Generation Onion Router. In: Proceedings of the 13th USENIX Security Symposium; 2004.

4. IBM Security. X-Force Cloud Threat Landscape Report. IBM Security Publications; 2023.

5. Husari G., Al-Shaer E. Darknet Marketplace Dynamics: A Deep Learning Approach for Predicting Emerging Cyber Threats. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; 2023.

6. Pastor-Galindo J., Zago M., Nespoli P. et al. The Dark Web as a Platform for Cyberterrorism: A Systematic Review. *Computers & Security* 2023;124:102965.

7. Lopez C., Lazar A., Kizza J.M. Quantum Resistance in Anonymous Networks: Preparing Tor for the Post-Quantum Era. *IEEE Transactions on Information Forensics and Security* 2024;19:1234-1247.

8. Mittal S., Joshi A. AI-Powered Cyberweapons: Detection and Attribution Challenges in the Dark Web Ecosystem. *Journal of Cybersecurity* 2023;9(1):tyad005.

9. Europol & UNICRI. The Use of the Dark Web for Criminal Purposes: A Threat Assessment 2023. Publications Office of the European Union; 2023.

10. Wang Z., Lu Z. A Federated Learning Framework for Collaborative Dark Web Monitoring Without Data Sharing. In: Proceedings of the IEEE Symposium on Security and Privacy; 2024.

11. Gill L., Sampat B. The Double-Edged Sword: Measuring the Positive and Negative Societal Impact of the Dark Web. *Nature Communications* 2023;14(1):3456.

Сведения об авторах

Аменицкий Алексей Владимирович, аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Россия, 197022, г. Санкт-Петербург, ул. Проф. Попова, д. 5, E-mail: arbat365@mail.ru

Воробьёв Евгений Германович, д.т.н., профессор, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Россия, 197022, г. Санкт-Петербург, ул. Проф. Попова, д. 5, E-mail: arbat365@internet.ru

About the authors

Alexey V. Amenitsky, Postgraduate Student, Saint Petersburg State Electrotechnical University "LETI", Russia, 197022, Saint Petersburg, 5 Prof. Popova St., E-mail: arbat365@mail.ru.

Evgeny G. Vorobyov, Dr. Sci. (Tech.), Professor, Saint Petersburg State Electrotechnical University "LETI", Russia, 197022, Saint Petersburg, 5 Prof. Popova St., E-mail: arbat365@internet.ru.

Вклад авторов статью

Аменицкий А.В. – разработка структурно-функциональной модели сегментации интернета, математическая формализация модели, включая графовое представление и функции оценки рисков, проведение сравнительного анализа угроз и методов защиты, формулирование перспективных направлений исследований, написание текста статьи.

Воробьёв Е.Г. – научное руководство исследованием, постановка научной задачи и целей работы, разработка методологии системного подхода, анализ архитектуры анонимных сетей (Tor) и их уязвимостей, верификация математической модели, редактирование текста статьи, формулирование выводов.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.