DOI 10.37882/2223-2974.2026.03.07

DIGITAL-CPTED: ТЕОРЕТИКО-КРИМИНОЛОГИЧЕСКИЕ ОСНОВЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ В ЦИФРОВОЙ СРЕДЕ

DIGITAL-CPTED: THEORETICAL AND CRIMINOLOGICAL FOUNDATIONS FOR CRIME PREVENTION IN THE DIGITAL ENVIRONMENT

M. Danilova

Summary. This article examines the theoretical and criminological basis for the Digital-CPTED (Crime Prevention Through Environmental Design) concept as a proactive strategy for preventing crime in the digital environment. The author substantiates the need to adapt classical CPTED principles to the specificities of the digital space, particularly social media. Based on an analysis of the specifics of social media as a criminogenic environment, the Digital-CPTED model is proposed, aimed at creating a «protective digital space.» The model examines mechanisms for implementing digital natural surveillance, digital territoriality, access control, and maintaining environmental quality. Particular attention is paid to the legal and ethical challenges associated with its implementation, and a hybrid legal model is proposed aimed at striking a balance between security, freedom, and privacy in cyberspace.

Keywords: Digital-CPTED, crime prevention, digital environment, social networks, situational prevention.

Данилова Мария Анатольевна
кандидат социологических наук, доцент, ФГБОУ ВО «Саратовская государственная юридическая академия»
dory@rambler.ru

Аннотация. В статье рассматривается теоретико-криминологическое обоснование концепции Digital-CPTED (Crime Prevention Through Environmental Design) как проактивной стратегии предупреждения преступности в цифровой среде. Автор обосновывает необходимость адаптации классических принципов CPTED к особенностям цифрового пространства, в частности, социальных сетей. На основе анализа специфики социальных сетей как криминогенной среды предлагается модель Digital-CPTED, ориентированная на создание «защищающего цифрового пространства». В рамках модели рассматриваются механизмы внедрения цифрового естественного надзора, цифровой территориальности, контроля доступа и поддержания качества среды. Особое внимание уделяется правовым и этическим вызовам, связанным с её внедрением, и предлагается гибридная правовая модель, направленная на баланс между безопасностью, свободой и приватностью в киберпространстве.

Ключевые слова: Digital-CPTED, предупреждение преступности, цифровая среда, социальные сети, ситуационная профилактика.

Введение

Цифровая трансформация общества привела к тому, что социальные сети стали не только ключевым пространством коммуникации, но и новой средой для криминальных проявлений. Этот тезис подтверждается как официальной статистикой, так и академическими исследованиями. Согласно данным МВД России, в 2025 году более трети всех регистрируемых в стране преступлений были связаны с использованием интернет-каналов [1], что прямо указывает на системную значимость цифровой среды для современной преступности.

Традиционные меры борьбы, такие как уголовно-правовые запреты и технические блокировки, носят преимущественно реактивный характер и не устраняют глубинные криминогенные факторы, заложенные в архитектуре цифровых платформ. В этой связи возникает необходимость в разработке проактивных, превентивных стратегий, способных влиять на среду, в которой формируются правонарушения [2, С. 48]. Перспективным направлением представляется адаптация концепции предупреждения преступности через дизайн среды (CPTED), успешно применяемой в криминологии для снижения преступности путём изменения физического пространства.

Однако системное применение принципов CPTED к цифровой среде остаётся малоизученным. Целью настоящего исследования является разработка теоретико-криминологических основ новой концепции — Digital-CPTED — применительно к социальным сетям. Это позволит перейти от реагирования на инциденты к проектированию цифровых пространств, снижающих саму возможность совершения преступлений.

1. Теоретико-методологические основы классической концепции CPTED в криминологии

Концепция предупреждения преступности через дизайн окружающей среды (CPTED) является ключевым подходом ситуационной профилактики в криминологии. Её суть состоит в целенаправленном изменении физического пространства для влияния на поведение, что увеличивает риски для потенциального правонарушите-

ля, снижает ожидаемые выгоды от преступления и укрепляет ответственность законопослушных граждан.

1.1. Источники и методологическая база

Теоретической основой работы послужили труды современных российских криминологов, исследующих эволюцию средового подхода и его связь с теориями рационального выбора и виктимологии [3–5]. Их положения о дихотомии «защищающего» и «защищённого» пространства, а также о связи градостроительного и цифрового регулирования приняты в качестве фундамента для последующей адаптации классических принципов.

Методологический подход направлен на адаптацию криминологических концепций к цифровой реальности. С помощью системного анализа социальные сети рассматриваются как целостная среда, где дизайн и алгоритмы являются активными факторами, формирующими поведение. Сравнительный анализ позволил выявить аналогии и различия между физическим и цифровым пространством как объектами профилактики. Ключевые принципы CPTED были перенесены в цифровой контекст методом аналогии и экстраполяции, что позволило избежать механического копирования и учесть уникальные свойства цифровой среды. Итоговая концептуальная модель Digital-CPTED построена методом теоретического моделирования, синтезирующим адаптированные принципы в целостную превентивную архитектуру.

1.2. Эволюция и ключевые принципы концепции CPTED

Теоретические основы CPTED разработаны во второй половине XX века. Идея Джейн Джекобс [6] о «глазах на улице» как факторе естественного неформального контроля и теория «защищаемого пространства» Оскара Ньюмена [7], продемонстрировавшая связь архитектурных решений с уровнем преступности, заложили фундамент средового подхода. Сам термин и первая систематизация принципов принадлежат К. Рэю Джеффри [8]. В современной парадигме CPTED опирается на криминологические теории рационального выбора [9], рутинной активности [10] и возможностей, воздействуя на их элементы через изменение среды.

Ключевыми принципами концепции выступают: «естественный надзор», обеспечивающий видимость и наблюдаемость; «территориальность», укрепляющая чувство хозяина и чёткие границы пространств; «контроль доступа», физически ограничивающий вход для неавторизованных лиц; «поддержание и качество среды», демонстрирующее заботу о территории и родственное теории «разбитых окон»; а также «легитимная активность», поощряющая социально-одобряемое поведение.

В российской криминологии выделяется дихотомия двух путей развития подхода: создание «защищающего пространства», ориентированного на социальную активность и общинный контроль, и «защищенного пространства», основанного на тотальном формальном и техногенном контроле [3]. Этот выбор определяет философию проектирования — способствовать ли интеграции и ответственности или вести к изоляции и стигматизации.

Несмотря на доказанную эффективность, CPTED подвергается критике за риск смещения преступности [11, с. 329], возможную социальную изоляцию и фортификацию, ведущую к созданию «стерилизованных» пространств, где безопасность обеспечивается ценой отчуждения и вытеснения человеческого взаимодействия [3, с. 6–7]. Эти ограничения подчёркивают необходимость сбалансированного применения. Современные трактовки, такие как «CPTED третьего поколения», смещают фокус с механистического контроля на создание сред, способствующих благополучию и социальной активности. Именно эта социально-ориентированная парадигма — модель «защищающего цифрового пространства» — избирается в качестве методологической основы для адаптации CPTED к цифровой среде в данном исследовании.

2. Цифровое пространство социальных сетей как новая криминогенная среда и объект проектирования

Трансформация социальных сетей из инструмента коммуникации в полноценную социальную среду обитания приводит к необходимости их криминологического осмысления в качестве особой криминогенной среды. Ее специфика обусловлена не физическими, а цифровыми и социально-психологическими свойствами, которые создают уникальный комплекс детерминант преступного и деструктивного поведения. В контексте инвайронментальной криминологии цифровая среда перестает быть нейтральным фоном, а становится активным фактором, формирующим поведенческие паттерны и возможности для правонарушений [4, 5].

2.1. Криминологическая характеристика цифровой среды социальных сетей

Социальные сети, трансформировавшись в полноценную социальную среду, обладают специфическими свойствами, которые формируют их криминогенный потенциал [12, С. 207]. Их ключевые свойства — нормированная анонимность и алгоритмическая виральность. Анонимность ослабляет внутренние сдерживающие механизмы и чувство ответственности. Алгоритмы, стремящиеся к максимальному вовлечению, непредвзято продвигают эмоционально заряженный, в том числе деструктивный, контент, делая троллинг ресурсом в «экономике внимания».

Эти особенности усугубляются масштабируемостью вреда и кризисом социальных сигналов. Одно действие может мгновенно достичь миллионов, а диффузия ответственности в коллективных актах минимизирует чувство личной вины. Отсутствие невербальных маркеров и физических ограничителей облегчает эскалацию конфликтов, устраняя «естественный надзор». В итоге формируется среда с высокой виктимогенностью, где личные границы легко преодолеваются, а пользователи лишены инструментов оценки рисков. Криминогенный потенциал реализуется и через латентную «архитектуру выбора» — дизайн, предопределяющий простые и социально одобряемые действия, системно направляя поведение.

2.2. Обоснование возможности криминологически-ориентированного проектирования

Если цифровая среда обладает свойствами, способствующими преступлению, то её дизайн должен рассматриваться не как нейтральный технологический фон, а как активный объект криминологического проектирования и правового регулирования. Логика ситуационной профилактики, доказавшая свою эффективность в физическом мире, применима и здесь, поскольку она апеллирует к универсальным механизмам принятия решений потенциальным правонарушителем и потенциальной жертвой: оценке риска, усилий, выгод и провоцирующих сигналов среды [5].

Исторический опыт осознанного проектирования городской среды для безопасности позволяет применить адаптированный подход к цифровому пространству. Концепции «цифровой территориальности», «цифрового естественного надзора» и «контроля цифрового доступа» предполагают установление чётких границ приватности, прозрачность действий и многоуровневые системы доступа. Таким образом, социальная сеть становится не просто технологией, а политико-правовым проектом. Её архитектура должна отвечать не только коммерческим целям, но и нормам публичной безопасности, защиты прав граждан и минимизации рисков. Это формирует теоретическую основу для адаптации принципов безопасного проектирования среды в цифровую эпоху.

3. Адаптация принципов CPTED к дизайну социальных сетей: концептуальная модель Digital-CPTED

Основываясь на философии «защищающего цифрового пространства», концепция Digital-CPTED предлагает системную адаптацию классических принципов предупреждения преступности к архитектуре социальных сетей. Данный подход фокусируется не на изоляции и всеобщем контроле, а на усилении социального капитала, прозрачности и ответственности пользователей через изменение самой «архитектуры выбора».

3.1. Цифровой естественный надзор

Ключевой тезис цифрового естественного надзора заключается в создании прозрачной среды, где действия пользователей имеют социальную заметность, что повышает субъективные риски обнаружения для потенциального нарушителя. Это достигается не через скрытый мониторинг, а путем внедрения видимых механизмов обратной связи, выполняющих функцию «цифровых очевидцев». На практике это реализуется в системах публичной социальной репутации, формируемых на основе истории конструктивных взаимодействий, аналогично репутации в физическом сообществе. Технически таким механизмом может стать децентрализованный протокол верификации действий на базе смарт-контрактов, где ключевые социально значимые действия (например, успешное посредничество в конфликте, создание высокооцененного экспертного контента) фиксируются в виде неизменяемых транзакций с цифровой подписью участников. Это создаст устойчивый, независимый от центральной платформы и защищенный от манипуляций «цифровой след» добросовестного поведения, который может учитываться при оценке доверия в различных сообществах внутри платформы. Дополнительным элементом является видимая маркировка действий модераторов и сохранение истории редактирования материалов, создающее эффект присутствия «цифрового патруля» и усиливая коллективную ответственность.

3.2. Цифровая территориальность создает у пользователей чувство ответственности за их виртуальные «владения», преодолевая анонимность сети. Он превращает абстрактный профиль или сообщество в четкую цифровую территорию с защищенными границами, нарушение которых становится заметным и технически сложным.

Техническим воплощением выступают гранулярные настройки приватности, позволяющие пользователю самостоятельно определять вариант доступа к своей личной информации, и визуальная маркировка типов пространств (открытые/закрытые группы). Инновационным развитием этого принципа может стать механизм «цифровых правоустанавливающих сигналов» для администраторов сообществ. По аналогии с публичной регистрацией прав на недвижимость, администратор крупного сообщества мог бы добровольно и публично регистрировать в специальном реестре платформы базовые правила, миссию и принципы модерации своего «цифрового муниципалитета». Это создавало бы прозрачные ожидания для пользователей, упрощало бы разрешение споров и повышало бы легитимность и ответственность модераторов, трансформируя их роль из неформальных «сторожей» в публично подотчетных «управляющих цифровой территорией».

3.3. Контроль цифрового доступа. Принцип контроля цифрового доступа предполагает сознательную сег-

ментацию пространства и установление обоснованных, многоуровневых барьеров, которые повышают субъективные «усилия» и организационные сложности для потенциального нарушителя, не создавая чрезмерных препятствий для рядового пользователя. Его фундаментом является многоуровневая верификация, привязанная к устойчивым цифровым идентификаторам, что служит основой для установления ответственности. Помимо стандартной практики (многофакторная аутентификация, функциональные ограничения для новых аккаунтов), перспективным механизмом может стать система динамического контекстуального доступа. Например, возможность совершать действия с высоким потенциалом влияния (массовая рассылка сообщений в крупном сообществе, создание опроса на всю платформу) могла бы предоставляться не просто на основе статической верификации, а по результатам анализа цифрового «портфеля доверия» пользователя. Такой портфель агрегировал бы данные о его репутации (принцип надзора), стаже ответственного администрирования «территорий» (принцип территориальности) и истории конструктивных публикаций. Таким образом, доступ к мощным инструментам стал бы производным от длительной социально одобряемой активности, а не результатом простой регистрации, что радикально повысило бы порог входа для злоумышленников.

3.4. Качество и поддержание цифровой среды. Принцип качества и поддержания цифровой среды отражает необходимость постоянного и, что критически важно, видимого для пользователя поддержания порядка, что само по себе служит мощным сигналом об управляемости пространства и коллективном неприятии деструктивных норм. Техническая реализация объединяет реактивные меры (приоритетное удаление спама, фейковых аккаунтов) и превентивные алгоритмические инструменты (исключение деструктивного контента из рекомендательных лент). Ключевым инновационным кейсом здесь является внедрение алгоритмов предиктивной санации среды на основе сетевого анализа. Вместо пассивной реакции на уже нанесенный ущерб, система могла бы в режиме, близком к реальному времени, выявлять формирующиеся координированные сети аккаунтов, демонстрирующих паттерны, характерные для будущих атак (например, синхронное вступление в сообщество, схожие паттерны низкоуровневого негативного комментирования). На основе этой аналитики платформа могла бы применять превентивные, но мягкие меры — например, временно ограничивать видимость контента от такой зарождающейся сети для остального сообщества до завершения автоматизированной и/или модераторской проверки. Это позволило бы «подметать цифровой мусор» до того, как он заполонит информационное пространство, реализуя цифровой аналог теории «разбитых окон» на прогностическом уровне.

3.5. Синтез принципов: комплексная модель «защищающего цифрового пространства». Эффективность Digital-CPTED заключается в синергетическом взаимодействии её принципов, создающем целостную превентивную архитектуру. Например, децентрализованная репутация служит основой для динамического контроля доступа, а данные сетевого анализа помогают укреплять цифровую территориальность сообществ. В совокупности эта модель изменяет баланс выгод и рисков для потенциального нарушителя, повышая предполагаемые усилия и вероятность обнаружения. Одновременно она снижает риски и усиливает защиту законопослушного пользователя. Таким образом, концепция предлагает философию проектирования, переносящую фокус профилактики с запоздалого преследования индивидов на проактивное структурирование среды, в которой принимаются поведенческие решения.

4. Место Digital-CPTED в системе предупреждения преступности и правовые границы ее применения

Концепция Digital-CPTED не может существовать изолированно и должна быть интегрирована в комплексную систему профилактики преступности с учётом правовых и этических ограничений. Её внедрение требует чёткого определения места не только в национальной системе профилактики, но и в контексте формирующихся глобальных парадигм цифровой безопасности.

4.1. Digital-CPTED как инструмент ситуационной и общинной профилактики в цифровой среде

Сравнительный анализ показывает, что предлагаемая модель концептуально соотносится с международными подходами, такими как «Safety by Design» (проактивное внедрение безопасности) [13], «Digital Citizenship» (ответственность пользователей) [14]. Ключевое отличие Digital-CPTED в том, что это не просто рекомендации, а целостная криминологическая система для проектирования. Она напрямую переносит проверенные принципы предотвращения преступлений в цифровую среду, создавая теоретическую основу для снижения рисков через дизайн интерфейсов и алгоритмов.

Концепция Digital-CPTED занимает стратегическую позицию на уровне ситуационной и общинной профилактики преступности. В отличие от работы с конкретным лицом, она изменяет характеристики самой среды, в которой возникает преступный умысел. По сравнению с реактивными правоохранительными мерами, Digital-CPTED выполняет превентивную функцию, снижая число инцидентов и разгружая систему. Одновременно она реализует виктимологическую профилактику, делая цифровую среду безопаснее по своей архитектуре. Таким образом, концепция занимает место между общими социальными мерами и уголовной репрессией, предлагая проак-

тивный слой профилактики на основе криминологически обоснованного проектирования цифровой среды.

4.2. Правовые и этические границы: вызовы «правового» киберпространства

Внедрение Digital-CPTED порождает серьезные правовые и этические вызовы. Главная проблема — это коллизия с правами на приватность, поскольку сбор поведенческих данных создает риск тотальной прозрачности. Существует также риск непрозрачной частной цензуры со стороны корпораций, управляющих дискурсом по неясным критериям. Дополнительным вызовом является алгоритмическая стигматизация, которая может противоречить принципу презумпции невиновности. Наконец, сложности добавляет трансграничность и конфликт национальных правовых систем, что создает юрисдикционную неопределенность при попытках внедрения единых стандартов.

4.3. Гибридная правовая модель для Digital-CPTED: между государством, рынком и сообществом

Учитывая правовые и этические вызовы, внедрение Digital-CPTED требует гибридной модели, балансирующей между государственным регулированием, корпоративной ответственностью и правами сообщества пользователей. Государство может задать вектор через «безопасное регулирование по дизайну», устанавливая законодательные стандарты безопасности цифровых платформ. Ключевым условием становится трансграничная прозрачность и подотчётность, обязывающая платформы отчитываться о работе алгоритмов. Для обеспечения доверия необходим независимый аудит с привлечением экспертов. Законодательство должно также гарантировать пользователям усиленные процессуальные права и доступ к механизмам цифрового правосудия. Таким образом, правовое оформление концепции становится процессом конструирования новой цифровой реальности, требующим сбалансированного участия всех сторон.

Заключение

Концепция Digital-CPTED — это научный подход к проактивному предупреждению преступности через адаптацию принципов ситуационной профилактики к архитектуре социальных сетей. Она призвана изменить баланс рисков и выгод для потенциальных нарушителей и снизить виктимогенный потенциал среды.

Проведенный анализ показывает, что уникальные свойства цифрового пространства требуют целенаправленного проектирования безопасных сред. Концепция предлагает конкретные инструменты, которые формируют устойчивую превентивную архитектуру.

Внедрение Digital-CPTED сопряжено с правовыми и этическими вызовами. Для минимизации этих рисков необходима гибридная модель регулирования.

Таким образом, Digital-CPTED является основой для формирования безопасной, инклюзивной и ответственной цифровой экосистемы. Дальнейшие исследования должны сосредоточиться на разработке конкретных технических решений, правовых механизмов и международно-правовых рамок.

ЛИТЕРАТУРА

1. МВД России: каждое третье преступление в стране связано с интернетом [Электронный ресурс] // Инфофорум. 2025. 10 сен. — URL: https://infoforum.ru/glavnoe/mvd-rossii-kazhdoe-trete-prestuplenie-v-strane-svjazano-s-internetom (дата обращения: 09.01.2026).
2. Степанова М. Н. Регулирование правоотношений в эпоху цифровой трансформации // Правопорядок: история, теория, практика. 2025. № 1 (44). С. 44–49. DOI: 10.47475/2311-69.
3. Разогреева А.М. Предупреждение преступлений при помощи средового проектирования: защищающее пространство и защищенное пространство / А.М. Разогреева // Всероссийский криминологический журнал. 2017. Т. 11, № 4. С. 706–716. DOI: 10.17150/2500-4255.2017.11(4).706-716.
4. Кузьменков В.А. Влияние экологической ситуации на преступность в мире и в регионах Российской Федерации //Ex jure. 2024. № 3. С. 153–165. DOI: 10.17072/2619-0648-2024-3-153-165.
5. Радостева, Ю.В. Жертва и пространство / Ю.В. Радостева // Правопорядок: история, теория, практика. 2021. № 1 (28). С. 90–93.
6. Jacobs J. The death and life of great American cities / Jane Jacobs. — New York: Vintage books, Cop. 1961. — 458 с.
7. Newman Oscar Defensible space Crime prevention through urban des. / Oscar Newman. — New York: Collier books, 1973. — XVIII, 264 с. ил.; 23.
8. Jeffery, C.R. (1971). Crime Prevention through Environmental Design. Beverly Hills, CA: Sage Publications.
9. Cornish, Derek B., and Ronald V. Clarke, editors. The Reasoning Criminal: Rational Choice Perspectives on Offending. Springer-Verlag, 1986.
10. Cozens PM, Saville G, Hillier D (2005), «Crime prevention through environmental design (CPTED): a review and modern bibliography». Property Management, Vol. 23 No. 5 pp. 328–356, doi: https://doi.org/10.1108/02637470510631483.
11. Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(August), 588–608.
12. Шут О.А. Свойства социальных сетей как фактор их криминализации // Прокурорский надзор и криминология. — 2022. — № 3. — С. 207–216. — DOI: 10.24412/2227-7315-2022-3-207-216.
13. Safety by Design (SbD) [Электронный ресурс] // Всемирный экономический форум. — URL: https://www.weforum.org/projects/safety-by-design-sbd/ (дата обращения: 07.01.2026).
14. Be Internet Awesome — A Program to Teach Kids Online Safety [Электронный ресурс] // Google. — URL: https://beinternetawesome.withgoogle.com/ (дата обращения: 07.01.2026).