СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ __

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ ИМЕНИ А.Я. СУХАРЕВА

ПРАВОВЫЕ АСПЕКТЫ БОРЬБЫ С ПРОЯВЛЕНИЯМИ КИБЕРЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Всероссийский круглый стол

(посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова)

29 мая 2026 года

Москва 2026

УДК 343
ББК 67.408

Н34 **Правовые аспекты борьбы с проявлениями киберэкстремизма и терроризма в молодежной среде**: материалы Всероссийского круглого стола, посвященного памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова (Москва, 29 мая 2026 г.). М.: Московская академия Следственного комитета имени А.Я. Сухарева, 2026. – 118 с.

Сборник сформирован по материалам, представленным участниками всероссийского круглого стола, проведенного в Московской академии Следственного комитета имени А.Я. Сухарева 29 мая 2026 года. В круглом столе приняли участие представители разных вузов, практические работники из разных ведомств и ученые по научной специальности 5.1.4 – Уголовно-правовые науки.

Сборник предназначен для юристов – учёных и практиков, а также для всех тех, кто интересуется вопросами борьбы с экстремизмом и терроризмом, и в частности – с киберэкстремизмом.

Редакционная коллегия обращает внимание, что научные подходы, идеи и взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

Правовые аспекты борьбы с проявлениями киберэкстремизма и терроризма в молодежной среде

Всероссийский круглый стол, посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова
(29 мая 2026 года)

В Московской академии Следственного комитета имени А.Я. Сухарева состоялся всероссийский круглый стол «Правовые аспекты борьбы с проявлениями киберэкстремизма и терроризма в молодежной среде», посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова.

В работе круглого стола приняли участие представители ведущих высших учебных заведений страны.

Модераторы круглого стола – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции Бычкова Екатерина Игоревна и доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, полковник юстиции Скобелин Сергей Юрьевич.

С приветственным словом к участникам конференции обратились *Владимир Антонович Прорвич* – профессор-исследователь Департамента уголовного права, процесса и криминалистики НИУ ВШЭ, почётный профессор Московской академии Следственного комитета имени А.Я. Сухарева, который отметил вклад Василия Васильевича Бычкова в создание Академии, развитие юридической науки в России и в разработку государственной программы борьбы с киберэкстремизмом.

В.А. Прорвич отметил: «Василий Васильевич Бычков большое внимание уделил в своих многочисленных научных трудах сбору самого разнообразного эмпирического материала, связанного с преступлениями рассматриваемого вида, включая не только изучение особенностей уголовных дел, завершенных расследованием и рассмотренных судами, но и многочисленные опросы не только следователей, но и различных групп представителей той молодежной среды, на которую и нацеливались организаторы экстремистских преступлений различного вида. Здесь необходимо отметить ту колоссальную организационную работу, которую провел В.В. Бычков, а также неоценимую помощь в организации опросов представителей МВД России, которую оказал профессор А.Ф. Волынский».

Среди выступающих – начальник кафедры теории государства и права Московского университета МВД России имени В.Я. Кикотя *Алексей Иванович Клименко*; профессора Президентской академии (РАНХиГС) *Сергей Борисович Вепрев* и *Александр Павлович Опальский,* которые уделили внимание в своих

выступлениях значительному вкладу В.В. Бычкова в решение проблем профилактики идеологии терроризма и киберэкстремизма.

Круглый стол стал эффективной площадкой для обсуждения вопросов борьбы с киберэкстремизмом и терроризмом в молодежной среде и диалога между учеными различных научных специальностей.

Оргкомитет конференции

Е.И. Бычкова[1]

ГОСУДАРСТВЕННО-ПРАВОВЫЕ АСПЕКТЫ МНОГОСТУПЕНЧАТОЙ ПРОФИЛАКТИКИ КИБЕРЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Аннотация. В статье раскрываются некоторые аспекты профилактики киберэкстремизма в молодежной среде. Предлагается выделять несколько ступеней профилактики, первой из которых является совершенствование правовой базы профилактики, второй – разработка воспитательно-образовательных мер и их реализация и третьей – реабилитация лиц, подвергнутых деструктивному воздействию

Ключевые слова: киберэкстремизм, профилактика, молодежная среда, реабилитация.

Стремительный рост числа пользователей информационно-телекоммуникационных сетей и общая тенденция к переходу многих общественных отношений в виртуальную среду, несомненно, имеет свои положительные стороны, однако создает почву для возникновения и новых форм совершения преступлений, в частности, широкому распространению экстремистского контента.

Отмечается, что наиболее активно вербовщики в экстремистские организации осуществляют свою деятельность среди социально незрелого слоя населения – молодежи. Именно молодежная среда стала благоприятной для распространения деструктивной идеологии экстремизма и не только в силу психологических, социальных особенностей молодых людей, но и благодаря алгоритмам социальных сетей, игровых платформ и мессенджеров.

Эмпирические данные подтверждают высокую степень уязвимости молодёжи в цифровом пространстве. По результатам анонимного анкетирования, проведённого В.В. Бычковым среди школьников, студентов и курсантов, аспирантов:

- значительная часть опрошенных демонстрирует недостаточный уровень критического восприятия интернет-контента;
- наблюдается латентная подверженность экстремистской пропаганде;
- выявлены случаи участия молодых людей в группах деструктивной направленности без осознания противоправности таких действий.

Несмотря на то, что по данным МВД России количество киберпреступлений в 2026 году существенно снизилось по сравнению с аналогичным периодом (январь-май) 2025 года (на 31%), степень их общественной опасности остается высокой. Благодаря профилактической работе правоохранительных органов, проводимой в информационно-телекоммуникационных сетях, снизилось количество совершаемых мошенничеств, краж, преступлений, связанных с распространением наркотических средств и психотропных веществ. Однако, МВД России отмечает рост преступлений экстремистской направленности в 2025 году, который составил более 30%. Об этом говорил и Генеральный

[1] Бычкова Екатерина Игоревна – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

прокурор РФ А.В. Гуцан на пленарном заседании Совета Федерации Федерального Собрания РФ 15 апреля 2026 года[1]. В докладе отмечается, что Роскомнадзор по требованию прокуратуры заблокировал доступ к 62 тысячам интернет-страниц с экстремистским содержанием.

Скорость распространения деструктивного контента не всегда позволяет правоохранительным органам своевременно принимать профилактические меры. На сегодняшний день, к сожалению, профилактика ограничивается блокировкой страниц в сети «Интернет», которые пропагандируют запрещенную в России идеологию экстремизма.

Представляется, что во многом такая ограниченность возможностей правоохранительных органов в реализации профилактических мер против распространения киберэкстремизма в молодежной среде связана с отсутствием единого, комплексного подхода к модели профилактики. Меры государственного реагирования на данную форму деструктивного воздействия должны быть последовательными и многоступенчатыми.

В условиях гибридных войн и геополитической нестабильности киберэкстремизм становится одной из ключевых угроз национальной безопасности, требующей переосмысления правовых и организационных механизмов противодействия.

В данной работе, под киберэкстремизмом будет пониматься системно организованные, целенаправленные, общественно опасные, сознательно совершаемые информационные индивидуальные или групповые атаки на сознание и психику неограниченного количества пользователей социальных сетей и других современных средств электронной информации, совершаемые с использованием компьютеризованных устройств, современных информационных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет, с целью возбуждения общественно опасных политических, идеологических, расовых, национальных, религиозных ненависти или вражды, а также ненависти или вражды в отношении какой-либо социальной группы, сопровождаемые соответствующими организационными, техническими и финансовыми мерами, запрещенные рядом уголовно-правовых норм Особенной части Уголовного кодекса РФ. [2]

Отметим, что профилактическая работа должна быть комплексной в масштабном межведомственном взаимодействии.

Предлагается выделить три основных уровня профилактики, которые будут последовательно реализоваться органами публичной власти во взаимодействии друг с другом:

1. Государственно-правовое регулирование – то есть создание юридического фундамента профилактической работы.

---

[1] Пленарное заседание Совета Федерации. Парламентская газета. URL: https://www.pnp.ru/social/genprokuror-kolichestvo-ekstremistskikh-prestupleniy-v-2025-godu-vyroslo-na-30.html

[2] Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. – 2024. – № 2. – С. 54-58.

2. Работа по снижению уязвимости молодых людей перед угрозой вовлечения в экстремистскую деятельность (воспитательно-образовательные меры).

3. Реабилитирующие меры – то есть создание платформы для работы с молодёжью, пострадавшей от деструктивного воздействия и создания условий возвращения их в социум.

Первый уровень – ключевой и определяющий. Новеллами российского законодательства в сфере профилактики киберэкстремизма стали ужесточение уголовной ответственности за вовлечение несовершеннолетних в совершение преступлений с использованием информационно-телекоммуникационных сетей, с увеличением срока наказания до 10 лет за квалифицированные составы.

Представляется, что прежде, чем обеспечивать правовое регулирование профилактики киберэкстремизма в молодежной среде, необходимо систематизировать и постоянно актуализировать перечь угроз, исходящих от цифровой среды. Совершенствование юридической базы профилактики не должно сводиться лишь к ужесточению ответственности, а должно включать в себя четкие процедуры выявления, фиксации и блокировки экстремистского контента.

Интеграция высоких технологий, включая элементы искусственного интеллекта, в деятельность по мониторингу сети «Интернет», должна сопровождаться чёткими правовыми рамками, обеспечивающими баланс между эффективностью профилактики и защитой конституционных прав граждан.

Субъектами профилактической работы будут выступать:

- государственные органы и органы местного самоуправления;
- образовательные организации;
- правоохранительные органы;
- общественные организации;
- органы социальной защиты и здравоохранение.

Второй уровень – это вклад государства в формирование молодежной среды, устойчивой к воздействию деструктивных идеологий. На данном уровне должна проводится планомерная, системная работа, в ходе которой необходимо проводить следующие мероприятия:

- развитие и укрепление правовой культуры молодежи (изучение в школах текста Конституции России, возвращение в учебные планы дисциплины «Обществознание» в школах с 5 класса, проведение во всех учебных заведениях страны праздничных мероприятий ко Дню Конституции);
- развитие медиа грамотности и критического мышления молодежи;
- создание платформ по вовлечению молодых людей в позитивные формы гражданской активности (проведение квестов, игр, например на тему «Мэр двора», стартапов по благоустройству территории, создание клубов IT-волонтеров, чья работа заключалась бы в отыскании фишинговых сайтов и фейков за призовые места в конкурсе «Детектив-месяца»). Следует обратить внимание, что такие формы социальной активности и активной гражданской позиции позволят «привязать» молодежь к месту, где они проживают, а, как думается, разрушать место, к которому есть эмоциональная привязка сложнее.

На уровне местного самоуправления в муниципальных образованиях можно учредить премию «Поступок» в социальных сетях муниципалитета, где каждый год будут избирать самого «полезного» представителя молодежной среды и поощрять, например, встречей с известной личностью;

- разработка маркеров вербовочного поведения и начиная с 1 класса школы говорить о них, ежегодно дополнять и обновлять с учетом формирования с течением времени новых форм работы вербовщиков;

- формирование корпуса профессиональных специалистов, деятельность которых будет направлена на профилактическую работу;

- введение системы оценки эффективности профилактической работы.

Третий уровень – практические меры реабилитации молодежи, пострадавшей от деструктивного влияния экстремистов.

На данном уровне можно выделить несколько этапов работы – адаптация, терапия, реинтеграция.

Ключевыми направлениями реабилитации могут стать следующие:

- работа психолога (проработать психотравмирующую ситуацию и скорректировать эмоциональные проблемы);

- важным аспектом работы с пострадавшими является восстановление представлений о мире, системе отношений между людьми, семье и традиционных ценностях, поэтому следует уделять внимание идейно-патриотическому и духовно-нравственному воспитанию;

- межведомственное взаимодействие. Создание единого механизма взаимодействия учреждений для реализации программ ресоциализации испытывает определенные сложности, для эффективного преодоления которых необходимо одновременное участие психологов, педагогов и социальных работников.

Список источников

1. Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. – 2024. – № 2. – С. 54-58.
2. Пленарное заседание Совета Федерации. Парламентская газета. URL: https://www.pnp.ru/social/genprokuror-kolichestvo-ekstremistskikh-prestupleniy-v-2025-godu-vyroslo-na-30.html

В.Ф. Васюков[1]
А.А. Титов[2]

ОПЕРАТИВНО-РОЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ БЕСКОНТАКТНОМУ СБЫТУ НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Аннотация. В статье на основе изучения и обобщения практики рассматривается соотношение сетевых сведений и наблюдения при выявлении бесконтактного сбыта наркотических средств. Цифровая организация такой деятельности анализируется не как замена физической передачи, а как распределение заказа, расчёта, перемещения и помещения наркотического средства в тайник между различными участниками. Изученные материалы позволяют определить условия, при которых сведения об учётных записях, платежах, координатах и изображениях приобретают проверяемую связь с лицом, транспортным средством, помещением и изъятым веществом. Особое внимание уделено пределам наблюдения, документированию последовательности полученных данных и ситуации параллельной оперативной разработки одного объекта. Обосновано различие между результатом оперативно-розыскной проверки и обстоятельствами, которые подлежат самостоятельному процессуальному доказыванию. Результаты изучения российской практики сопоставлены с отдельными положениями международной практики для определения условий, при которых обмен цифровыми сведениями способствует установлению материальных стадий наркосбыта.

Ключевые слова. Оперативно-розыскная деятельность, бесконтактный сбыт наркотических средств, наблюдение, тайник (закладка), теневой сегмент сети «Интернет», цифровые следы, организованная группа, параллельные оперативные разработки.

Изучение практики выявления бесконтактного сбыта показывает, что заказ наркотического средства, расчёт и его фактическая передача могут распределяться между участниками организованной группы. Интернет-магазин обеспечивает размещение предложений и обмен сообщениями, цифровая валюта используется для оплаты, а сведения о тайнике направляются после подтверждения платежа. Непосредственная встреча сбытчика с приобретателем из этой последовательности исключается, однако сам предмет требуется получить, расфасовать, переместить и скрыть в определённом месте. Полученные результаты позволяют характеризовать бесконтактность прежде всего как распределение цифровых и материальных действий, а не как их полное перемещение в информационно-телекоммуникационную сеть. Такое различение задаёт и направление оперативной проверки, поскольку наблюдаемыми остаются лица, помещения, транспорт и операции с наркотическим средством.

Статистические данные обозначают масштаб технологически опосредованного наркооборота, но не раскрывают структуру каждого способа

[1] Васюков Виталий Федорович – главный научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета имени А.Я. Сухарева, доктор юридических наук, профессор.
[2] Титов Андрей Александрович – начальник отдела УРОПД Следственного департамента МВД России, кандидат юридических наук.

сбыта. В 2024 г. в Российской Федерации зарегистрировано 193 тыс. преступлений, связанных с незаконным оборотом наркотиков, в том числе 135 тыс. фактов сбыта. Количество наркопреступлений, совершённых с использованием информационно-телекоммуникационных технологий и сети «Интернет», достигло 118,2 тыс. и превысило показатель предыдущего года на 13,6 процента[1]. Эта категория включает различные формы применения технологий, поэтому её нельзя непосредственно отождествлять с продажей через тайники. Тем не менее соотношение показателей даёт основание рассматривать переход от сетевых данных к конкретным лицам, маршрутам и местам хранения как устойчивую, а не исключительную задачу оперативных подразделений.

В научной литературе цифровая сторона бесконтактного сбыта раскрывается через анонимизацию участников, защищённые каналы связи, безналичные расчёты и порядок фиксации электронных данных. Е.А. Усачева связывает использование информационно-телекоммуникационных технологий с изменением способов организации незаконного оборота и возникающими трудностями его выявления[2]. М.М. Шакирьянов обращает внимание на комплекс оперативно-розыскных мероприятий и необходимость документирования отдельных стадий взаимодействия[3]. Вместе с тем изолированное рассмотрение сетевой коммуникации оставляет за пределами объяснения перемещение самого наркотического средства. Обобщение практики уточняет содержание комплексного подхода. Его образует не количество проведённых мероприятий, а проверяемая связь учётной записи и заказа с действиями лица, автомобилем, помещением и тайником.

Эмпирическую основу статьи составили результаты изучения и обобщения практики выявления и расследования бесконтактного сбыта наркотических средств, осуществляемого межрегиональными организованными группами[4]. При отборе материалов учитывались ситуации, в которых заказ, расчёт и физическое перемещение наркотического средства распределялись между участниками и несколькими территориями. Персональные данные и сведения, раскрытие которых могло бы причинить вред оперативно-служебной деятельности, в статье не воспроизводятся. Состав изученных материалов не позволяет распространять выявленные особенности на все формы бесконтактного сбыта. Он достаточен для анализа повторяющихся способов

---

[1] Совет Безопасности Российской Федерации. Секретарь Совета Безопасности Российской Федерации Сергей Шойгу в интервью агентству ТАСС. 25 апреля 2025 г. [Электронный ресурс]. URL: https://www.scrf.gov.ru/news/speeches/3804/ (дата обращения: 27.07.2026).

[2] Усачева Е.А. Влияние информационно-телекоммуникационных технологий на незаконный оборот наркотических средств и психотропных веществ: криминалистический анализ // Вестник Восточно-Сибирского института МВД России. 2023. № 3 (106). С. 244-253.

[3] Шакирьянов М.М. Особенности проведения оперативно-розыскных мероприятий по выявлению и раскрытию бесконтактного сбыта наркотических средств // Вестник Самарского юридического института. 2019. № 2 (33). С. 92-96.

[4] Изучение и обобщение практики проведено авторами по материалам выявления и расследования межрегионального бесконтактного сбыта наркотических средств. Персональные данные и сведения ограниченного доступа в статье не воспроизводятся.

получения и проверки сведений, а также организационных затруднений, возникающих при межрегиональном характере деятельности.

Обобщение практики показывает, что территория совершения отдельных эпизодов не всегда совпадает с территорией управления сбытом. Одни участники получают оптовые партии, другие обеспечивают фасовку, третьи перевозят свёртки и помещают их в тайники. Организационные указания могут исходить из другого региона, тогда как расчёт и физическое перемещение наркотического средства могут не совпадать по времени. Вследствие этого место обнаружения тайника характеризует конкретный эпизод, но не позволяет само по себе установить структуру группы. Связь между эпизодами выявляется после сопоставления ролей, учётных записей, способов упаковки, маршрутов и расчётных операций. Практический предел территориальной проверки здесь состоит в том, что локальный объект приобретает объяснительное значение лишь в совокупности со сведениями, полученными за пределами соответствующего региона.

В одном из изученных материалов деятельность интернет-магазина продолжалась с 2013 г. и последовательно перемещалась между несколькими площадками теневого сегмента сети. Предложения размещались на «RAMP», с 2015 г. - на «Hydra», а после прекращения её работы в апреле 2022 г. - на других ресурсах, включая «Solaris» и «Kraken». При смене площадки сохранились распределение функций, поставщики, помещения, способы фасовки и логистические связи. Это обстоятельство ограничивает выводы, которые могут основываться на факте блокирования отдельного сетевого ресурса. Площадка выполняла функции витрины и канала связи, но организационная устойчивость поддерживалась людьми и материальными средствами вне её инфраструктуры. Поэтому прекращение доступа к ресурсу способно осложнить сбыт, не исключая его возобновления на иной технической основе.

Разделение труда снижало объём сведений, доступных отдельному исполнителю. В изученных материалах выделялись руководители, операторы, кураторы, лица, выполнявшие расчётные функции, кладовщики, фасовщики и курьеры. Участники нижнего уровня могли знать только конкретную партию, маршрут и учётную запись куратора. Инструкции передавались через защищённые каналы связи, а отчётность включала сообщения, фотографии и координаты. Задержание одного исполнителя при такой организации не обязательно открывало сведения о других звеньях. По этой причине наименования ролей и показания отдельных лиц нуждались в сопоставлении с повторяемостью функций, системой расчётов, используемыми помещениями и движением партий. Именно устойчивость этих связей, а не формальное обозначение участника в переписке, имела значение для проверки группового характера деятельности.

Дистанционный набор исполнителей одновременно поддерживал сменяемость состава и создавал сведения об организации магазина. На сетевых ресурсах размещались предложения о выполнении отдельных функций, требования к кандидатам и условия вознаграждения. Содержание инструкций, правила упаковки, обозначение ролей и порядок отчётности повторялись при

вовлечении новых лиц. Эти данные могут характеризовать общий способ управления, однако их значение зависит от подтверждённого происхождения и связи с конкретным пользователем. Без такой проверки совпадение терминов или шаблонов сообщений остаётся ориентирующей информацией. При обобщении практики организационный вывод формировался после сопоставления цифровых записей с последующими действиями исполнителей, выплатами и обнаруженными предметами.

Средства конспирации применялись как к коммуникации, так и к операциям в физическом пространстве. Участники использовали псевдонимы, отдельные учётные записи, защищённые средства связи и цифровую валюту, меняли маршруты и проверяли возможное наблюдение. Для хранения и фасовки использовались квартиры, где были обнаружены весы, вакуумное оборудование, упаковочные материалы и маркированные свёртки. Изъятые партии включали мефедрон, кокаин, гашиш, каннабис, а также смеси метамфетамина и МДМА. Масса отдельных видов исчислялась килограммами. Перечисленные объекты выполняли неодинаковую доказательственную функцию. Вещество и оборудование раскрывали материальные операции, тогда как устройства и учётные записи использовались для проверки их связи с магазином и другими участниками.

При уличной передаче встреча сторон образует единое наблюдаемое событие, в котором могут быть одновременно зафиксированы участники и передаваемый предмет. Бесконтактный способ распределяет эти элементы по времени. Реклама и заказ размещаются на сетевой площадке, расчёт не сопровождается передачей наличных денег, а сведения о тайнике направляются после оплаты. Каждое действие, взятое отдельно, способно допускать нейтральное объяснение. Поэтому единицей оперативного наблюдения становится не встреча продавца и приобретателя, а последовательность взаимосвязанных эпизодов. Обоснованность вывода о назначении конкретного перемещения зависит от того, удалось ли соотнести его с заказом, координатами, изображением места и последующим обнаружением вещества.

Отсутствие личного контакта не устраняет физически необходимые стадии передачи. Получение партии, её разделение, упаковка, перевозка и помещение в тайник предполагают участие лица и использование помещений, транспорта, упаковочных материалов и устройств. При повторении этих действий возникают маршруты и устойчивые связи с определёнными объектами. Их наблюдаемость не означает, что любое посещение места либо перемещение предмета имеет преступное содержание. Значение таких фактов возникает после их сопоставления с иными данными. Изученные материалы показывают, что вещная природа наркотического средства создаёт возможность проверить сетевую информацию через физическую активность участников, не подменяя этой активностью доказательство конкретного эпизода.

Цифровые сведения и наблюдение выполняли взаимодополняющие функции. Переписка, данные о платеже, фотографии и координаты помогали определить предполагаемый объект и место дальнейших действий. Наблюдение давало сведения о перемещениях лица, используемых автомобилях, помещениях и

контактах с предметами. Ни один из этих источников не обладал заранее установленным приоритетом. Файл на устройстве не всегда указывает на фактического пользователя, а маршрут без связи с заказом не раскрывает назначения поездки. Аналитический результат возникал в точках совпадения независимых данных. Такой порядок уменьшает риск приписать цифровой записи либо наблюдаемому действию содержание, которое не подтверждается другими материалами.

В одном из изученных материалов после поступления первичной информации о возможной причастности нескольких лиц оперативное подразделение проводило наблюдение в течение нескольких суток. Были установлены маршруты, используемый автомобиль и квартира, связанная с хранением и фасовкой. Действия возле транспортного средства привлекли внимание к обшивке багажного отделения, где впоследствии обнаружили оборудованные места сокрытия. Сведения о перемещениях учитывались при выборе момента задержания, позволявшего сохранить предметы и исключить их дальнейшее распространение. В описанной ситуации наблюдение обеспечило переход от общей информации об интернет-магазине к индивидуализированным объектам. Его результативность определялась последующим обнаружением и процессуальной фиксацией, а не самим фактом продолжительного контроля.

Фактические возможности наблюдения расширялись за счёт городских систем видеофиксации и информационно-поисковых ресурсов, содержащих сведения о перемещении транспортных средств. Такие данные использовались для восстановления маршрута, проверки периодичности появления автомобиля и выбора дистанции сопровождения. В малолюдной местности непосредственное сближение повышало риск обнаружения сотрудников, поэтому обращение к техническим источникам позволяло сохранить непрерывность проверки. Сам вид оборудования не определял правовой режим полученных сведений. Для их последующего использования существенными оставались основание доступа, цель получения и принадлежность соответствующего действия к конкретному оперативно-розыскному мероприятию.

Федеральный закон «Об оперативно-розыскной деятельности» относит наблюдение к числу оперативно-розыскных мероприятий[1]. Применение видеозаписи и информационно-поисковых систем может расширять способы его проведения, не образуя нового мероприятия. П.В. Миненко и А.В. Пучнин, рассматривая массивы компьютерной информации как объект оперативно-розыскных мероприятий, обращают внимание на изменение фактических возможностей получения и обработки данных[2]. Из этого не следует единый режим доступа ко всем источникам. Открытое изображение, сведения ведомственной системы и охраняемая законом информация различаются по условиям получения. Их последующее объединение для сопоставления не

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 27.07.2026).

[2] Миненко П.В., Пучнин А.В. Массивы компьютерной информации как объект оперативно-розыскных мероприятий // Общество и право. 2020. № 4 (74). С. 87-91.

устраняет необходимости обосновать законность обращения к каждому исходному массиву.

Проверяемость результата зависит от того, насколько условия мероприятия соотнесены с характером затрагиваемых прав. В своей работе А.Е. Чечётин связывает законность оперативно-розыскных мероприятий с наличием предусмотренных оснований и соблюдением специальных условий их проведения[1]. Применительно к наблюдению это предполагает определённость объекта, периода и используемых средств, а также учёт режима получаемой информации. Мероприятия, ограничивающие конституционные права, не могут обосновываться теми же доводами, что и действия, не влекущие такого ограничения. Общая ссылка на противодействие организованному сбыту объясняет служебную цель, но не заменяет правового основания конкретного способа получения данных.

Документирование наблюдения приобретает смысл при сохранении последовательности, в которой возникали основания для дальнейших действий. Исходное сообщение, результаты его проверки, зафиксированные перемещения, обнаруженные совпадения и решение о проведении иных мероприятий отражают разные этапы получения знания об объекте. Если итоговый документ содержит только вывод о причастности, становится затруднительно проверить, на каких фактах он основан. Поэтому описание места, времени, способа идентификации автомобиля или лица и сохранение первичных записей имеют самостоятельное значение. Справка, подготовленная по памяти либо по неполному набору кадров, способна воспроизвести вывод сотрудника, но не восстанавливает утраченный источник.

Связь сетевых и физических действий наиболее отчётливо проявляется при использовании тайника. Его значение не исчерпывается местом обнаружения наркотического средства. Тайник завершает последовательность, включающую получение партии, расфасовку, перевозку, сокрытие и передачу приобретателю сведений о месте. Каждая стадия оставляет данные о времени, участниках и используемых предметах, хотя содержание этих данных неодинаково. В статье указанная последовательность обозначается как материально-предметное звено бесконтактного сбыта. Его выделение служит не созданию новой классификации, а определению тех действий, без которых цифровой заказ не может завершиться фактической передачей наркотического средства.

Материально-предметное звено следует отличать и от предмета преступления, и от совокупности уже образовавшихся следов. Наркотическое средство выступает предметом незаконных действий, тогда как звено характеризует операции с ним. Материальные следы фиксируют результат отдельных действий, но не всегда раскрывают предшествующую им последовательность. Например, сходство упаковки может связывать несколько партий после их изъятия, а наблюдение за перемещением упаковочного материала способно привести к помещению ещё до обнаружения готовых свёртков. Аналитическая

[1] Чечётин А.Е. Условия проведения оперативно-розыскных мероприятий: учебное пособие. Барнаул: Барнаульский юридический институт МВД России, 2023. 48 с.

функция этого различения состоит в выборе проверяемой стадии, а не в переименовании известных объектов.

В одном из изученных материалов фотографии участков местности и сохранённые координаты были обнаружены в телефоне и ноутбуке участника. Их проверка на месте привела к обнаружению тайника с наркотическим средством. Цифровая запись в этом эпизоде выполняла ориентирующую функцию, а наличие вещества подтверждалось осмотром, изъятием и экспертным заключением. Отдельной проверки требовала связь файла с устройством и пользователем. Само нахождение изображения на носителе не определяет время создания, источник получения и лицо, фактически использовавшее данные. Доказательственная связь формировалась посредством сопоставления цифрового объекта, результатов проверки места и иных сведений о действиях участника.

Распределённая организация сбыта побуждает участников создавать сведения, необходимые для внутреннего контроля. Исполнитель фотографирует тайник, сохраняет координаты и направляет отчёт, поскольку оператору требуется передать место приобретателю и подтвердить выполненную работу. Куратор учитывает количество размещённых свёртков и выплаты. Такие записи возникают как условие управления группой, несмотря на применяемую конспирацию. Их информативность, однако, зависит от контекста. Изолированное изображение местности допускает несколько объяснений, тогда как последовательность сообщения, координат, фотографии, сведений устройства и проверки места существенно сужает круг возможных интерпретаций.

Выбор между цифровыми и физическими источниками был бы методически неточным. Тайник, обнаруженный без связи с магазином, может остаться самостоятельным эпизодом, не раскрывающим управление группой. Сетевое наблюдение без выхода к предмету, напротив, не обеспечивает проверки фактической передачи. Изученные материалы показывают иную последовательность. Цифровые данные выделяли объект и позволяли прогнозировать его действия, наблюдение связывало их с помещениями и транспортом, а следственные действия закрепляли обнаруженные предметы и сведения. Значение источника определялось тем, какое обстоятельство он подтверждал и сохранялась ли возможность проверить его происхождение.

Относимость результатов оперативно-розыскной деятельности к событию преступления ещё не придаёт им статуса доказательств. Н.В. Макеева обращает внимание на достаточность и законность материалов уже на начальной стадии уголовного судопроизводства[1].

В специальной литературе представление и последующее процессуальное использование результатов рассматриваются как взаимосвязанные, но не

[1] Макеева Н.В. Документирование результатов оперативно-разыскной деятельности и их использование как повод и основание для возбуждения уголовного дела о незаконном сбыте наркотических средств бесконтактным способом с использованием информационно-телекоммуникационных сетей // Вестник Московского университета МВД России. 2019. № 5. С. 36-39.

тождественные этапы[1]. Для электронных данных это различие проявляется в необходимости сохранить носитель или иную проверяемую форму, описать способ получения и идентифицировать учётную запись. Процессуальное оформление не заменяет источник, а создаёт условия для проверки его происхождения, целостности и содержания.

Изучение практики выявило несоответствие между межрегиональной организацией сбыта и территориальным распределением оперативных сил. В отдельных ситуациях одни и те же лица независимо разрабатывались двумя подразделениями, получившими различную первичную информацию. О совпадении объектов стало известно только на поздней стадии. Такая параллельная работа не повлекла утраты результата, но создала риск взаимного обнаружения сотрудников и несогласованных действий при задержании. Этот факт не характеризует качество работы конкретного подразделения. Он указывает на организационное затруднение, возникающее тогда, когда перемещения участника и используемые им учётные записи выходят за пределы одной территории.

Один участник мог перемещаться между регионами, менять автомобили и использовать несколько учётных записей, поэтому сведения о нём поступали в разные органы. При отсутствии раннего сопоставления каждый фрагмент воспринимался как самостоятельный объект. Это вело не только к повторному расходованию сил. Наблюдение одного подразделения могло быть ошибочно принято другим за действия соучастников либо за угрозу раскрытия. Несогласованное вмешательство способно изменить поведение лица и лишить ранее полученные ориентиры практической пригодности. Проблема, следовательно, связана не с самим совпадением оперативного интереса, закономерным для распределённой деятельности, а со временем его обнаружения.

Ранняя сверка совпадающих объектов может рассматриваться как средство организационного согласования, если её результат не подменяет основания для мероприятия. Минимальный набор идентификаторов способен включать сведения о лице, учётной записи, транспортном средстве, адресе и устойчивом способе действий без раскрытия содержания разработки всем пользователям. При выявлении совпадения достаточно уведомить уполномоченных руководителей, после чего определяются ответственное подразделение, пределы обмена и порядок дальнейших действий.

В.Ф. Луговик и А.Л. Осипенко связывают развитие информационных средств с необходимостью правового определения доступа и ответственности за использование полученных сведений[2]. Это ограничение особенно существенно для незавершённых оперативных материалов.

---

[1] Сущность результатов оперативно-розыскной деятельности и их использование в уголовном судопроизводстве: учебное пособие / К.И. Масленников, Г.В. Бушин, А.В. Сидоренко, Н.А. Нигметов. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2024. 64 с.

[2] Луговик В.Ф., Осипенко А.Л. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. 2015. № 4. С. 7-12.

Система сверки, не ограниченная целью и составом данных, сама создаёт правовые риски. Накопление сведений обо всех объектах оперативного интереса повышает вероятность избыточного хранения, несанкционированного доступа и использования информации вне первоначальной цели. Соразмерность такого механизма может обеспечиваться разграничением полномочий, регистрацией обращений, сроками хранения и удалением неподтверждённых совпадений. Результат сверки имеет организационное, а не доказательственное назначение. Он сообщает о вероятном совпадении и позволяет согласовать действия, но не устанавливает причастность лица и не устраняет требования к основаниям конкретного мероприятия.

Уголовно-правовая оценка бесконтактного сбыта зависит от фактически совершённых действий, а не от технической формы взаимодействия. Обнаружение расфасованного вещества, координат или переписки само по себе не отвечает на вопрос о приготовлении, покушении либо оконченном сбыте. Для разграничения имеют значение направленность умысла, наличие приобретателя, содержание действий по передаче и причины, по которым наркотическое средство не поступило другому лицу. Оперативное вмешательство способно остановить дальнейшее развитие эпизода, однако момент изъятия не предопределяет юридическую квалификацию. Она требует восстановления той стадии передачи, которая была достигнута к этому моменту.

Пункт 13.1 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 связывает оконченный сбыт с выполнением всех необходимых действий по передаче наркотического средства независимо от его фактического получения приобретателем. Согласно пункту 13.2 покушение имеет место, когда направленные на реализацию действия не завершились передачей по обстоятельствам, не зависящим от лица[1]. Применительно к тайнику оконченный сбыт возможен, если свёрток размещён и конкретному приобретателю сообщены достаточные сведения для его получения. Перевозка партии или оборудование тайника до завершения действий по передаче при соответствующем умысле могут получить иную оценку. Следовательно, факт изъятия сотрудниками учитывается наряду с содержанием предшествовавших действий, а не используется как единственный критерий.

Использование информационно-телекоммуникационной сети характеризует способ сбыта при установленной связи сети с действиями по незаконной передаче. В изученных материалах посредством сетевых ресурсов размещались предложения, принимались заказы, передавались инструкции и сведения о тайниках. Однако обнаружение соответствующего приложения на телефоне либо посещение ресурса не раскрывает назначения конкретной коммуникации. Обоснование квалифицирующего признака требует установить пользователя учётной записи, содержание сообщений и их отношение к определённой

[1] Пункты 13.1 и 13.2 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» [Электронный ресурс]. URL: https://www.vsrf.ru/files/14948/ (дата обращения: 27.07.2026).

операции. Сопоставление с платежом, маршрутом, тайником и изъятым веществом позволяет отличить участие в механизме сбыта от иного использования цифрового сервиса.

Наименования ролей в переписке также не образуют достаточной основы для вывода об организованной группе. Проверке подлежат устойчивость объединения, предварительная согласованность действий, распределение функций и общая направленность деятельности. Псевдонимы и отсутствие личного знакомства между исполнителями совместимы с организованностью, но не доказывают её сами по себе. При оценке изученных материалов учитывались продолжительность работы магазина, повторяемость функций, правила отчётности, система оплаты, общие помещения и связь партий с руководящими учётными записями. Оперативные сведения помогали обнаружить соответствующие связи, тогда как их процессуальная проверка проводилась отдельно в отношении каждого обвиняемого.

Вид и масса изъятого вещества имеют самостоятельную доказательственную основу. Наблюдение может способствовать обнаружению партии до её разделения, объяснять место изъятия и действия лиц, однако не заменяет экспертного заключения. Крупный и особо крупный размеры устанавливаются применительно к конкретному виду наркотического средства и предусмотренным пороговым значениям. При обнаружении нескольких веществ общая характеристика масштаба деятельности группы не восполняет определение каждого объекта. Разграничение функций источников здесь особенно наглядно. Наблюдение раскрывает обстоятельства обнаружения, а экспертное заключение - свойства и массу вещества, необходимые для уголовно-правовой оценки.

Возможность использовать результаты оперативно-розыскного мероприятия в доказывании связана с законностью их получения и соблюдением порядка передачи следователю. Верховный Суд Российской Федерации исходит из наличия предусмотренных законом задач, оснований и условий мероприятия, а также из самостоятельного формирования умысла лица вне побуждающего воздействия сотрудников[1]. Хотя эти положения сформулированы применительно к соответствующей судебной практике, их значение не ограничивается проверочной закупкой. Последующее приобщение документа не устраняет нарушение, допущенное при первоначальном получении сведений. Эффективность наблюдения поэтому соотносится не только с объёмом полученной информации, но и с возможностью проверить её источник и использовать результат в допустимой процессуальной форме.

Материалы Интерпола раскрывают международный аспект работы с теневыми сетевыми площадками и цифровыми валютами. Созданная организацией рабочая группа служит площадкой для обмена методами

[1] Пункт 14 постановления Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» [Электронный ресурс]. URL: https://www.vsrf.ru/files/14948/ (дата обращения: 27.07.2026).

расследования, сведениями об используемых сервисах и подходами к прослеживанию операций[1]. Такой обмен обусловлен тем, что сетевой ресурс, сервер, платёжная инфраструктура, продавец и место доставки могут относиться к разным юрисдикциям. Его результативность, однако, нельзя оценивать только количеством переданных данных. Прикладное значение возникает, когда сведения помогают индивидуализировать участника, обнаружить наркотическое средство или ограничить используемую инфраструктуру и могут быть проверены по правилам государства, в котором предполагается их применение.

Всемирный доклад Управления ООН по наркотикам и преступности рассматривает теневой сегмент сети как один из каналов предложения наркотиков и отмечает данные, возникающие при оплате и доставке[2]. Эти стадии способны связать сетевое предложение с движением имущества и физическим маршрутом. Доклад описывает тенденции рынка, но не устанавливает процессуальный алгоритм для национальных органов. Порядок получения финансовых сведений, проведения наблюдения и использования электронных данных определяется внутренним правом. Поэтому сравнительное значение материала состоит в выделении общего объекта внимания - перехода от сетевого взаимодействия к передаче предмета, а не в заимствовании конкретной процедуры.

Закон Республики Казахстан предусматривает систему оперативно-розыскных мероприятий и правила использования полученной информации[3]. Верховный Суд Республики Казахстан связывает допустимость оперативного закупа и иных мероприятий с наличием законных оснований, контролем уполномоченного органа и отсутствием склонения лица к правонарушению[4]. Сопоставление с российским регулированием обнаруживает сходство не технических решений, а правовых ограничений вмешательства. Цифровой способ выявления не отменяет требований законности и проверяемости результата. По этой причине казахстанский материал уместен для анализа связи оперативной информации, физического изъятия и последующей судебной оценки, но не даёт основания механически переносить организационные процедуры в российскую практику.

Приведённые международные материалы относятся к разным уровням регулирования. Интерпол обеспечивает координацию и обмен сведениями,

---

[1] INTERPOL holds first DarkNet and Cryptocurrencies Working Group. INTERPOL, 2018 [Electronic resource]. URL: https://www.interpol.int/News-and-Events/News/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group (accessed: 27.07.2026).

[2] United Nations Office on Drugs and Crime. World Drug Report 2020. Booklet 4. Cross-cutting issues: evolving trends and new challenges. Vienna, 2020 [Electronic resource]. URL: https://wdr.unodc.org/wdr2020/en/cross-cutting.html (accessed: 27.07.2026).

[3] Об оперативно-розыскной деятельности: Закон Республики Казахстан от 15 сентября 1994 г. № 154-XIII [Электронный ресурс]. URL: https://www.adilet.zan.kz/rus/docs/Z940004000_ (дата обращения: 27.07.2026).

[4] Пункт 9.4 нормативного постановления Верховного Суда Республики Казахстан от 14 мая 1998 г. № 3 «О применении законодательства по делам, связанным с незаконным оборотом наркотических средств, психотропных веществ, их аналогов и прекурсоров» [Электронный ресурс]. URL: https://www.adilet.zan.kz/rus/docs/P98000003S_ (дата обращения: 27.07.2026).

Управление ООН по наркотикам и преступности описывает рынки и риски, национальные органы действуют в рамках собственных правовых процедур. Их сопоставление не образует единой модели противодействия. Общим является более ограниченное положение. Сетевой ресурс, операция с цифровым активом и зашифрованная переписка не исчерпывают фактический механизм передачи наркотического средства. Одновременно цифровые данные не сводятся к предварительному ориентиру, если они после проверки раскрывают структуру группы, финансовую связь или содержание конкретного заказа.

Результаты изучения практики позволяют точнее определить место наблюдения без его противопоставления цифровым средствам. Наиболее результативным наблюдение оказалось при установлении физической активности участников, автомобилей и помещений. Информационно-поисковые системы увеличивали продолжительность и точность контроля, не изменяя правовой природы мероприятия. Сетевые сведения связывали наблюдаемые действия с магазином, заказами и тайниками. Такой результат относится к конкретной совокупности обстоятельств и не означает универсального приоритета наблюдения во всех ситуациях. Существенной оказалась последовательность переходов между источниками, каждый из которых проверял отдельную часть общей версии.

Материально-предметное звено сохраняет значение при высокой технической защищённости коммуникации, поскольку наркотическое средство должно быть получено либо изготовлено, расфасовано, перемещено и передано. Тайник составляет лишь один элемент этой последовательности. К ней относятся также помещения хранения, упаковка, транспорт и действия с оптовой партией. Учёт названных стадий расширяет объект наблюдения за пределы исполнителя, помещающего свёрток. В зависимости от исходных данных проверка может быть направлена на снабжение, место фасовки либо связь с управляющей учётной записью. Тем самым физические операции рассматриваются не отдельно от сетевого заказа, а как условия его реализации.

Параллельная разработка одного объекта показывает организационный предел даже технически оснащённого наблюдения. Подразделения, не располагающие сведениями о совпадении, способны взаимно затруднять работу и создавать риск преждевременного обнаружения. Ранняя сверка уменьшает этот риск лишь при соблюдении нескольких ограничений. Она должна использовать необходимый минимум идентификаторов, исключать необоснованный доступ и сохранять самостоятельность оснований каждого мероприятия. При таких условиях согласование выступает средством сохранения получаемого результата. Без указанных гарантий информационная система может создать новые риски, не устранив первоначальную проблему.

Доказательственное использование материалов предполагает разграничение оперативного результата и процессуально установленного обстоятельства. Фотографии, координаты, переписка, сведения об операциях и наблюдаемые действия оцениваются после проверки их происхождения, содержания и связи с конкретным лицом. Вид и масса вещества устанавливаются экспертным заключением. Признаки организованной группы выводятся из совокупности

данных о согласованности и устойчивости. Стадия сбыта определяется по действиям, направленным на передачу приобретателю. Такое распределение познавательных функций не ослабляет значение оперативных материалов, а устанавливает предел, за которым ориентирующий вывод нуждается в самостоятельном процессуальном подтверждении.

Цифровая организация бесконтактного сбыта изменяет расположение сведений о преступной деятельности, не устраняя операций с наркотическим средством. Исходным объектом проверки может стать платёж, маршрут автомобиля либо координаты тайника. Ни один из этих источников не обладает достаточностью вне связи с последующими данными. При выявлении бесконтактного сбыта определяющей является возможность восстановить проверяемую последовательность от первоначального сообщения до обнаружения предмета и процессуального решения. Эта последовательность соотносит сетевую коммуникацию с действиями конкретных участников и одновременно ограничивает выводы теми обстоятельствами, которые действительно подтверждены.

Список источников:

1. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск, Омская академия МВД России, 2009. 480 с.
2. Миненко П.В., Пучнин А.В. Массивы компьютерной информации как объект оперативно-розыскных мероприятий // Общество и право. 2020. № 4 (74). С. 87-91.
3. Усачева Е.А. Влияние информационно-телекоммуникационных технологий на незаконный оборот наркотических средств и психотропных веществ: криминалистический анализ // Вестник Восточно-Сибирского института МВД России. 2023. № 3 (106). С. 244-253. DOI 10.55001/2312-3184.2023.38.78.021.
4. Шакирьянов М.М. Особенности проведения оперативно-розыскных мероприятий по выявлению и раскрытию бесконтактного сбыта наркотических средств // Вестник Самарского юридического института. 2019. № 2 (33). С. 92-96.
5. Макеева Н.В. Документирование результатов оперативно-разыскной деятельности и их использование как повод и основание для возбуждения уголовного дела о незаконном сбыте наркотических средств бесконтактным способом с использованием информационно-телекоммуникационных сетей // Вестник Московского университета МВД России. 2019. № 5. С. 36-39. DOI 10.24411/2073-0454-2019-10249.
6. Луговик В.Ф., Осипенко А.Л. Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. 2015. № 4. С. 7-12.
7. Чечётин А.Е. Условия проведения оперативно-розыскных мероприятий. Учебное пособие. Барнаул, Барнаульский юридический институт МВД России, 2023. 48 с.

8. Сущность результатов оперативно-розыскной деятельности и их использование в уголовном судопроизводстве. Учебное пособие / К.И. Масленников, Г.В. Бушин, А.В. Сидоренко, Н.А. Нигметов. Санкт-Петербург, Санкт-Петербургский университет МВД России, 2024. 64 с.
9. Об оперативно-розыскной деятельности. Федеральный закон от 12 августа 1995 г. № 144-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 27.07.2026).
10. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 27.07.2026).
11. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами. Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 г. № 14 с последующими изменениями [Электронный ресурс]. URL: https://www.vsrf.ru/files/12355/ (дата обращения: 27.07.2026).
12. Совет Безопасности Российской Федерации. Секретарь Совета Безопасности Российской Федерации Сергей Шойгу в интервью агентству ТАСС. 25 апреля 2025 г. [Электронный ресурс]. URL: https://www.scrf.gov.ru/news/speeches/3804/ (дата обращения: 27.07.2026).
13. INTERPOL holds first DarkNet and Cryptocurrencies Working Group. INTERPOL, 2018 [Electronic resource]. URL: https://www.interpol.int/News-and-Events/News/2018/INTERPOL-holds-first-DarkNet-and-Cryptocurrencies-Working-Group (accessed: 27.07.2026).
14. United Nations Office on Drugs and Crime. World Drug Report 2020. Booklet 4. Cross-cutting issues. Evolving trends and new challenges. Vienna, 2020 [Electronic resource]. URL: https://wdr.unodc.org/wdr2020/en/cross-cutting.html (accessed: 27.07.2026).
15. Об оперативно-розыскной деятельности. Закон Республики Казахстан от 15 сентября 1994 г. № 154-XIII [Электронный ресурс]. URL: https://www.adilet.zan.kz/rus/docs/Z940004000_ (дата обращения: 27.07.2026).
16. О применении законодательства по делам, связанным с незаконным оборотом наркотических средств, психотропных веществ, их аналогов и прекурсоров. Нормативное постановление Верховного Суда Республики Казахстан от 14 мая 1998 г. № 3 [Электронный ресурс]. URL: https://www.adilet.zan.kz/rus/docs/P98000003S_ (дата обращения: 27.07.2026).

С.Б. Вепрев[1]
С.А. Нестерович[2]

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ СРЕДСТВ

Аннотация. В последние годы наблюдается устойчивая тенденция к увеличению кибератак на программные средства автоматизированных систем. Основываются они, как правило, на выявлении уязвимостей в операционных системах и программных продуктах. Количество кибератак не только увеличилось, но они становятся все более опасными с точки зрения корректного функционирования вычислительных систем и обеспечения их информационной безопасности. Все более актуальной становится задача совершенствования и улучшения мер безопасности программных средств.

Ключевые слова: информационная безопасность, автоматизированная система, программные средства,

Анализ современных проблемам информационной безопасности программных средств показывает, что кибератаки становятся все более изощренными и скрытными. Зачастую их сложно, если не невозможно, оперативно выявить и обезвредить. Создаются такие вредоносные программы, против которых пока еще отсутствуют защитные механизмы. Они направлены на «обход» аутентификации и осуществление удаленного доступа к ресурсам информационной системы. В более трети успешных атак на программные средства были использованы уязвимости программного обеспечения операционных систем. Важно заметить, что в ряде случаев использовалась инсайдерская информация. Использование сведений от инсайдеров сложно выявить и их анализ не поддается четкому количественному отображению. Злоумышленнику гораздо легче осуществить проникновение в систему при наличии знания об использовании конкретных ОС и программных продуктов, использовании и в ней тех или иных средств защиты. Следует отметить, что «традиционные» причины возникновения угроз безопасности до сих пор остаются все теми же. Согласно данным портала информационной безопасности Content Security степень опасности возникновения внутренних и внешних угроз такова:

- разглашение (излишняя болтливость сотрудников) — 32%;
- несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок — 24%;
- отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности — 14%;
- традиционный обмен производственным опытом — 12%;
- бесконтрольное использование информационных систем — 10%;

[1] Вепрев Сергей Борисович – профессор Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, доктор технических наук, профессор.

[2] Нестерович Сергей Александрович – доцент кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества Российского государственного социального университета, кандидат технических наук, доцент.

- наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива — 8%.

Статистические данные показывают, что в последние годы наблюдается устойчивый рост кибератак на информационные системы на основе выявления новых уязвимостей в их системном программном обеспечении. Следует отметить процесс интенсивного постоянного совершенствования программных средств и внедрение новых подходов обработки данных. Очевидно, что при создании новых перспективных информационных систем очень сложно учесть все их возможные уязвимости, что и способствует появления новых угроз информационной безопасности. Данные только лишь по количеству новых зарегистрированных уязвимостей в программном обеспечении ОС и ППП согласно CVE (база данных общественных уязвимостей информационной безопасности) за последние пять лет показали их рост на 67%.

Следует отметить, что выявленные уязвимости представляют разный уровень угрозы информационной безопасности, среди которых следует выделить критические уязвимости, которые либо нарушают функционирование информационной системы в целом, либо осуществляют контроль за ее функционированием. При этом следует отметить, что результаты внутреннего тестирования на выявление угроз не могут считаться полностью достоверными. Приблизительно четыре процента всех уязвимостей являются критическими. При этом, наблюдается их устойчивый рост в процентном отношении.

Особое внимание привлекли уязвимости в продуктах IvantiConnectSecure (решение для доступа сотрудников, партнеров и клиентов к корпоративным данным и приложениям) и IvantiPolicySecure (решение для контроля сетевого доступа). Эти уязвимости включают CVE-2023-46805 (высокий уровень опасности) и CVE-2024-21887 (критический уровень опасности). Первая уязвимость позволяет обходить протокол аутентификации, а вторая – выполнять произвольные команды с удаленного доступа.

К ключевым уязвимостям относятся:

Уязвимости нулевого дня – коды, против которых пока еще отсутствуют защитные механизмы. Злоумышленник получает возможность непосредственного воздействия на ОС или программное средство. Уязвимости нулевого дня выявлены и в таких ОС, как Windows и Linux и macOS. Отмечается их рост и в прикладных программных средствах - веб-браузерах, офисных приложениях, системах управления базами данных.

Уязвимости управления данными. Они, как правило, основываются на переполнении буфера памяти. В результате были осуществлены действия по выполнению вредоносной программы, которая запускалась при попытке очистить буфер памяти.

Уязвимости в механизмах аутентификации. Данные уязвимости очень опасны, так как позволяют злоумышленнику бесконтрольно осуществлять соответствующие противоправные действия и дают возможность осуществлять

несанкционированный доступ к информационным ресурсам и программным средствам.

Обеспечение информационной безопасности программных продуктов подразумевает использование комплексного подхода, включающего использование современных методов машинного обучения, инструментальных средств и виртуальных контейнеров, таких, как Coverity или Checkmarx, проведения тестов на проникновение вредоносных программных продуктов (платформы HackerOne и Bugcrowd). Использование методологии безопасной разработки программных средств в режиме реального времени (DevSecOps) позволит обеспечить их большую защищенность.

Отметим необходимость разработки соответствующих отечественных средств противодействия уязвимостям, ибо, как показывает практика, использование чужого инструментария определяет зависимость и невозможность его объективного контроля. В современных условиях этот факт становится еще одной угрозой информационной безопасности программных средств. В данных обстоятельствах, следует отметить разработку и развитие отечественных средств обеспечения кибербезопасности. Так, по данным Центра стратегических разработок в России в области NGFW (защита от сетевых угроз) объем рынка составил 52,2 млрд рублей и его рост составил боле 30 процентов, что выше мировых показателей. В этом аспекте отмечаются ведущие российские компании: Лаборатория Касперского, Код безопасности, Инфросистемы ДЖЕТ, ГК Солар, User Gate, Positive Tecnologies и др. РОСТЕЛЕКОМ разработал Кибериндекс - инструментарий для оценки безопасности данных, в котором реализован опыт зарубежных аналогов, включая стандарт ISO 27001/27002 (международный стандарт требований к системам менеджмента информационной безопасности).

Полный переход на использование качественных отечественных средств обеспечения информационной безопасности в стратегически важных программных продуктах позволит значительно повысить уровень кибербезопасности российских информационных систем.

Н.В. Золотухина[1]
А.А. Долусов[2]

ПРОЦЕССУАЛЬНЫЙ ПОРЯДОК ПРИМЕНЕНИЯ ПРИСМОТРА ЗА НЕСОВЕРШЕННОЛЕТНИМИ

Аннотация. Авторы рассматривают уголовно-процессуальные и организационные особенности избрания меры пресечения в виде присмотра за несовершеннолетним

[1] Золотухина Наталья Валерьевна – доцент кафедры управления и психологии следственной деятельности (Высшие академические курсы) факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева.

[2] Долусов Арсений Андреевич – следователь Демидовского Межрайонного Следственного отдела Следственного Управления Следственного комитета Российской Федерации по Смоленской области, лейтенант юстиции.

подозреваемым (обвиняемым). Приводят примеры практики применения и особенностей определения цели и задач данной меры пресечения, выделяющей её из ряда других мер, предусмотренных уголовно-процессуальным законодательством. Дают рекомендации по его процессуальному оформлению.

Ключевые слова: меры пресечения; присмотр за несовершеннолетним; расследование преступлений; следователь; подозреваемый; обвиняемый; законный представитель; уголовное дело.

Меры пресечения относятся к самым существенным видам уголовно-процессуального принуждения, для избрания которых в уголовно-процессуальном законодательстве предусмотрены соответствующие основания и условия. Аргументированное, правильное решение об использовании меры пресечения, принятое в соответствии с законом, способствует более оперативному расследованию правонарушений в полном объеме, предотвращает совершение ряда незаконных действий, гарантирует назначение наказания за преступления, а также помогает в соблюдении прав и законных интересов обвиняемых.

Недостатком действующего законодательства следует назвать то обстоятельство, что цели применения мер пресечения не обозначены в УПК РФ. Среди исследователей не утихают активные дискуссии относительно определения целей присмотра за несовершеннолетними обвиняемыми и подозреваемыми, несмотря на их законодательное закрепление в нормах УПК РФ, что, по нашему мнению, обуславливается многоаспектным характером присмотра как меры пресечения. В данном вопросе у них нет консенсуса, высказываются самые разнообразные точки зрения, характеризующиеся своей неоднозначностью и противоречивостью.

А.В. Шишов полагает, что цели присмотра носят комплексный характер и очерчиваются не только недопущением уклонения обвиняемого от явки по вызовам, но и предупреждением продолжения несовершеннолетним обвиняемым или подозреваемым противоправной деятельности, возможности оказания какого-либо давления на следствие, потерпевших, укрытие следов преступления[1].

Анализ судебной практики позволил прийти к однозначному выводу о существовании негативной тенденции, связанной с тем, что многие суды по-прежнему исходят из превалирования тяжести совершенного преступления при избрании меры пресечения несмотря на то, что присмотр может избираться по всем категориям преступлений, но в зависимости от обстоятельств совершенного преступления и личности несовершеннолетнего преступника. В данном отношений уголовно-процессуальный закон никаких ограничений и изъятий не предусматривает.

Следует также констатировать, что суды в недостаточной степени в приговорах обосновывают применение данной меры пресечения, ограничиваясь

[1] См.: Шишов А.В. Понятие, цели, основные свойства залога как меры пресечения в уголовном судопроизводстве // Закон и право. 2019. № 3. С. 80-82.

только общими формулировками закона, чем нивелируется значение целей и задач присмотра как самостоятельной меры пресечения.

Присмотр, будучи признан самостоятельной мерой пресечения, в первую очередь преследует обеспечение надлежащего поведения несовершеннолетнего обвиняемого или подозреваемого, его непосредственного участия в необходимых следственных и иных процессуальных действиях, которые потребуются для расследования уголовного дела. В тоже время такой цели присмотра непосредственно в ст. 105 УПК РФ не предусматривается. Несмотря на это, присмотр является более удобной мерой пресечения по сравнению с заключением под стражей.

Ряд авторов в качестве самостоятельной цели присмотра отмечают предупреждение сокрытия преступника от уголовного преследования[1]. Как показывает исследование, несовершеннолетние обвиняемые (подозреваемые), в отношении которых избирается присмотр, весьма редко уклоняются от органов следствия и суда и скрываются впоследствии. Это во многом обусловлено несколькими обстоятельствами:

– возможностью отмены присмотра на более строгую меру пресечения, в частности, заключение под стражу;

– осуществление присмотра за несовершеннолетними родителями, опекунами, попечителями или другими заслуживающими доверия лицами, а также должностными лицами специализированного детского учреждения;

– наличие в ч. 3 ст. 105 УПК РФ возможности применения мер взыскания к лицам, которым несовершеннолетний подозреваемый, обвиняемый был отдан под присмотр, в случае невыполнения ими принятого обязательства, в порядке, предусмотренном ст. 103 УПК РФ.

Ввиду изложенного, следует говорить, что в данной мере уголовного пресечения в большей степени заинтересованы сами несовершеннолетние обвиняемые (подозреваемые), которые не лишаются физической свободы и их изоляция от общества не носит абсолютного характера. В тоже время полагаем, что государство также должно быть заинтересовано в избрании этой меры пресечения по следующим причинам:

– сокращаются расходы на содержание несовершеннолетних обвиняемых (подозреваемых) в изоляторах;

– стимулируется поведенческая установка несовершеннолетнего обвиняемого (подозреваемого) на правомерное поведение;

– исключается возможность влияния криминальных элементов на личность несовершеннолетнего обвиняемого (подозреваемого), формирование негативных привычек, свойственных в местах отбывания наказания, происходит предупреждение рецидивной преступности.

Условиями избрания меры пресечения в виде присмотра за несовершеннолетним подозреваемыми (обвиняемыми) являются:

1) наличие возбужденного уголовного дела;

[1] См.: Жунусов К.М. Цели применения меры пресечения «залог» в российском уголовном процессе // Достижения науки и образования. 2018. № 7. С. 56-58.

2) мера пресечения не может быть избрана при отсутствии фактических оснований ее избрания;

3) мера пресечения применяется к несовершеннолетнему подозреваемому (обвиняемому).

По нашему мнению, достаточность оснований для избрания присмотра как меры пресечения предполагает наличие полного и достаточного объема достоверных фактических сведений, свидетельствующих о факте неправомерного поведения несовершеннолетнего обвиняемого (подозреваемого), т.е. наличие совокупности доказательств, установленных по уголовному делу. Избрание конкретной меры пресечения в отношении подозреваемого, обвиняемого должно основываться на достаточности собранных по делу доказательствах. Поэтому правы те авторы, которые убеждены, что если у органов следствия отсутствуют доказательства, свидетельствующие о причастности подозреваемого к совершению преступления, то отсутствуют и основания, позволяющие избирать в отношении него меру пресечения[1]. В тоже время в данном вопросе необходимо соблюдать определенные баланс. Так, медлить с избранием меры пресечения также не следует, если для этого имеются необходимые основания.

Анализ судебной практики, в частности обзоров Верховного Суда РФ, позволяет сделать вывод о том, что присмотр за несовершеннолетним, в отличие от других мер пресечения, чаще применяется по делам о преступлениях небольшой и средней тяжести (в соответствии с классификацией, установленной ст. 15 Уголовного кодекса РФ). Это обусловлено как особенностями личности несовершеннолетних правонарушителей, так и презумпцией применения к ним более мягких мер воздействия, что соответствует принципам, закрепленным в ст.ст. 87-96 УК РФ.

При решении вопроса об избрании меры пресечения в отношении несовершеннолетнего подозреваемого (обвиняемого) дознаватель, следователь, суд должен изначально рассмотреть вопрос о возможности отдачи несовершеннолетнего под присмотр родителей или иных заслуживающих доверия лиц, для чего необходимо получить согласие родителей, опекунов, попечителей или других заслуживающих доверия лиц, а также должностных лиц специализированного детского учреждения, в котором он находится. Данное согласие согласно ч. 2 ст. 105 УК РФ оформляется в письменной форме.

В обязательстве обычно не пишется, что несовершеннолетний подозреваемый (обвиняемый) не будет совершать в ходе уголовного судопроизводства преступлений и не станет препятствовать исполнению приговора, но обеспечение такого поведения несовершеннолетнего подозреваемого (обвиняемого) предполагается.

Заслуживает критических замечаний позиция законодателя, который в ст. 105 УК РФ не стал конкретизировать положение, что присмотр допускается не только вследствие письменного волеизъявления лиц, обеспечивающих

[1] См.: Кондрат И.Н. Обеспечение прав личности в досудебном производстве по уголовным делам: законодательное регулирование и правоприменительная практика. М., 2015. С. 132.

примерное поведение несовершеннолетнего, но и требует обязательного согласия самого несовершеннолетнего подозреваемого или обвиняемого. Данный процесс носят обоюдный характер, где необходимо согласие всех сторон. Этот момент еще важен с точки зрения выяснения обстоятельств о личности обвиняемого при принятии решения об избрании присмотра, о чем умалчивается в ст. 105 УК РФ.

Согласимся, что если несовершеннолетний подозреваемый или обвиняемый характеризуется отрицательно, ведет антисоциальный образ жизни, злоупотребляет алкогольными напитками, нигде не работает, имеются факты применения насилия, то даже поручительство со стороны родителей и иных лиц об обеспечении надлежащего присмотра за несовершеннолетним не может являться достаточным основанием для избрания данной меры пресечения.

Следует обратить внимание дознавателя, следователя, суд, что нельзя допускать возможность отдачи несовершеннолетнего под присмотр родителя, лишенных родительских прав. Не исключены случаи совместного проживания указанных лиц, которые по «привычке» являются по вызову дознавателя, следователя и суда для реализации прав законных представителей.

Из содержания ст. 105 УПК РФ можно прийти к выводу, что законодатель допускает избрание присмотра в случае совершения несовершеннолетним подозреваемым или обвиняемым преступления любой тяжести. Вместе с тем, необходимо, чтобы в судебных решениях отражались результаты исследования личности обвиняемого (подозреваемого). Это должно повысить прозрачность и понятность процедуры назначения присмотра.

В тоже время считаем, что избрание присмотра в отношении несовершеннолетних, совершивших преступления небольшой или средней тяжести, должно носить распространённый характер ввиду отсутствия, как правило, существенной общественной опасности совершенных преступлений, а также некриминальности личности виновного. В тоже время представляется, что в случае совершения тяжкого или особо тяжкого преступления избрание присмотра является не всегда целесообразным, но допустимым при наличии к тому достаточных оснований. В тоже время не все исследователи согласны с такой трактовкой, полагая, что избрание меры пресечения в отношении лиц, совершивших тяжкие или особо тяжкие преступления, является просто недопустимым[1].

Позволим опровергнуть такую позицию, поскольку она не учитывает сущность и предназначение присмотра, заключающееся в обеспечении надлежащего поведения несовершеннолетнего подозреваемого или обвиняемого лица. Поэтому закреплять в УПК РФ подобного рода ограничения в отношении лиц, вина которых еще не доказана, нецелесообразно, за определенными исключениями, касающихся, например, закрепления в УПК РФ положения, что обязательным условием избрания присмотра при совершении тяжких или особо тяжких преступлений является установление дополнительных запретов.

[1] См.: Тетюев С.В. Избрание мер пресечения в отношении несовершеннолетних // Судья. 2015. № 7. С. 20-23.

В качестве другого предложения выскажем идею о закреплении исчерпывающего перечня категорий дел, по которым не допускается избрание присмотра при совершении тяжких или особо тяжких преступлений, например, при совершении убийства при отягчающих обстоятельствах, иных насильственных преступлений, преступлений экстремистской и террористической направленности.

Разрешая вопрос о необходимости применить к несовершеннолетнему подозреваемому (обвиняемому) меру пресечения в виде присмотра, а также об избрании той или иной из них, следователь учитывает, помимо характера и содержания фактических оснований избрания меры пресечения: тяжесть совершенного преступления и, соответственно, предъявленного обвинения; личность подозреваемого (обвиняемого); возраст; семейное положение (женат или нет, наличие на иждивении детей); характер и род занятий (деятельности); состояние здоровья; данные о трудоспособности; наличие места учебы, работы и жительства по месту производства предварительного расследования (судебного разбирательства); наличие государственных, иных наград и т.п.; наличие (отсутствие) судимости, срок отбывания наказания в местах лишения свободы, сколько времени после освобождения находится на свободе; факты, характеризующие его как члена общества (по месту жительства, учебы, работы, увлечениям и т.п.); события его биографии (к примеру, спас тонущего ребенка, участвовал в предотвращении последствий пожара и т.п.) и др.

При применении данной меры пресечения допускается установление обязанностей и ограничений, предусмотренных ст. 102 УПК РФ:

1) не покидать место жительства или место пребывания без разрешения дознавателя, следователя или суда;
2) в назначенный срок являться по вызовам дознавателя, следователя и в суд;
3) иным путем не препятствовать производству по уголовному делу.

Таким образом, законодатель допустил распространение в отношении присмотра правовых норм, регламентирующих другую меру пресечения – подписку о невыезде и надлежащем поведении. Перечень таких обязанностей и запретов, по-нашему мнению, более правильным было бы сделать открытым, допустив возможность следователю, дознавателю, суду самостоятельно определять иные запреты, которые будут наиболее эффективно способствовать исполнению данной меры пресечения в конкретной ситуации.

Контроль за соблюдением несовершеннолетним исполнения меры пресечения в виде присмотра возлагается на соответствующих лиц, изъявивших желание. Они являются ответственными за воспитание несовершеннолетних, соблюдение ими законопослушного поведения и возложенных на них мер ограничений и запретов.

Д.И. Ережипалиев обосновывает необходимость дополнения УПК РФ нормой, предусматривающей обязанность следователей и дознавателей оповещать специализированные органы и учреждения системы профилактики безнадзорности и правонарушений детей и подростков в случае избрания в

отношении несовершеннолетнего меры пресечения и возлагать на них обязанность по контролю за исполнением данной меры пресечения[1].

При определенных обстоятельствах уголовно-процессуальное законодательство допускает замену присмотра на иную меру пресечения. Непосредственно в ст. 105 УПК РФ не закреплено специальных положений замены присмотра, в связи с чем, вопросы изменения присмотра на иную меру пресечения регламентируются положениями ст. 110 УПК РФ.

Для изменения присмотра на более строгую меру пресечения необходимые соответствующие обстоятельства. К таковым можно отнести следующие:

– возможность совершения несовершеннолетним обвиняемым (подозреваемым) процессуального нарушения;

– неспособность присмотра обеспечить надлежащее поведение несовершеннолетнего обвиняемого или подозреваемого;

– нарушение условий предусмотренных ограничений.

В тоже время в ст. 105 УПК РФ такие обстоятельства не прописаны, что существенным образом затруднят инициирование процедуры изменения присмотра.

Подводя итоги отметим, что действующее законодательство и судебная практика в сфере применения присмотра как меры пресечения не лишено определенных правовых пробелов и противоречий, требующих своего разрешения. Полагаем, что рассмотренные вопросы способны преодолеть имеющиеся сложности и противоречия и способствовать оптимизации правоотношений в данной сфере, повысить эффективность защиты прав несовершеннолетних обвиняемых и подозреваемых, а также сделать практику применения присмотра более распространенной.

Список источников

1. Ережипалиев Д.И. Особенности прокурорского надзора за исполнением законов при избрании и применении мер пресечения в отношении несовершеннолетних // Законы России: опыт, анализ, практика. 2014. № 5. С. 65-70.
2. Жунусов К.М. Цели применения меры пресечения «залог» в российском уголовном процессе // Достижения науки и образования. 2018. № 7. С. 56-58.
3. Захарова В.О. О качестве расследования преступлений // Пробелы в российском законодательства. 2023. № 7. С. 131-135.
4. Кондрат И.Н. Обеспечение прав личности в досудебном производстве по уголовным делам: законодательное регулирование и правоприменительная практика. М., 2015. С. 132.

[1] См.: Ережипалиев Д.И. Особенности прокурорского надзора за исполнением законов при избрании и применении мер пресечения в отношении несовершеннолетних // Законы России: опыт, анализ, практика. 2014. № 5. С. 65-70.

5. Коновалова М.А. Охрана прав участников уголовного судопроизводства при применении мер пресечения // в сб. Актуальные проблемы уголовного судопроизводства: материалы III Всероссийской научно-практической конференции (Новосибирск, 18 мая 2023 года). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 72-76
6. Тетюев С.В. Избрание мер пресечения в отношении несовершеннолетних // Судья. 2015. № 7. С. 20-23.
7. Шишов А.В. Понятие, цели, основные свойства залога как меры пресечения в уголовном судопроизводстве // Закон и право. 2019. № 3. С. 80-82.

О.В. Зуева[1]

ДОВЕРИЕ МОЛОДЕЖИ К ИНСТИТУТАМ ПРАВОПОРЯДКА КАК ЭЛЕМЕНТ СИСТЕМЫ ЗАЩИТЫ ОТ ПРОЯВЛЕНИЙ КИРЕБЕРЭКСТРЕМИЗМА И ТЕРРОРИЗМА

Аннотация. В статье рассматривается доверие молодежи к институтам правопорядка как ресурс профилактики киберэкстремизма и терроризма. Отмечается, что в условиях высокой цифровой включенности молодежи, противодействия через мониторинг и силовое реагирование недостаточно. Важна легитимность правоохранительных институтов и готовность молодых людей обращаться за помощью. По данным ВЦИОМ, Левада-Центра, НИУ ВШЭ и МВД России, молодежь – одновременно самая цифровизированная группа и ключевая аудитория профилактики онлайн-угроз. Делается вывод о необходимости развития справедливых, прозрачных и ориентированных на молодежь форм взаимодействия между институтами правопорядка, образовательными организациями, семьями и молодыми гражданами.

Ключевые слова: молодежь, доверие, полиция, институты правопорядка, киберэкстремизм, терроризм, цифровая среда, профилактика, социальная безопасность.

Современные формы экстремизма и терроризма все чаще связаны с цифровой средой. Интернет и социальные платформы используются не только для распространения радикальных идей, но и для вербовки, психологического воздействия, координации противоправных действий, вовлечения несовершеннолетних и молодежи в рискованные или преступные практики. Поэтому защита от киберэкстремизма и терроризма сегодня должна рассматриваться не только как техническая или уголовно-правовая задача, но и как социальная система, в которой важную роль играет доверие граждан к институтам правопорядка.

Особенно значимой в этом отношении является молодежь. По данным DataReportal, в январе 2025 г. в России насчитывалось 133 млн интернет-пользователей, а уровень проникновения интернета составлял 92,2% населения; число пользовательских идентичностей в социальных сетях оценивалось в 106 млн, или 73,4% населения страны. При этом сам источник отдельно

[1] Зуева Ольга Владимировна – заведующий кафедрой гуманитарных и социально-экономических дисциплин факультета подготовки следователей, Московской академии Следственного комитета имени А.Я. Сухарева, кандидат социологических наук, доцент.

подчеркивает, что такие показатели социальных сетей не всегда равны числу уникальных людей, поскольку речь идет именно об учетных записях и рекламных охватах платформ[1].

Молодежь является наиболее интенсивной аудиторией цифровой коммуникации. Согласно исследованию, ВЦИОМ 2025 г., российская молодежь чаще общается с друзьями и родственниками онлайн, чем вживую: 61% против 33%. В группе 18-24 лет этот разрыв еще заметнее: 69% предпочитают онлайн-общение, тогда как 24% чаще общаются офлайн. ВЦИОМ также фиксирует, что медианное время использования социальных сетей и мессенджеров молодежью составляет около девяти часов в день, а Telegram используется в среднем три-четыре часа в день; 28% молодых пользователей проводят в нем более пяти часов ежедневно[2].

Эти данные показывают, что цифровая среда для молодежи является не внешним дополнением к социальной жизни, а одной из ее базовых сред. Следовательно, профилактика киберэкстремизма и терроризма должна строиться с учетом того, насколько молодые люди доверяют тем институтам, которые призваны обеспечивать безопасность, реагировать на угрозы и помогать в ситуациях риска.

В рамках данной статьи под киберэкстремизмом понимается проявление проявления экстремистской активности с использованием цифровых технологий, а именно распространение радикальной пропаганды, вовлечение в экстремистские сообщества, вербовка, координация действий и психологическое давление. Такое понимание помогает анализировать проблему в социологическом ключе - через коммуникации и механизмы вовлечения, не подменяя юридических определений.

Доверие к институтам правопорядка отражает представление граждан о том, что институт действует предсказуемо, справедливо и в рамках закона. Согласно исследованиям процедурной справедливости, такое доверие повышает готовность людей сотрудничать с правоохранительными органами и соблюдать правовые нормы.

Это принципиально для профилактики киберэкстремизма: если институты воспринимаются как справедливые и компетентные, люди с большей вероятностью обратятся за помощью при столкновении с радикальным контентом или вербовочными сообщениями - и тем самым помогут предупредить угрозы на раннем этапе. Если же институты кажутся закрытыми или карательными, вероятность обращения снижается.

Официальная статистика МВД России показывает, что цифровой компонент преступности остается крайне значимым. В январе-декабре 2025 г. в России было зарегистрировано 1 771,2 тыс. преступлений, что на 7,3% меньше, чем в 2024 г. Однако число преступлений, совершенных с использованием информационно-

[1] Digital 2025: The Russian Federation. 2025 // https://datareportal.com/reports/digital-2025-russian-federation

[2] Живущие в сети, или Медиапотребление современной молодежи. 24 июня 2025 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/zhivushchie-v-seti-ili-mediapotreblenie-sovremennoi-molodezhi

телекоммуникационных технологий или в сфере компьютерной информации, составило 675,4 тыс.; их доля в общей структуре преступности достигла 38,1%. При этом 52,2% таких преступлений относились к тяжким и особо тяжким[1].

Особую тревогу вызывает рост зарегистрированных преступлений террористического и экстремистского характера. По данным МВД России, в 2025 г. было зарегистрировано 5920 преступлений террористического характера, что на 59,4% больше, чем годом ранее, а также 2241 преступление экстремистской направленности, что на 30,4% больше показателя 2024 г. Рост может быть связан не только с распространением угроз, но и с активностью выявления и изменением практик учета.

Особую тревогу вызывает вовлечение молодежи. В 2024 г. несовершеннолетними было совершено 98 преступлений террористического характера и 97 преступлений экстремистской направленности. Там же подчеркивается, что интернет стал одной из основных площадок вовлечения подростков и молодежи в деструктивную активность, включая диверсионные, насильственные, экстремистские и террористические действия. Кроме того, несовершеннолетними в 2024 г. было совершено 7,7 тыс. преступлений с использованием информационно-коммуникационных технологий, что составило почти каждое третье преступное деяние данной возрастной группы[2].

Таким образом, цифровизация молодежной среды требует новых подходов к профилактике. Значительная часть молодежи активно присутствует в молодежной среде, но не всегда обладает достаточной компетентностью для безопасной навигации в ней.

Вопрос доверия к полиции и другим институтам правопорядка имеет особую значимость, поскольку именно доверие определяет готовность граждан к взаимодействию, обращению за помощью и участию в профилактике. По данным ВЦИОМ 2023 г., общий уровень доверия россиян к полиции в своем регионе составлял 66%, тогда как среди молодежи 18–24 лет этот показатель был существенно выше - 85%[3]. Более поздние данные ВЦИОМ 2026 г. также фиксируют высокий уровень доверия к полиции в целом по населению. Согласно исследованию, полиции доверяют 68% россиян, не доверяют 24%, а индекс доверия достиг 44 пунктов[4].

Вместе с тем молодежное доверие к полиции существует на фоне низкого уровня обобщенного межличностного доверия. По данным ВЦИОМ о доверии в России, 73% россиян считают, что в отношениях с людьми следует быть осторожными, и только 24% полагают, что большинству людей можно доверять. Среди молодежи 18–24 лет осторожность выражена еще сильнее: 88% считают,

---

[1] Состояние преступности в России за январь-декабрь 2025 года. https://мвд.рф/reports/item/77848182/

[2] Опасный возраст - время выбора. 2025 г. https://mvdmedia.ru/publications/police-of-russia/sluzhba-pol/opasnyy-vozrast-vremya-vybora/

[3] Профессия: полицейский. 3 ноября 2023 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/professija-policeiskii

[4] Реформа МВД: 15 лет спустя. 2026 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/reforma-mvd-15-let-spustja

что в отношениях с людьми необходимо быть осторожными, а лишь 12% говорят, что большинству людей можно доверять.

Это создает важный социологический парадокс. С одной стороны, молодежь демонстрирует низкий уровень межличностного доверия, что может усиливать тревожность, замкнутость и склонность полагаться на узкие онлайн-сообщества. С другой стороны, высокий уровень доверия к полиции среди молодых граждан может выступать институциональным компенсатором: при правильной организации взаимодействия институты правопорядка способны становиться для молодежи не только силовой структурой, но и понятным каналом защиты.

Доверие молодежи к институтам правопорядка выполняет несколько функций в системе защиты от киберэкстремизма и терроризма.

Во-первых, оно снижает барьер первичного обращения. При столкновении с вербовкой или радикальным контентом молодой человек с большей вероятностью обратится в полицию или другие структуры.

Во-вторых, доверие повышает эффективность профилактической коммуникации. Предупреждения о рисках вовлечения в экстремизм лучше воспринимаются, если правоохранительные институты считаются компетентными и справедливыми.

В-третьих, доверие способствует формированию совместной безопасности. Раннее выявление угроз в онлайн-среде зависит от готовности молодежи сообщать о подозрительной активности – а это возможно при наличии доверия.

В-четвертых, доверие помогает предотвращать вторичную радикализацию. Профилактика на принципах процедурной справедливости (уважительное обращение, защита конфиденциальности, отказ от стигматизации) снижает риск отчуждения и восприимчивости к радикальным идеям.

С учетом приведенных данных можно выделить несколько направлений развития системы защиты молодежи от киберэкстремизма и терроризма.

Первое направление - создание понятных и безопасных каналов обращения. Обеспечить молодежь доступными цифровыми формами консультации: чат-боты, разделы на сайтах, возможностью анонимизированных обращений и понятными инструкциями на случай подозрительных контактов в сети.

Второе направление - развитие профилактики в образовательной среде. Заменить общие темы лекций о терроризме разбором реальных сценариев вовлечения.

Третье направление - повышение процедурной справедливости в контактах с молодежью. Строить профилактическое взаимодействие с молодежью как диалог, а не как давление – негативный опыт общения с правоохранителями снижает доверие к ним в целом.

Четвертое направление - работа с родителями, педагогами и значимыми взрослыми. Помочь им распознать тревожные сигналы в поведении подростков и создать условия для обращения за помощью без страха «навредить» ребенку.

Пятое направление - регулярная социологическая диагностика. Оценивать эффективность профилактики не только по числу мероприятий или выявленных материалов, но и по уровню доверия молодёжи к полиции, готовности обращаться за помощью, уровню цифровой и правовой грамотности и т.д.

Доверие молодежи к институтам правопорядка является не второстепенным моральным ресурсом, а важным элементом системы защиты от киберэкстремизма и терроризма. В условиях, когда молодежь проводит значительную часть социальной жизни в цифровой среде, а преступления террористического и экстремистского характера демонстрируют заметный рост в официальной статистике, профилактика должна опираться не только на контроль и блокировку опасного контента, но и на устойчивую коммуникацию между молодежью и институтами безопасности.

Социологические данные показывают, что у российских молодых граждан существует значительный потенциал институционального доверия: по данным ВЦИОМ, в 2023 г. полиции в своем регионе доверяли 85% респондентов 18–24 лет. Однако этот ресурс не является гарантированным. Он требует постоянного поддержания через справедливые процедуры, уважительное обращение, прозрачные каналы помощи и молодежно-ориентированную профилактику.

Таким образом, доверие молодежи к институтам правопорядка можно рассматривать как один из элементов социальной устойчивости общества перед угрозами киберэкстремизма и терроризма. Оно повышает вероятность раннего обращения за помощью, усиливает восприимчивость к профилактическим сообщениям, способствует общественному участию в выявлении рисков и снижает отчуждение, которым часто пользуются радикальные онлайн-сообщества.

Список источников

1. Digital 2025: The Russian Federation. 2025 // https://datareportal.com/reports/digital-2025-russian-federation
2. Живущие в сети, или Медиапотребление современной молодежи. 24 июня 2025 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/zhivushchie-v-seti-ili-mediapotreblenie-sovremennoi-molodezhi
3. Состояние преступности в России за январь-декабрь 2025 года. https://мвд.рф/reports/item/77848182/
4. Опасный возраст - время выбора. 2025 г. https://mvdmedia.ru/publications/police-of-russia/sluzhba-pol/opasnyy-vozrast-vremya-vybora/
5. Профессия: полицейский. 3 ноября 2023 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/professija-policeiskii
6. Реформа МВД: 15 лет спустя. 2026 г. // https://wciom.ru/analytical-reviews/analiticheskii-obzor/reforma-mvd-15-let-spustja

А.А. Лебедева[1]

ИГРОВЫЕ ПЛАТФОРМЫ КАК СРЕДСТВА ВЕРБОВКИ БИОДРОНОВ

Аннотация. В статье рассмотрена возможность использования игровых платформ в качестве мест вовлечение в противоправную деятельность. Материал подкреплен примерами из судебной и следственной практики.

Ключевые слова: расследование, способ совершения преступления, вербовка, видеоигры, биодроны.

В российском юридической действительности всё чаще употребляется термин «биодрон» или «биологический дрон», используемый сотрудниками правоохранительных органов в отношении обозначения лиц, завербованных для совершения экстремистских действий и террористических актов на территории РФ.

«Биодрон» представляет собой живой организм, генетически модифицированный или обученный для выполнения специфических задач. Это может быть насекомое, птица или даже млекопитающее, оснащенное микроэлектронными устройствами для передачи данных и выполнения команд. Управление «биодроном» требует от оператора не только технических навыков, но и глубокого понимания психологии. Операторы должны уметь установить эмоциональную связь с организмом, что может быть сложно из-за биологических различий[2].

В научной литературе понятие «биодроны» используются для обозначения индивидов, чьи действия находятся под внешним контролем и управлением. «Биодроны», «зомби-террористы» легко поддаются манипуляциям и могут быть направлены на совершение любых диверсионных, противоправных и агрессивных действий, вплоть до убийств.[3]

---

1 Лебедева Анна андреевна – заведующая кафедрой информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, к.ю.н., доцент

2 Чудаков А.Ю. Новая эра боевых действий: влияние беспилотных летательных аппаратов на тактику войск и медицинскую поддержку в зоне СВО / А.Ю. Чудаков, А.А. Жуков, С.А. Бондаренко, А.В. Вертаев // Забота о здоровье военнослужащих Росгвардии – вклад в обороноспособность и стабильность государства: сборник научных трудов. Сер. «Теория и методика обучения и воспитания взрослых». СПб., 2025. С. 27-31.

3 Ениколопов С.Н. Терроризм и агрессивное поведение // Национальный психологический журнал. 2006. № 1. С. 28-32.; Психология и психопатология терроризма. Гуманитарные стратегии антитеррора / Под ред. проф. М.М. Решетникова. СПб.: Изд. «Юрайт», 2025. 257 с.; Спирина Е.В. Суицидный терроризм – субъект в структуре угроз национальной безопасности и нарушения политической стабильности на территории Российской Федерации // Молодой ученый. 2013. № 5 (52). С. 566-572.

Так, Дарья Трепова, осуждена за организацию теракта в кафе на Университетской набережной в Санкт-Петербурге, в результате которого погиб военкор Владлен Татарский.

Первазивная игра — это видеоигра, в которой игровой опыт распространяется на реальный мир, или где вымышленный, виртуальный мир, в котором происходит действие игры, сливается с физическим миром.[1]

Первое определение первазивной игры звучало так: «игра в жанре живой ролевой игры (Live action role-playing game), дополненная вычислительными и коммуникационными технологиями таким образом, что физическое и цифровое пространство объединяются».[2] Термин имеет несколько интерпретаций — от использования «нестандартных устройств ввода» до игры, которая «сочетается с повседневным опытом».

Одной из разновидности первазивной игры является так называемая «игра в альтернативной реальности» - ARG (Alternative Reality Game).

В ARG главный герой, не выдуманный персонаж, а сам человек. Грань между воображением и действительностью стирается. У игрока при глубокой степени погруженности в игровую среду, формируется впечатление о реальности происходящего. Лицо перестает отделять виртуальную реальность с игровым контентом, от действий и событий в физическом мире.

В 2005 году появилась видеоигра «Last Call Poker», действия которой разворачивались как в виртуальном пространстве на покерном сайте, так и на территории городских кладбищ, где игроки приводили в порядок заброшенные могилы и выполняли другие задания.[3]

В июле 2013 года Walt Disney Imagineering Research & Development и The Walt Disney Studios выпустили ARG игру «The Optimist». Концепция игры подразумевала «выход» за пределы интернета в реальность и использование различных форм взаимодействия — от социальных сетей и мобильных устройств до физического посещения городских локаций для поиска артефактов[4].

В отличие от традиционного агента, биодрон не проходит длительную подготовку, его поиск осуществляется в интернете: в чатах геймеров, на сайтах знакомств, при помощи виртуальных механизмов в видеоиграх.

Так, С., обвиняемый в убийстве предпринимательницы, мог стать объектом внимания мошенников из-за участия в телеграм-чатах по теме ставок. Обвиняемый страдает игроманией, но официально пользоваться услугами

---

1 Benford, Steve; Magerkurth, Carsten; Ljungstrand, Peter (2005), Bridging the physical and digital in pervasive gaming (PDF), Communications of the ACM, ACM, pp. 54–57, archived from the original (PDF) on 11 November 2014

2 Schneider, Jay; Kortuem, Gerd (2001). "How to Host a Pervasive Game: Supporting Face-to-Face Interactions in Live-Action Roleplaying". Designing Ubiquitous Computing Games Workshop at UbiComp (position paper). Atlanta, Georgia, USA. pp. 1–6.

3 Daniel Terdiman 'Last Call Poker' celebrates cemeteries// URL//https://www.cnet.com/tech/gaming/last-call-poker-celebrates-cemeteries (дата обращения 29.05.26)

4 Michael Andersen "The Optimist" Draws Fans Into Fictionalized Disney History// URL// https://web.archive.org/web/20190116200808/https://www.wired.com/2013/07/disney-the-optimist-arg/ (дата обращения 29.05.26)

букмекеров не мог — его аккаунт сразу бы заблокировали из-за запрета FIFA для профессиональных спортсменов. Поэтому С. делал ставки через специальные чаты, пока не стал жертвой вербовщиков.

По мнению следствия, подобным же образом вербовщики могли склонить к сотрудничеству и С., которая в чате инди-игры «Sky: Дети света», переписывалась с гражданами Украины.[1]

Виртуальные механизмы, используемые в компьютерных играх – технологические решения и системы, которые обеспечивают взаимодействие игрока с игровым миром, его погружение в виртуальную среду, анимацию персонажей и другие аспекты геймплея. К ним относят аккаунты и внутриигровые чаты.

Аккаунт – это учётная запись пользователя, которая позволяет взаимодействовать с игровым миром. Через аккаунт игрок может: создавать персонажей; совершенствовать навыки и характеристики; покупать или получать так называемое «виртуальное игровое имущество», взаимодействовать с другими игроками или службой поддержки, сохранять прогресс игры.

Внутриигровые чаты — инструменты для общения игроков друг с другом в реальном времени. Они бывают двух основных типов:

Текстовый чат — позволяет игрокам обмениваться сообщениями в структурированной форме. Может включать заранее заданные сообщения, шаблоны или ограниченные текстовые поля, блокирующие определённые слова или фразы.

Голосовой чат — даёт возможность игрокам общаться через микрофоны и динамики. Позволяет разрабатывать стратегии, общаться «онлайн».

Внутриигровые чаты могут использоваться как для вовлечения лиц, в том числе несовершеннолетних в преступную деятельность, так и для обсуждения преступления.

Вербовщики в таких чатах маскируются под опытных игроков или администраторов сообщества. Они предлагают участникам присоединиться к первазивной игре, в которой задания пошагово переносятся из виртуальной реальности на физические объекты.

Так, трое несовершеннолетних осуждены за подготовку взрывов в зданиях силовых структур. Обвинение основывалось на переписке подростков в чате, где они обсуждали планы диверсии в здании ФСБ в виртуальном мире Minecraft.[2]

Осужденный за подготовку к теракту, в судебной стадии показал, что его настраивал «против власти» «лидер» группы. *«У нас были одни и те же взгляды, анархические. Потом наш лидер начал нас заинтересовывать взрывчатыми веществами, обучал нас этому со временем. Потом он начал нам внушать,*

[1] URL:https://life.ru/p/1852888 (дата обращения:18.04.2026).

[2] Шарапов В. Российского подростка посадили за подготовку взрыва здания ФСБ в игре Minecraft. URL:https://lenta.ru/brief/2022/02/10/minecraft/(дата обращения:18.04.2026).

что ФСБ, ну, власть — наш главный враг, [что] мы должны подорвать здание ФСБ, чтобы отомстить за политзаключенных», заявил несовершеннолетний[1].

Многие игровые платформы сегодня функционируют как социальные сети, предлагая пользователям возможности для публикации контента, обмена сообщениями и участия в игровых сообществах.

Начиная с 2022 года, согласно сведениям правоохранительных органов, количество интернет-ресурсов с признаками вербовки биодронов для диверсионной деятельности возросло в разы, а сайты игровых платформ используются чаще.

Список источников

1. Ениколопов С.Н. Терроризм и агрессивное поведение // Национальный психологический журнал. 2006. № 1. С. 28-32.; Психология и психопатология терроризма. Гуманитарные стратегии антитеррора / Под ред. проф. М.М. Решетникова. СПб.: Изд. «Юрайт», 2025. 257 с.;
2. Спирина Е.В. Суицидный терроризм – субъект в структуре угроз национальной безопасности и нарушения политической стабильности на территории Российской Федерации // Молодой ученый. 2013. № 5 (52). С. 566-572.
3. Чудаков А.Ю. Новая эра боевых действий: влияние беспилотных летательных аппаратов на тактику войск и медицинскую поддержку в зоне СВО / А.Ю. Чудаков, А.А. Жуков, С.А. Бондаренко, А.В. Вертаев // Забота о здоровье военнослужащих Росгвардии – вклад в обороноспособность и стабильность государства: сборник научных трудов. Сер. «Теория и методика обучения и воспитания взрослых». СПб., 2025. С. 27-31.
4. Шарапов В. Российского подростка посадили за подготовку взрыва здания ФСБ в игре Minecraft. URL:https://lenta.ru/brief/2022/02/10/minecraft/(дата обращения:18.04.2026).
5. Benford, Steve; Magerkurth, Carsten; Ljungstrand, Peter (2005), Bridging the physical and digital in pervasive gaming (PDF), Communications of the ACM, ACM, pp. 54–57, archived from the original (PDF) on 11 November 2014
6. Daniel Terdiman ‘Last Call Poker’ celebrates cemeteries// URL//https://www.cnet.com/tech/gaming/last-call-poker-celebrates-cemeteries (дата обращения 29.05.26)
7. Michael Andersen "The Optimist" Draws Fans Into Fictionalized Disney History// URL// https:// web.archive.org/web/20190116200808/https://www.wired.com/2013/07/disney-the-optimist-arg/ (дата обращения 29.05.26)

[1] Шарапов В. Российского подростка посадили за подготовку взрыва здания ФСБ в игре Minecraft. URL:https://lenta.ru/brief/2022/02/10/minecraft/(дата обращения:18.04.2026).

8. Schneider, Jay; Kortuem, Gerd (2001). "How to Host a Pervasive Game: Supporting Face-to-Face Interactions in Live-Action Roleplaying". Designing Ubiquitous Computing Games Workshop at UbiComp (position paper). Atlanta, Georgia, USA. pp. 1–6.
9. URL:https://life.ru/p/1852888 (дата обращения:18.04.2026).

Е.Д. Леонтьев[1]
Научный руководитель: **Е.И. Бычкова**[2]

КИБЕРНЕТИЧЕСКИЙ ПОДХОД В АНАЛИЗЕ ВЛИЯНИЯ НОВЫХ ФОРМ ДИСТАНЦИОННОГО ВОЗДЕЙСТВИЯ КИБЕРЭКСТРЕМИСТОВ НА САМОСОЗНАНИЕ МОЛОДЕЖНОЙ АУДИТОРИИ

Аннотация. В статье с позиций кибернетического подхода анализируется влияние киберэкстремистов на российскую молодежь. Раскрывается феномен двойного управления, закон необходимого разнообразия Эшби и динамика преступлений экстремистской направленности с использованием сети Интернет в 2024–2025 гг.

Ключевые слова: киберэкстремизм, кибернетический подход, молодежь, дистанционное воздействие, двойное управление.

Как известно, перед Российской Федерацией предстают перспективы социального и экономического развития. Вместе с тем вызовы наступившей информационной эры и осложненной геополитической обстановки требуют совершенствовать меры обеспечения безопасности общества. Подобные тенденции сопровождаются активизацией отдельных субъектов, целью которых является дестабилизация общественного порядка и законности. Вышеупомянутые лица, радикально действуя против общества и государства, широко применяют нетривиальные способы, отличающиеся своей новизной. При этом необходимо отметить, что зачастую противоправные деяния направлены против и молодежи.

Актуальность обуславливается тем, что Стратегия национальной безопасности РФ определяет цели государственной и общественной безопасности, достижение которых находится в прямой зависимости от реализации политики в области профилактики экстремистских (киберэкстремизм – подвид экстремизма) и иных преступных проявлений, особенно среди наиболее уязвимой группы населения - молодежи. Также применение кибернетического подхода позволит рассмотреть проблему киберэкстремизма в молодежной среде с точки зрения отдельной синтетической науки, сформулировать выводы, применяя нетрадиционный в юриспруденции понятийно-категориальный аппарат.

---

[1] Леонтьев Егор Дмитриевич – курсант 1 курса факультета подготовки следователей Московской академии Следственного комитета имени А.Я. Сухарева.

[2] Бычкова Екатерина Игоревна – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

Основные постулаты и законы кибернетики позволят рассмотреть отдельные стороны указанного противоправного деяния и уделить внимание причинам распространения киберэкстремизма на поведение подростков (в том числе и молодежи в целом). При этом отметим, что работа носит обзорно-аналитический характер.

Кибернетика, являясь наукой «*об общих закономерностях процессов управления и передачи информации в различных системах, будь то машины, живые организмы или общество*»[1], фокусируется на изучении саморегулирующейся системы функционирования субъекта управления, который контролирует и корректирует управляемый субъект путем управления[2].

Центральным понятием в теории Н. Винера является обратная связь, механизм которой позволяет системе корректировать свое поведение на основе поступающих данных о результатах предыдущих действий. В данном контексте информация приобретает значение не просто как передаваемое сообщение, а как содержательный компонент сигнала, который способен изменять состояние системы.

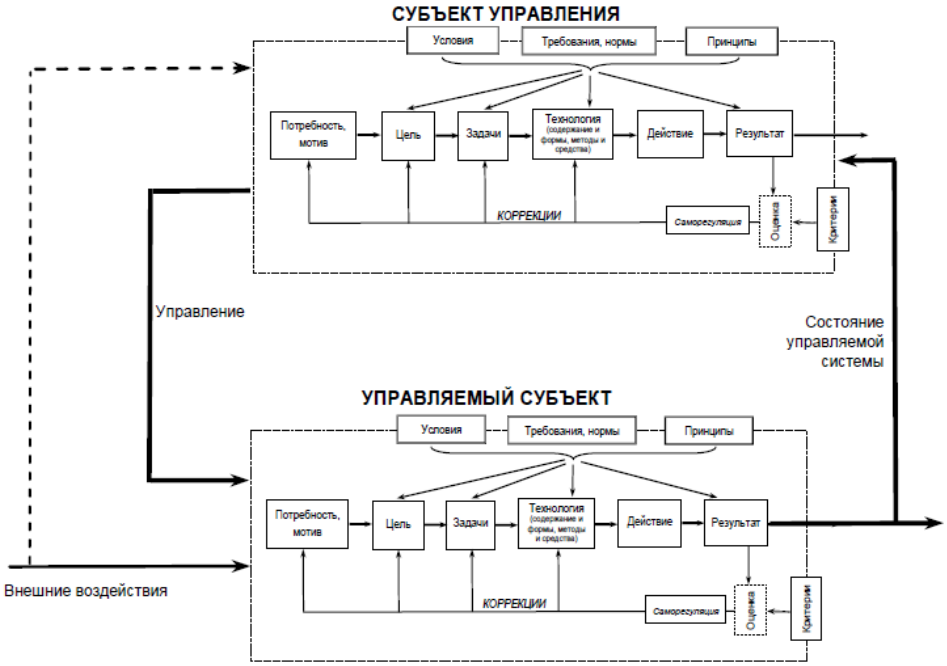

Рис.1 Структура управленческой деятельности

В области права, **субъектом управления** выступает государство, его органы и аппарат публичной власти, которые воздействуют на **управляемый субъект** путем реализации государственной воли (правотворчества и правоприменения в том числе). Государство формирует **управляющее воздействие** в виде законов, подзаконные актов, судебных решений и других нормативных актов. Общество, подвергаясь применению государственной воли, претерпевает изменение: с течением времени субъекты общественных отношений корректируют модели

[1] Винер Н. Кибернетика или управление и связь в животном и машине. – М.: Наука, 1983. – 338 с.

[2] Управление – это систематизированная совокупность способов и приемов по изменению параметров управляемого субъекта.

поведения, что в количественном выражении при нормальных условиях влияет на поддержание стабильности в системе.

Информация о достигнутом результате поступает к управляющему субъекту по **каналу обратной связи** (судебная статистика, отчёты правоохранительных органов, протестные акции, прокурорские проверки). Полученная информация сравнивается с первоначальной целью, и при отклонении показателей корректируется форма управляющего воздействия.

Таким образом, главной целью такой системы является поддержание законности и правопорядка, а равно сохранение безопасности внутри государства и общества. Однако, напротив, возникают противоправные явления, которые дестабилизируют состояние общества.

По признанию В.В. Бычкова, киберэкстремизм – «*системно организованные, целенаправленные, общественно опасные, сознательно совершаемые информационные индивидуальные или групповые* ***атаки на сознание и психику*** *неограниченного количества пользователей социальных сетей и других современных средств электронной информации, совершаемые с использованием компьютеризованных устройств, современных информационных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет, с целью возбуждения общественно опасных политических, идеологических, расовых, национальных, религиозных ненависти или вражды, а также ненависти или вражды в отношении какой-либо социальной группы, сопровождаемые соответствующими организационными, техническими и финансовыми мерами, запрещенные рядом уголовно-правовых норм Особенной части Уголовного кодекса РФ*»[1].

Опираясь на дефиницию, представленную выше, отметим, что в одном из смыслов, киберэкстремист – субъект, совершающий противоправные деяния по вовлечению лиц в деятельность экстремистской направленности. С кибернетической точки зрения, можно сказать, что данный субъект также претендует на роль субъекта управления по отношению к российской молодежи, реализуя свою деструктивную волю. Таким образом, российская молодежь подвергается двойному управлению, последнее из которых прямо является угрозой национальной безопасности РФ.

Анализируя уникальное явление, необходимо упомянуть закон «необходимого разнообразия» У.Р. Эшби[2]. Согласно закону, государству, выступая регулятором, необходимо поддерживать такое разнообразие применяемых правовых средств, которое соответствовало бы сложности управляемого субъекта. Такое разнообразие детерминируется социально-экономическими условиями жизнедеятельности представителей молодежи, их возрастом, соблюдением правовых норм субъектами правоотношений в отдельных территориальных образованиях страны, удовлетворением

---

[1] Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д. ю. н., д. т. н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. 572 с.

[2] Эшби У.Р. Введение в кибернетику. М.: Мир, 1966. 432 с.

потребностей населения и иных критериев, влияющих на подчинение государственной воле. Приведенные условия сохранения удовлетворенности в молодежной среде занимают ключевое место в обеспечении общественной безопасности, минимизируя проявление заинтересованности к идеологии экстремизма.

Указанные критерии киберэкстремисты также учитывают в формировании информационного воздействия на представителей молодежной аудитории, так как подобные условия определяют психоэмоциональное состояние индивида, степень его вовлеченности в изучении экстремистских идей. У представителей последней возрастной группы ввиду физиологических причин в полной мере не сформировались навыки критического мышления. Критическое мышление, выступающее ключевым условием распознавания информационного воздействия экстремистского характера, окончательно формируется только к возрасту 23-25 лет, а пока до этого возраста лица особенно подвержены деструктивному влиянию[1].

В Уголовном кодексе РФ, по мнению А.Э. Побегайло, к преступлениям экстремистского характера можно отнести: ст. 280, 280.1, 280.3, 280.4, 282, 282.1, 282.2, 282.3[2]. Более того, превалирующая часть указанных составов преступлений совершается с активным применением информационно-коммуникационных технологий[3].

Табл.1

Динамика преступлений экстремистской направленности, совершаемых несовершеннолетними с использованием сети Интернет за 2024-2025 гг.

№	Показатель	2024 г.	2025 г.	Источник
1.	Общее количество преступлений с использованием ИКТ в РФ	Около 765 тыс.	-	Интерфакс – Россия[4]; Вести.ru[5]
2.	Доля преступлений несовершеннолетних,	-	30,4%	Парламентская газета[6]

[1] Бычков В. В. Дети и молодежь как объект киберэкстремизма // Вестник Московского университета МВД России. 2022. № 3. С. 48–53.

[2] Побегайло А.Э. Киберэкстремизм – угроза национальной безопасности // Обозреватель–Observer. – 2025. – № 5. – С. 105-119.

[3] Там же.

[4] Число преступлений с использованием интернет-ресурсов возросло в РФ за семь лет в 7,5 раза – Бастрыкин URL: https://www.interfax-russia.ru/military/news/637564 / (дата обращения: 27.05.2026).

[5] МВД: почти 40% преступлений совершаются с использованием IT-технологий URL: https://www.vesti.ru/article/4309832 / (дата обращения: 27.05.2026).

[6] МВД: Почти треть преступлений подростков совершены с использованием IT-технологий URL: https://www.pnp.ru/social/mvd-pochti-tret-prestupleniy-podrostkov-soversheny-s-ispolzovaniem-it-tekhnologiy.html / (дата обращения: 27.05.2026).

	совершенных с использованием ИКТ			
3.	Количество преступлений, несовершеннолетних с использованием ИКТ	Около 7,7 тыс.	8,8 тыс.	Парламентская газета[1]
4.	Количество преступлений экстремистского и террористического характера, совершенных несовершеннолетними с использованием ИКТ	- около 258 (показатель рассчитан ретроспективно исходя из официального роста в 2025 г.)	266	Парламентская газета[2]
5.	Количество несовершеннолетних, осужденных за террористические преступления	48	-	Вести.ru[3]
6.	Рост преступлений экстремистской направленности в РФ	-	+ 36,2%	МВД Медиа[4]
7.	Рост террористических преступлений в РФ	-	+ 75%	Парламентская газета[5]

Приведенная статистика, основанная на сведениях официальных ресурсов государственных органов (каналах обратной связи), позволяет обоснованно предположить, что киберэкстремисты более верно применяют формы дистанционного воздействия, среди которых:

- таргетированное «дружеское» вовлечение через фейковые аккаунты;
- шантаж и компрометация (доксинг);
- функционирование ботов - «провокаторов» в комментариях известных публичных лиц;
- экстремистские челленджи и флешмобы;
- подмена понятий через квазиобразовательный процесс;
- дистанционное «кураторство» малых групп (метод «спящих ячеек»);
- трансформация онлайн-знакомств в реальные встречи;
- игровое вовлечение на платформах (Roblox, Minecraft);
- медиа-вирусы в формах легкозапоминающихся семантических конструкций;
- анонимные опросы и тесты на «патриотизм».

[1] Там же.
[2] Там же.
[3] В РФ за террористические преступления осудили 870 человек в 2024 году URL: https://www.vesti.ru/article/4459811 / (дата обращения: 27.05.2026).
[4] МВД Медиа. Статистика и аналитика / О состоянии преступности в Российской Федерации за январь-апрель 2025 г. URL: https://mvdmedia.ru/news/official/ / (дата обращения: 27.05.2026).
[5] Число террористических преступлений выросло на 75 % URL: https://www.pnp.ru/social/chislo-terroristicheskikh-prestupleniy-vyroslo-na-75.html / (дата обращения: 27.05.2026).

Если рассмотреть явление киберэкстремизма через призму кибернетики, то становится очевидно, что деструктивные группы создали параллельную систему управления молодежной аудиторией. В отличие от государства, которое действует открыто, реализуя комплекс правовых средств, киберэкстремисты конструируют замкнутые контуры обратной связи. Последние отслеживают реакции подростков (лайки, репосты, личные сообщения) и мгновенно подстраивают свои воздействия. Молодежь оказывается в ситуации двойного управления, где регулятор (государство) не всегда успевает за скоростью и разнообразием деструктивных сигналов.

При этом очень важно подчеркнуть, что экстремизм в своей сущности также является формой обратной связи от общества к государству. На феномен экстремизма влияет большое количество факторов, одним из которых является действующая система законодательства государства. Более того, до государственных органов отклик о дисфункции безопасности доходит после нарушения состояния защищенности.

Особенно уязвимыми молодых людей делает незавершенное формирование критического мышления - по данным возрастной психологии, оно окончательно складывается лишь к 23–25 годам. В этих условиях действует закон «необходимого разнообразия» Эшби: чтобы управлять сложной системой (в данном случае - молодежной средой с ее разными социальными, возрастными и психологическими характеристиками), регулятор должен обладать не меньшим разнообразием инструментов.

Государство же пока в некоторой степени действует шаблонно, хоть и предпринимает попытки создания контр-информационных воздействий (например, «Лига безопасного интернета»), однако вопрос об их эффективности остается открытым.

На «выходе» системы можно наблюдать устойчивый рост зафиксированных преступлений экстремистской направленности среди несовершеннолетних в 2024–2025 гг. Данный статистические данные выступают явным сигналом потенциальной деструкции системы.

Особую озабоченность проблемой вызывает положение, согласно которому можно утверждать, что люди в возрасте 26-35 лет при условии сложившегося навыка критического мышления идут на совершение преступления экстремистской направленности. Возможно, число правонарушений кратно меньше, чем в более раннем возрасте, однако необходимо подчеркнуть, что психический фактор в принятии решения человеком в любом возрасте о преступлении границы закона является неисчерпывающим.

По мнению А.М. Багмета и В.В. Бычкова, эффективность противодействия экстремизму и, в частности, преступлениям экстремистской направленности, повысится в случае устранения подпитывающей их базы из числа подростков и молодежи[1].

[1] Багмет А. М., Бычков В. В. и др. Молодежный экстремизм. Понятие и противодействие: учеб. пособие / под ред. А. М. Багмета. М. : ЮНИТИ-ДАНА, 2020.

Для нейтрализации угроз киберэкстремизма предлагается комплекс мер, нацеленных на восстановление кибернетической «законности». Во-первых, повысить разнообразие управляющих воздействий: внедрить нейросетевой мониторинг закрытых каналов связи (мессенджеры, игровые платформы) с функцией раннего выявления криминогенных паттернов. Во-вторых, усилить канал позитивной обратной связи – организовать системную контрпропаганду через лидеров мнений и блогеров, ориентированных на молодёжь, с разъяснением правовых последствий участия в экстремистской деятельности. В-третьих, интегрировать в образовательные программы модули по развитию критического мышления и цифровой гигиены, начиная с младшего школьного возраста. В-четвёртых, совершенствовать институт ресоциализации несовершеннолетних правонарушителей (в том числе с привлечением психологов и бывших участников деструктивных групп). Реализация предложенных мер позволит сократить латентность киберэкстремизма и снизить уязвимость молодёжной аудитории перед деструктивным информационным воздействием.

Список источников

1. Багмет А.М., Бычков В. В. и др. Молодежный экстремизм. Понятие и противодействие: учеб. пособие / под ред. А. М. Багмета. М. : ЮНИТИ-ДАНА, 2020.
2. Бычков В.В. Дети и молодежь как объект киберэкстремизма // Вестник Московского университета МВД России. 2022. № 3. С. 48–53.
3. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография / под ред. д. ю. н., д. т. н., проф. В.А. Прорвича. М.: Альпен-Принт, 2024. 572 с.
4. Винер Н. Кибернетика или управление и связь в животном и машине. – М.: Наука, 1983. – 338 с.
5. Побегайло А.Э. Киберэкстремизм – угроза национальной безопасности // Обозреватель–Observer. – 2025. – № 5. – С. 105-119.
6. Эшби У.Р. Введение в кибернетику. М.: Мир, 1966. 432 с.
7. В РФ за террористические преступления осудили 870 человек в 2024 году URL: https://www.vesti.ru/article/4459811 / (дата обращения: 27.05.2026).
8. МВД: почти 40% преступлений совершаются с использованием IT-технологий URL: https://www.vesti.ru/article/4309832 / (дата обращения: 27.05.2026).
9. МВД: Почти треть преступлений подростков совершены с использованием IT-технологий URL: https://www.pnp.ru/social/mvd-pochti-tret-prestupleniy-podrostkov-soversheny-s-ispolzovaniem-it-tekhnologiy.html / (дата обращения: 27.05.2026).
10. МВД Медиа. Статистика и аналитика / О состоянии преступности в Российской Федерации за январь-апрель 2025 г. URL: https://mvdmedia.ru/news/official/ / (дата обращения: 27.05.2026).

11. Число преступлений с использованием интернет-ресурсов возросло в РФ за семь лет в 7,5 раза – Бастрыкин URL: https://www.interfax-russia.ru/military/news/637564 / (дата обращения: 27.05.2026).
12. Число террористических преступлений выросло на 75 % URL: https://www.pnp.ru/social/chislo-terroristicheskikh-prestupleniy-vyroslo-na-75.html / (дата обращения: 27.05.2026).

А.П. Опальский[1]
М.Р. Зинуров[2]

ПРОФИЛАКТИКА ИДЕОЛОГИИ ТЕРРОРИЗМА: ОТ СИЛОВОГО РЕАГИРОВАНИЯ К СОЦИАЛЬНОМУ ИММУНИТЕТУ

Аннотация. В статье рассматриваются основные каналы проникновения радикальных религиозных идей, социально-экономические факторы, способствующие их укоренению, а также региональная специфика этого процесса. Особое внимание уделяется трансформации методов вербовки в условиях цифровизации и миграционных потоков. Киберпреступления не меняют сущность того, на что они направлены, поскольку основная цель кибертерроризма – террор, устрашение – достигается с использованием либо средств массовой информации, либо устройств с программными продуктами.

Представлен анализ существующих государственных и общественных механизмов противодействия терроризму, выявлены их слабые стороны и предложен комплекс мер по профилактике радикализации.

Ключевые слова: миграционные потоки, радикализация, профилактика терроризма

Публикации последнего времени ставят в один ряд такие социальные явления, как терроризм и экстремизм. Но если терроризм всегда связан с насилием, то попытка нарушения целостности государства, отрыв части от целого и образование новой политической организации власти на определённой территории может быть осуществлена «мирным» путём, как это было, например, при создании Калужской Советской Республики (февраль – июль 1918 г.), Горской республики (май 1917 г. – март 1920 г.) и, конечно же, Уральской республики (июль – ноябрь 1993 г.).

Мирно ушёл со своего поста первый мэр Москвы Гавриил Харитонович Попов, а вот второй мэр – Юрий Михайлович Лужков – был снят с должности по указу Президента Медведева в связи с утратой доверия.

Неравномерное развитие регионов, зависимость периферии от центра плюс миграционные потоки вызывают центробежные социальные процессы. Здесь необходимо вспомнить про сепаратизм, под которым понимается деятельность, направленная на подрыв целостности государства путём отделения от последнего какой-либо его части. Некоторые авторы считают, что это «может выражаться как в насильственных действиях, так и в информационно-

[1] Опальский Александр Павлович – профессор Института государственной службы и управления Президентской академии (РАНХиГС), д-р экономических наук, профессор.
[2] Зинуров Максим Рафаэлевич – магистрант Президентской академии (РАНХиГС).

психологическом и гуманитарно-технологическом воздействии» [4]. В определении понятий «сепаратизм», «экстремизм», «терроризм» Россия опирается на подписанную ей Шанхайскую конвенцию о борьбе с терроризмом, сепаратизмом и экстремизмом. В этом документе сепаратизмом называется деяние (или его планирование и подготовка), направленные на нарушение территориальной целостности государства, совершаемое насильственным путём.

Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (с изм. и доп.) определяет проявления экстремизма такими видами, как: насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации (в том числе отчуждение части территории Российской Федерации), за исключением делимитации, демаркации, редемаркации Государственной границы Российской Федерации с сопредельными государствами; публичное оправдание терроризма и иная террористическая деятельность и другими.

В 1996 году Россель первым из российских губернаторов подписал договор о разграничении полномочий области с центром, после чего предпринимал попытки введения в области «не прописанных ни в одном федеральном законе местных налогов», а также использования в регионе собственной валюты – уральского франка.

Борис Савинков в книге «Воспоминания террориста» приводит проект устава боевой организации, в котором описана её цель. Она заключается «в борьбе с существующим строем посредством устранения тех представителей его, которые будут признаны наиболее преступными и опасными врагами свободы. Устраняя их, боевая организация совершает не только акт самозащиты, но и действует наступательно, внося страх и дезорганизацию в правящие сферы, и стремится довести правительство до сознания невозможности сохранять далее самодержавный строй» [6, с.83].

В конечном счёте самодержавный строй был сметён революцией 1917 года. А развитие советского государства началось с «красного террора». Как оказалось «благими целями вымощена дорога в ад».

Современная антитеррористическая политика всё больше смещается от реактивной модели к профилактической парадигме, направленной на устранение коренных причин радикализации. Как показывает мировая практика, устойчивая защита от терроризма формируется не только за счёт спецопераций, но и через социальный, культурный и образовательный иммунитет населения [5, с.62–69]. Это объясняется тем, что как антисоциальное явление – терроризм редко возникает «на пустом месте». Его питательной средой становятся:

- социальное отчуждение (особенно среди молодёжи мигрантского происхождения);
- идеологическая пустота (поиск смысла через радикальные идеологии);
- экономическая маргинализация (бедность, отсутствие перспектив);
- информационная уязвимость (неспособность критически оценивать контент в соцсетях). [1, с.67]

Эти факторы требуют не столько силового, сколько социально-психологического и просветительского воздействия. профилактика идеологии терроризма отличается от борьбы с терроризмом. Во-первых, для борьбы создаются специальные органы, силовые структуры, а в профилактику вовлечены все институты гражданского общества. Понятно, что среди основных мер борьбы «силовых» ведомств с терроризмом будет предотвращение попадания оружия к террористам, защита критически важной инфраструктуры и противодействие финансированию экстремистской деятельности. Гражданские же инициативы могут принимать самые разные формы: от просветительских проектов до социальных программ, направленных на интеграцию различных групп населения. Например, досуговая занятость молодёжи через образовательные лагеря или летние школы помогает молодым людям найти позитивные способы самореализации и отвлечься от радикальных идей. Также важную роль играют средства массовой информации, которые способны формировать общественное мнение, разъяснять опасность экстремистской идеологии и способствовать воспитанию ответственного политического сознания. Кроме того, религиозные организации активно участвуют в создании атмосферы неприятия религиозной нетерпимости, а творческие деятели используют искусство как мощный инструмент воздействия на сознание людей, разоблачая человеконенавистническую сущность экстремизма. Важным аспектом является также взаимодействие с мигрантами, поскольку их интеграция может снизить риски возникновения межэтнических конфликтов и радикализационных настроений среди местного населения.

Стоит признать, что только усилий гражданского общества недостаточно. Для эффективной профилактики необходима консолидированная позиция государства, которое должно создавать организационные и правовые условия, поддерживать общественные инициативы и координировать действия всех заинтересованных сторон. Таким образом, должны быть исследованы прямые и обратные связи межведомственного взаимодействия и соответствующей модели профилактики, требующей системного анализа.

Таблица 1

Участие федеральных органов власти в профилактике терроризма

Министерство	Ключевые меры
Минобрнауки	Внедрение модулей «Цифровая грамотность» и «Критическое мышление» в школьные программы [7, с.55–60]
Минздрав	Психологическая диагностика и сопровождение лиц из группы риска [3, с.142]
Минкультуры	Финансирование межконфессиональных форумов и культурных обменов [10, с.88]
Минэкономразвития	Программы создания рабочих мест в социально напряжённых регионах
Минцифры	Разработка ИИ-инструментов для мониторинга деструктивного контента [2, с. 44–53]

Комплексный подход, который имеет место в исследовательской практике, предполагает, что каждое министерство выполняет свою антитеррористическую миссию (см. таблицу 1). Систематизация межведомственного взаимодействия предполагает реализацию:

- работы общественных антитеррористических советов (ОАС) при антитеррористических комитетах в каждом субъекте РФ;
- средств федерального грантового фонда «Граждане против террора» с годовым объём бюджета в 2 млрд. рублей);
- проекта «Безопасное сообщество» на уровне муниципалитетов [8, с. 33–39.].

Можно привести успешные примеры профилактики идеологии терроризма.

Пример 1. Республика Дагестан — «Молодёжь против террора» (с 2022 года). Студенты вузов проводят лекции в школах по темам манипуляций в соцсетях и ценностей традиционного ислама. Результат: за 3 года снижение вербовки подростков на 41% [11].

Пример 2. Новосибирск — «Школа антитеррористической грамотности» (2025). 16-часовой курс для учащихся 8–11 классов. Результат: после курса 78 % выпускников корректно идентифицировали террористический призыв в фейковом Telegram-канале (до курса — только 16%).

Для того чтобы профилактика терроризма была закреплена в Национальной стратегии противодействия терроризму как отдельное, самостоятельное направление, в документе должны быть чётко зафиксированы следующие положения:

1. Закрепить профилактику терроризма как отдельное стратегическое направление, стоящее в одном ряду с борьбой и ликвидацией последствий терроризма. Это должно быть отражено в структуре документа, перечне задач и направлений деятельности. Необходимо дать чёткое определение профилактики терроризма (например: «деятельность по выявлению и устранению причин и условий, способствующих возникновению и распространению терроризма»), а также сформулировать её основные задачи:

- разработка и реализация мер по устранению причин и условий, способствующих терроризму;
- противодействие распространению идеологии терроризма;
- прогнозирование и выявление террористических угроз;
- использование разрешённых методов воздействия на лиц, склонных к участию в террористической деятельности;

2. Документ должен содержать перечень конкретных мер по каждому из направлений:

- политические (разрешение конфликтов, снижение напряжённости);
- социально-экономические (оздоровление экономики, социальная защита);
- правовые (неотвратимость наказания, регулирование миграционных процессов);
- информационные (формирование неприятия идеологии насилия, контрпропаганда);

- культурно-образовательные (просвещение, воспитание, межнациональный диалог);

- организационно-технические (защита объектов инфраструктуры);

3. Ввести обязательные межведомственные планы в каждом субъекте РФ. Дополнительно необходимо чётко определить, какие органы власти (федеральные, региональные, муниципальные), институты гражданского общества и граждане участвуют в профилактической деятельности, а также установить механизмы их взаимодействия и координации (например, через НАК);

4. Создать федеральную платформу «Профилактика.РФ» для обмена лучшими практиками [12]. Обеспечить распространение антитеррористического контента, работу со СМИ и Интернет-пространством для формирования в обществе стойкого неприятия идеологии терроризма;

5. Обеспечить финансирование через целевые статьи в бюджете (не менее 0,5% от расходов на безопасность).

Таким образом, профилактика терроризма — это не «мягкая» альтернатива силовым мерам, а их необходимое дополнение. Для закрепления профилактики как отдельного направления в Национальной стратегии требуется её явное выделение в структуре документа, детализация целей, задач, уровней и мер, а также определение ответственных субъектов и механизмов их взаимодействия. Как показывают примеры из Дагестана и Новосибирска, партнёрство государства и общества даёт устойчивый эффект, недоступный ни одной спецслужбе в одиночку.

Список источников:

1. Абдулатипов Р.Г. Региональные аспекты противодействия терроризму (на примере СКФО). — М.: ИД «Проспект», 2023.
2. Белоусов А.В. Цифровая трансформация в обеспечении национальной безопасности // Вопросы государственного и муниципального управления. — 2025. — № 2.
3. Демина О.А. Управление в сфере национальной безопасности: учебное пособие. — М.: РАНХиГС, 2024.
4. Клачков П.В., Подъяпольский С.А. Понятие и значение сепаратизма // Теория и практика общественного развития. 2013. № 12 / URL: https://cyberleninka.ru/article/n/ponyatie-i-znachenie-separatizma?ysclid=mpnxv39vg5273816227 (дата обращения: 27.05.2026)
5. Лебедева Н.М. Социальная профилактика терроризма: международный опыт // Социологические исследования. — 2023. — № 9.
6. Савинков Б.В. Воспоминания террориста / Борис Савинков. – СПб: Азбука, Азбука-Аттикус, 2016.
7. Соколова М.И. Профилактика терроризма в образовательной среде // Образование и общество. — 2024. — № 3.
8. Федоров И.А. Роль гражданского общества в профилактике терроризма // Государственное управление. — 2024. — № 1.

9. Чурилов С.А., Сироткин С.Г. О новом Комплексном плане противодействия идеологии терроризма в Российской Федерации на 2024-2028 годы
10. Шамахов В.А. Антитеррористическая политика: от реакции к предупреждению. — М.: ИМЭМО РАН, 2025.
11. Официальный сайт Правительства Республики Дагестан. Отчёт о реализации проекта «Молодёжь против террора» за 2025 год [Электронный ресурс]. URL: https://dagmintrud.ru
12. Минцифры России. Стратегия развития искусственного интеллекта в Российской Федерации на 2024–2030 годы. — М., 2024.

Н.В. Османова[1]

УГОЛОВНОЕ ПРЕСЛЕДОВАНИЕ ЗА СОВЕРШЕНИЕ ЭКСТРЕМИЗМА ПО МАТЕРИАЛАМ ПРАКТИКИ СЛЕДСТВЕННОГО КОМИТЕТА РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ

Аннотация. В статье на основе материалов практики Следственного комитета Российской Федерации, разъяснений Верховного и Конституционного судов Российской Федерации анализируются процессуальные особенности установления оснований возбуждения уголовных дел о преступлениях экстремистской направленности и определения достаточности доказательств для привлечения лица в качестве обвиняемого. Сформулированы авторские выводы о двухэлементной структуре основания возбуждения уголовного дела по составам с административной преюдицией и о необходимости процессуального ограничения роли судебной экспертизы при оценке достаточности доказательств.

Ключевые слова: уголовное преследование, экстремизм, возбуждение уголовного дела, достаточность доказательств.

Специфика уголовного преследования по делам о преступлениях экстремистской направленности определяется двойственным характером предмета доказывания: наряду с деянием и его последствиями следователь обязан устанавливать мотив политической, идеологической, расовой, национальной или религиозной ненависти либо вражды, что предусмотрено пунктом 2 части 1 статьи 73 УПК РФ и находит дополнительное разъяснения в позиции Пленума Верховного Суда Российской Федерации[2]. Указанное обстоятельство существенно накладывает определенную специфику как на этап возбуждения уголовного дела, так и на последующую оценку достаточности доказательств для привлечения лица в качестве обвиняемого.

---

[1] Османова Надежда Валерьевна – декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

[2] Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (в ред. постановления Пленума Верховного Суда РФ от 23 декабря 2025 г. № 43) // Официальный сайт Верховного Суда Российской Федерации. URL: https://www.vsrf.ru/ (дата обращения: 07.08.2026).

Актуальность темы обусловлена устойчивым ростом числа уголовных дел данной категории. Согласно официальным данным, число подростков, причастных к преступлениям экстремистского и террористического характера, в 2026 г. увеличилось в два раза[1]. Столь значительная динамика делает необходимым системный анализ процессуальных проблем, возникающих на досудебных стадиях производства по делам данной категории.

«Экстремизм и терроризм, – по мнению Председателя Следственного комитета Российской Федерации А.И. Бастрыкина, – являются серьезными вызовами для всего мирового сообщества. Борьба с этими проявлениями — важнейшее направление нашей работы»[2].

Особенности установления оснований возбуждения уголовных дел о преступлениях экстремистской направленности. Согласно части 2 статьи 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления. Применительно к делам экстремистской направленности данное положение приобретает содержательную специфику: уже на стадии доследственной проверки сообщения о преступлении следователь Следственного комитета Российской Федерации обязан не просто зафиксировать событие, подпадающее под признаки состава преступления, предусмотренного статьями 205², 280, 280¹, 282, 282¹, 282², 282³ или 282⁴ УК РФ, но и получить данные, позволяющие с достаточной степенью вероятности полагать наличие специального мотива либо цели, отграничивающих экстремистское преступление от смежных составов.

Пленум Верховного Суда Российской Федерации прямо указывает, что преступления против жизни и здоровья, совершённые по мотивам политической, идеологической, расовой, национальной или религиозной ненависти либо вражды, необходимо отграничивать от преступлений, совершённых на почве личных неприязненных отношений; для этого следует учитывать длительность межличностных отношений подсудимого с потерпевшим, наличие конфликтов, не связанных с указанными мотивами[3]. Полученные на стадии проверки сообщения материалы должны содержать сведения, исключающие, например, бытовую версию конфликта, прежде чем дело будет возбуждено по признакам экстремистского состава.

Типичными поводами для возбуждения уголовных дел данной категории служат сообщения органов ФСБ России и МВД России. При этом для дел о

---

[1] В России удвоилось число причастных к терроризму и экстремизму подростков // Информационное агентство России ТАСС. 30.06.2026. URL: https://tass.ru/proisshestviya/27872615/ (дата обращения: 07.08.2026).

[2] Интервью Председателя СК России «Российской газете» // Следственный комитет Российской Федерации. 15.01.2025. URL: https://sledcom.ru/press/interview/item/1944953/ (дата обращения: 07.08.2026).

[3] Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (в ред. постановления Пленума Верховного Суда РФ от 23 декабря 2025 г. № 43) // Официальный сайт Верховного Суда Российской Федерации. URL: https://www.vsrf.ru/files/13652/ (дата обращения: 07.08.2026).

преступлениях, совершённых с использованием информационно-телекоммуникационных сетей, повышенное значение приобретает получение доказательств, связанных с использованием интернет-ресурсов, поскольку содержание страницы пользователя может быть удалено самим пользователем либо администрацией ресурса еще до момента возбуждения дела.

Отдельную процессуальную проблему составляет определение подследственности. В соответствии с пунктом 1 части 2 статьи 151 УПК РФ предварительное следствие по делам о преступлениях, предусмотренных, в частности, статьями 282¹ и 282² УК РФ, отнесено к компетенции следователей Следственного комитета Российской Федерации, тогда как отдельные смежные составы могут расследоваться также следователями органов внутренних дел, что порождает на практике необходимость своевременного разрешения споров о подследственности, особенно в случаях, когда в ходе проверки выявляются признаки создания либо участия в деятельности экстремистского сообщества, требующие передачи материалов в Следственный комитет Российской Федерации.

Особого внимание следует уделять выявлению признаков составов, предусмотренных статьями 282¹ и 282² УК РФ. На целесообразность расширения оснований для проведения проверок указывал Председатель Следственного комитета Российской Федерации А.И. Бастрыкин: «Представляется целесообразным силами надзирающих и контролирующих органов организовать широкомасштабную и детальную проверку соответствия федеральному законодательству деятельности всех религиозных, национально-культурных и молодежных организаций, в отношении которых есть основания полагать, что они занимаются запрещенной экстремистской деятельностью»[1]. Данная позиция демонстрирует стремление к упреждающему выявлению признаков составов, связанных с проявлением экстремизма, ещё на этапе, предшествующем поступлению конкретного сообщения о преступлении.

Определение достаточности доказательств для привлечения лица в качестве обвиняемого. Пределы определения достаточности доказательств, установленные частью 1 статьи 171 УПК РФ, требуют наличия достаточных доказательств, дающих основания для обвинения лица в совершении преступления. По делам экстремистской направленности данный порог формируется совокупностью объективных и субъективных признаков, установление которых на досудебной стадии сопряжено с существенными методическими трудностями, обусловленными спецификой доказывания цели и мотива, а не только факта совершения действия.

Верховный Суд Российской Федерации разъяснил, что при определении умысла на возбуждение ненависти либо вражды суд, а значит, и следователь при оценке достаточности доказательств, должен учитывать совокупность обстоятельств: обращения к группе людей в общественных местах, на собраниях,

[1] Глава СК считает нужным провести в РФ проверку религиозных организаций // РИА Новости. 18.04.2016. URL: https://ria.ru/20160418/1413852617.html (дата обращения: 07.08.2026).

митингах, демонстрациях, распространение листовок, вывешивание плакатов, размещение обращения в информационно-телекоммуникационных сетях общего пользования, включая сеть Интернет, например на сайтах, в блогах или на форумах, распространение обращений путем веерной рассылки электронных сообщений и т. п. Указанный перечень признаков образует основу для формирования доказательственной базы уже на этапе, предшествующем предъявлению обвинения.

Центральным элементом доказывания по делам о преступлениях, связанных с экстремизмом, выступает судебная лингвистическая, а при необходимости – комплексная (к производству экспертизы могут привлекаться, помимо лингвистов, и специалисты соответствующей области знаний (психологи, историки, религиоведы, антропологи, философы, политологи и др.) экспертиза, назначаемая для определения целевой направленности информационных материалов. При этом Пленум Верховного Суда Российской Федерации прямо указывает, что перед экспертом не могут быть поставлены не входящие в его компетенцию правовые вопросы, в частности вопросы о том, содержатся ли в тексте призывы к экстремистской деятельности либо направлены ли информационные материалы на возбуждение ненависти или вражды, поскольку разрешение таких вопросов относится к исключительной компетенции суда.

Данное ограничение детально исследовано В.В. Бычковым, который отмечает, что «Верховным Судом РФ разъяснено, что в необходимых случаях для определения целевой направленности информационных материалов может быть назначено производство лингвистической экспертизы», и обосновывает необходимость привлечения к производству комплексных экспертиз специалистов смежных областей знания при расследовании преступлений, совершаемых с использованием сети «Интернет»[1]. Указанная позиция сохраняет практическую значимость: неверная идентификация экспертной специализации по делам о киберэкстремизме нередко становится источником юридических ошибок уже на стадии предъявления обвинения.

В совместной работе В.В. Бычкова и В.А. Прорвича обоснована необходимость дифференцирования признаков составов преступлений, связанных с высокотехнологичным экстремизмом, поскольку, как указывают авторы, нередко из-за неверной идентификации состава конкретного преступления рассматриваемого вида возникают юридические ошибки[2]; авторами предложена система алгоритмов информационного обеспечения следственных действий, реализуемая в рамках интерактивной экспертной

[1] Бычков В.В. К вопросу о назначении комплексных лингвистических экспертиз при расследовании киберэкстремизма // Актуальные вопросы профилактики и расследования преступлений экстремистской и террористической направленности: материалы межд. науч.-практ. конф. М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 31-36.

[2] Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершённых с использованием сети Интернет // Российский журнал правовых исследований. 2021. Т. 8. № 1. С. 89-96.

системы, позволяющей следователю получать поддержку в режиме реального времени при оценке достаточности собранных доказательств.

Существенной особенностью установления достаточности доказательств по составам с административной преюдицией (статья 280[1], пункт «а» части 1 статьи 282, статья 282[4] УК РФ) является необходимость проверки не только признаков самого деяния, но и факта предшествующего привлечения лица к административной ответственности по статьям 20.3, 20.3[1] либо частям 1 или 2 статьи 20.3[2] КоАП РФ. В редакции постановления Пленума Верховного Суда Российской Федерации от 23 декабря 2025 г. № 43 прямо указано на необходимость проверки того, вступило ли в законную силу постановление о назначении административного наказания на момент совершения повторного деяния, исполнено ли оно и не истёк ли годичный срок со дня окончания его исполнения либо со дня уплаты административного штрафа, а при наличии обстоятельств, препятствующих постановлению приговора, – возвращения уголовного дела прокурору либо, на досудебной стадии, отказа от предъявления обвинения до устранения соответствующего препятствия.

Изложенное позволяет сформулировать авторский вывод: применительно к составам с административной преюдицией основание для привлечения лица в качестве обвиняемого приобретает двухэлементную структуру, включающую, во-первых, доказательства самого деяния и специального мотива, во-вторых – самостоятельный блок доказательств административно-правового характера (факт, вступление в силу и неистечение срока действия административного наказания). Отсутствие любого из указанных элементов исключает не только обвинение, но и саму возможность вынесения законного постановления о возбуждении уголовного дела по данному основанию.

Позиции высших судебных инстанций. Конституционный Суд Российской Федерации неоднократно рассматривал жалобы на неопределённость статьи 282 УК РФ и последовательно отказывал в их принятии к рассмотрению. В Определении от 22 апреля 2010 г. № 564-О-О по жалобе Р.В. Замураева Конституционный Суд Российской Федерации указал, что данная норма направлена на охрану общественных отношений, гарантирующих признание и уважение достоинства личности ... и устанавливает уголовную ответственность не за любые действия, а только за те, которые совершаются с прямым умыслом, направленным на возбуждение ненависти или вражды, унижение достоинства человека или группы лиц, в связи с чем неопределённости не содержит[1].

[1] Определение Конституционного Суда Российской Федерации от 22 апреля 2010 г. № 564-О «Об отказе в принятии к рассмотрению жалобы гражданина Замураева Романа Владимировича на нарушение его конституционных прав положением части первой статьи 282 УК РФ» // СПС КонсультантПлюс (дата обращения: 07.08.2026).

Данная позиция была подтверждена в определениях по жалобам А.Б. Носика[1] и А.А. Поткина[2], в которых Конституционный Суд Российской Федерации со ссылкой на постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 подчеркнул, что критика политических организаций, идеологических и религиозных объединений, а также политических, идеологических или религиозных убеждений сама по себе не должна рассматриваться как действие, направленное на возбуждение ненависти либо вражды, что процессуально означает недопустимость возбуждения уголовного дела исключительно на основании факта высказывания критических суждений без установления цели возбуждения ненависти или вражды.

В более поздней практике Конституционный Суд Российской Федерации подтвердил общий процессуальный принцип, согласно которому суд обязан, «рассмотрев уголовное дело по существу и оценив все собранные доказательства и доводы сторон, вынести законное, обоснованное» решение[3], что применительно к делам экстремистской направленности означает недопустимость формального подхода к оценке достаточности доказательств на любой стадии производства, включая досудебную.

Верховный Суд Российской Федерации в редакции постановления Пленума от 23 декабря 2025 г. № 43 закрепил важное процессуальное правило: фактические обстоятельства, послужившие основанием для привлечения лица к административной ответственности, сами по себе не предопределяют выводы о виновности в совершении соответствующего преступления, поскольку такая виновность устанавливается судом в предусмотренных уголовно-процессуальным законом процедурах на основе всей совокупности доказательств, включая не исследованные при рассмотрении дела об административном правонарушении[4]. Данное разъяснение прямо ограничивает возможность автоматического переноса административно-правовой оценки на

---

[1] Определение Конституционного Суда РФ от 27.06.2017 № 1411-О «Об отказе в принятии к рассмотрению жалобы гражданина Носика Антона Борисовича на нарушение его конституционных прав статьей 282 УК РФ» // СПС КонсультантПлюс (дата обращения: 07.08.2026).

[2] Определение Конституционного Суда РФ от 18.07.2017 № 1502-О «Об отказе в принятии к рассмотрению жалобы гражданина Поткина Александра Анатольевича на нарушение его конституционных прав статьей 282 УК РФ» // СПС КонсультантПлюс (дата обращения: 07.08.2026).

3 Определение Конституционного Суда РФ от 27.11.2025 « 3192-О «Об отказе в принятии к рассмотрению жалобы гражданина Бахарчиева Магомеда Сайдамиевича на нарушение его конституционных прав пунктом "в" части первой статьи 104.1 и пунктом "а" части четвертой статьи 162 УК РФ, частью первой статьи 18 и пунктом 3 части второй статьи 38 Уголовно-процессуального кодекса Российской Федерации» // СПС КонсультантПлюс (дата обращения: 07.08.2026).

4 Постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» (в ред. постановления Пленума Верховного Суда РФ от 23 декабря 2025 г. № 43) // Официальный сайт Верховного Суда Российской Федерации. URL: https://www.vsrf.ru/ (дата обращения: 07.08.2026).

уголовно-процессуальную стадию, требуя самостоятельного собирания доказательств следователем.

Кроме того, Пленум указал, что решение о рассмотрении уголовного дела о преступлении, предусмотренном статьёй 280^1, пунктом «а» части 1 статьи 282 или статьёй 282^4 УК РФ, в особом порядке судебного разбирательства принимается только при условии, что обвинение, с которым согласился обвиняемый, является обоснованным и подтверждается собранными по делу доказательствами (часть 7 статьи 316 УПК РФ), что исключает возможность упрощённого прохождения такого дела через суд без надлежащей проверки достаточности доказательств, собранных на стадии предварительного следствия.

Важнейшим инструментом повышения качества следствия и сокращения сроков расследования преступлений является непрерывное совершенствование криминалистического и экспертного обеспечения. Применительно к процессуальной проблематике данное утверждение означает, что достаточность доказательств по делам экстремистской направленности напрямую зависит от качества и своевременности назначения судебных экспертиз.

Проведённый анализ разъяснений Верховного и Конституционного судов Российской Федерации, а также доктринальных позиций позволяет сформулировать следующие выводы. Экстремизм представляет собой серьезный вызов для всего мирового сообщества. Борьба с этими проявлениями является одним из важнейших направлений правоохранительных органов. Основание возбуждения уголовного дела о преступлении экстремистской направленности имеет усложнённую структуру по сравнению с общим стандартом части 2 статьи 140 УПК РФ: наряду с данными о деянии оно должно включать сведения, позволяющие с достаточной степенью вероятности установить специальный мотив либо цель, а по составам с административной преюдицией – дополнительно самостоятельный блок доказательств административно-правового характера. Отсутствие любого из данных элементов исключает законность возбуждения уголовного дела. Определение достаточности доказательств для привлечения лица в качестве обвиняемого по данной категории дел также обусловлено указанными особенностями.

Список источников

1. Бычков В.В. К вопросу о назначении комплексных лингвистических экспертиз при расследовании киберэкстремизма // Актуальные вопросы профилактики и расследования преступлений экстремистской и террористической направленности: материалы межд. науч.-практ. конф. М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 31-36.
2. Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершённых с использованием сети Интернет // Российский журнал правовых исследований. 2021. Т. 8. № 1. С. 89-96.

3. В России удвоилось число причастных к терроризму и экстремизму подростков // Информационное агентство России ТАСС. 30.06.2026. URL: https://tass.ru/proisshestviya/27872615/ (дата обращения: 07.08.2026).
4. Глава СК считает нужным провести в РФ проверку религиозных организаций // РИА Новости. 18.04.2016. URL: https://ria.ru/20160418/1413852617.html (дата обращения: 07.08.2026).
5. Интервью Председателя СК России «Российской газете» // Следственный комитет Российской Федерации. 15.01.2025. URL: https://sledcom.ru/press/interview/item/1944953/ (дата обращения: 07.08.2026).

И.Н. Правкина[1],
С.Р. Фурсова[2]

ПРАВОВЫЕ МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ ВИКТИМИЗАЦИИ МОЛОДЕЖИ В ЦИФРОВОЙ СРЕДЕ

Аннотация. В статье с позиций виктимологического подхода анализируется проблема цифровой виктимизации несовершеннолетних. Раскрываются детерминанты вовлечения молодежи в деструктивную, экстремистскую и террористическую деятельность посредством сети Интернет, оценивается уровень виктимности, предлагаются правовые, социальные и образовательные меры противодействия угрозам в информационно-телекоммуникационных сетях.

Ключевые слова: цифровая виктимизация, виктимологическое противодействие, несовершеннолетние, правовое воспитание, экстремизм, информационно-телекоммуникационные сети.

Информационно-телекоммуникационные технологии выступают неотъемлемым элементом функционирования современного общества, основной тенденцией развития которого является формирование нового поколения пользователей, активно взаимодействующих с виртуальным пространством на ранних этапах социализации. В связи с чем нельзя не согласиться с очевидным высказыванием А.В. Майорова, который отмечает, что развитие новых технологий в различных областях жизнедеятельности человека создает благоприятные условия в социальной сфере, неся определенные угрозы для уязвимых слоев населения[3]. Очевидно, что в современных условиях глобальная сеть трансформирует массовое правосознание, выступая мощным катализатором изменения ценностно-правовых ориентаций. И.Н. Правкина и И.В. Правкин подчеркивают, что особенности влияния информационно-

[1] Правкина Ирина Николаевна – доцент кафедры правовых дисциплин Московского экономического института, кандидат юридических наук, доцент.
[2] Фурсова Софья Равилевна – курсант 5 курса факультета подготовки следователей Московской академии Следственного комитета имени А.Я. Сухарева.
[3] Майоров А.В. Виктимологическое противодействие цифровой виктимизации несовершеннолетних, вовлекаемых в экстремистскую и террористическую деятельность / А.В. Майоров // Виктимология. – 2025. – Т. 12, № 3. – С. 363-374.

телекоммуникационных технологий определяются социально-политическим контекстом[1].

Повсеместное внедрение цифровых решений влечет возникновение технологических рисков. Уязвимой категорией признаются лица, не достигшие 18 лет. Несформированная психика, ограниченный объем знаний основ информационной безопасности обуславливают высокий риск превращения подростка в жертву преступного посягательства. Виктимизация представляет собой процесс трансформации лица в жертву преступления, формирующийся вследствие воздействия множества детерминант.

Цифровая среда модифицирует классические способы вовлечения молодежи в антиобщественную деятельность. Анонимизация субъектов, дистанционный характер взаимодействия, использование технологий шифрования минимизируют издержки криминальных структур. Несовершеннолетние испытывают острую потребность в признании, независимости, самореализации. Виртуальный мир предоставляет мнимое ощущение безопасности, компенсируя дефицит коммуникации в реальности.

К.С. Тарабрина отмечает, что подростки часто добровольно транслируют личные данные, фотоматериалы, видеозаписи, не осознавая возможных негативных последствий[2]. Р.А. Субботина указывает, что психологические особенности юношеского возраста служат самостоятельной причиной роста виктимного поведения[3].

Использование информационно-телекоммуникационных сетей позволяет организаторам радикальных сообществ мгновенно распространять деструктивный контент. Вербовка осуществляется посредством создания дискуссионных площадок, тематических форумов, закрытых чатов. Молодежь легко поддается манипулированию. Статистика подтверждает возрастание интенсивности криминальных процессов. За 7 месяцев 2025 года выявлено 722 преступления, связанных с вовлечением несовершеннолетних в антиобщественную деятельность. Количество преступлений экстремистской направленности увеличилось на 30 % в 2024 году[4].

Противодействие обозначенным негативным тенденциям требует выработки комплексной системы защитных механизмов. Основополагающим вектором

---

[1] Правкина И.Н. Влияние информационно-телекоммуникационных технологий на правосознание современного общества / И.Н. Правкина, И.В. Правкин // История государства и права. – 2020. – № 10. – С. 77-80.

[2] Тарабрина К.С. Виктимное поведение несовершеннолетних в цифровом пространстве / К.С. Тарабрина // Уголовная политика России на современном этапе: состояние, тенденции, перспективы: Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г.А. Аванесова. В 2-х частях, Москва, 27 сентября 2024 года. – Москва: Академия управления МВД России, 2024. – С. 291-297.

[3] Субботина Р.А. Психологические особенности проявления виктимного поведения в юношеском возрасте / Р. А. Субботина // Путь науки. – 2015. – № 5(15). – С. 118-123.

[4] Майоров А.В. Виктимологическое противодействие цифровой виктимизации несовершеннолетних, вовлекаемых в экстремистскую и террористическую деятельность / А.В. Майоров // Виктимология. – 2025. – Т. 12, № 3. – С. 363-374.

выступает совершенствование нормативной базы. Государственная политика ориентирована на обеспечение защиты детей от информации, причиняющей вред здоровью, нравственному развитию. Базовые правовые механизмы защиты регламентированы положениями Федеральных законов от 24 июня 1999 года № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»[1] и от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[2], устанавливающими жесткую обязанность применения технических средств ограничения доступа к деструктивной информации.

Внесенные изменения в уголовное законодательство предусматривают ужесточение ответственности за вовлечение несовершеннолетних в совершение общественно опасных деяний посредством «Всемирной паутины». Федеральным законом от 28 декабря 2024 года № 514-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[3] скорректированы диспозиции статей 150 и 151 Уголовного кодекса Российской Федерации. Введены новые квалифицирующие признаки: совершение деяния с использованием информационно-телекоммуникационных сетей, вовлечение 2 и более лиц, а также лиц младше 14 лет. Срок лишения свободы за вовлечение в преступную группу достигает 10 лет. Регламентированы санкции за умышленный поиск заведомо экстремистских материалов, доступ к заблокированным ресурсам посредством специализированных программно-аппаратных средств.

Кроме того, с 1 сентября 2025 года нормативно закреплено наложение административных штрафов за применение технологий шифрования трафика и VPN-сервисов для получения доступа к базам данных, включенным в федеральный список экстремистских материалов. А.Ю. Гарашко, Д.С. Давидов и С.В. Зыкова резюмируют, что нормативно-правовой массив нуждается в постоянной адаптации к меняющимся технологическим реалиям цифровизации[4].

Предупреждение цифровой виктимизации основывается на превентивном воздействии. Система виктимологического противодействия включает 3 уровня: общесоциальный, специально-криминологический, индивидуальный. Общесоциальный уровень предполагает реализацию государственных программ, направленных на повышение информационной грамотности населения. Важным элементом выступает правовое воспитание,

---

[1] Федеральный закон от 24 июня 1999 г. N 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» // Гарант URL: https://base.garant.ru/12116087/?ysclid=ms282ayks771446144 (дата обращения: 26.07.2026).

[2] Федеральный закон от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // Гарант URL: https://base.garant.ru/12181695/?ysclid=ms283uuqgp343148323 (дата обращения: 26.07.2026).

[3] Федеральный закон от 28 декабря 2024 года № 514-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Гарант URL: https://base.garant.ru/411232417/?ysclid=ms28576ept225607030 (дата обращения: 26.07.2026).

[4] Теоретико-правовые проблемы информатизации (цифровизации) нормотворческой и правоприменительной деятельности органов внутренних дел / А.Ю. Гарашко, Д.С. Давидов, С.В. Зыкова [и др.]. – Москва: Издательский дом «Граница», 2023. – С. 35.

рассматриваемое как целенаправленная деятельность по трансляции юридического опыта, формированию позитивных установок.

Так, И.Н. Правкина и И.В. Правкин констатируют, что правовое воспитание является сложной, полисубъектной деятельностью, играющей значимую роль в формировании правового сознания и правовой культуры современного общества[1]. Цель правовоспитательного процесса заключается в укреплении ценностных ориентаций, стимулировании правовой активности, поддержании правопорядка. Эффективность просветительской работы детерминирована различными факторами. Значимую роль играют объективные условия, специфика политического режима, исторически сложившиеся ценности.

Субъективный аспект включает внутреннюю потребность индивида в самовоспитании, повышении уровня правовой культуры. Организация правового воспитания подчиняется ряду принципов. Принцип координации требует объединения усилий государственных институтов и структур гражданского общества; принцип историчности указывает на обусловленность содержания просветительской работы текущим этапом социокультурного развития; принцип полиморфизма допускает реализацию защитных механизмов в разнообразных формах общественной жизни.

Необходимо отметить, что внедрение информационных технологий в образовательный процесс открывает новые возможности. Рекомендуется создание специализированных онлайн-площадок, интерактивных платформ, предоставляющих достоверную юридическую информацию. Виртуальные ресурсы способны формировать навыки безопасного поведения, развивать критическое мышление. Виктимогенные факторы носят многоаспектный характер. Семейное неблагополучие, отсутствие контроля со стороны законных представителей многократно усиливают вероятность вовлечения подростка в «криминальные схемы».

Родительский контроль призван включать жесткое ограничение времени пребывания в сети, использование программного обеспечения для фильтрации контента. Финансовые трудности побуждают несовершеннолетних искать нелегальный доход, включая продажу приватных фотографий. Проблемы в реальном общении действуют аналогично – школьники, отвергнутые классом, пытаются найти поддержку в сетевых группах.

Возникшей уязвимостью пользуются преступники, применяющие методы психологической манипуляции для сближения с жертвой. Травля в сети, домогательства и склонение к суициду наносят вред психическому и физическому здоровью детей.

Практика показывает, что после первого инцидента риск повторных посягательств заметно возрастает. Злоумышленники координируют действия в закрытых чатах, обмениваются контактами потенциальных жертв и методиками совращения. Безопасность напрямую зависит от цифровой грамотности

[1] Правкина И.Н. Правовое воспитание в современном обществе / И.Н. Правкина, И.В. Правкин // Вестник Саратовской государственной юридической академии. – 2023. – № 5(154). – С. 188-194.

пользователя. Однако законодательная база зачастую отстает от темпов развития технологий, в то время как подростки мгновенно перенимают сетевые формы поведения.

Отсутствие контроля за потребляемым контентом и слабое критическое мышление упрощают задачу вербовщикам. Правонарушители детально изучают страницы в социальных сетях, вычисляя страхи и потребности подростка. Общение выстраивается от дружеской поддержки к внушению чувства исключительности. Целью манипуляций является изолирование ребенка от влияния семьи и учителей. Оказавшись в информационном вакууме, подросток принимает радикальные взгляды и соглашается на противоправные действия. В связи с этим, снизить риски возможно посредством контроля социальных платформ и интернет-провайдеров.

В рамках Федерального закона от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности»[1] закреплен механизм оперативной внесудебной блокировки сайтов, пропагандирующих экстремистскую деятельность. Уполномоченные ведомства наделены компетенцией по немедленному ограничению доступа к выявленным деструктивным сообществам.

На сегодняшний день, одним из актуальных остается требование в автоматизированном мониторинге сети, оперативной блокировке опасных ресурсов и устранении анонимности нарушителей. Подросткам, в свою очередь, необходимо обучение цифровой гигиене с целью формирования безопасного интернет-контента[2]. Защита молодежи от дестабилизирующей сетевой среды обеспечивается комплексным взаимодействием семьи, общества и государства. Доверительные отношения, родительский контроль и фильтрация интернет-контента снижают риски вовлечения несовершеннолетних в противозаконную деятельность. Указанной цели также способствует выявление радикальных сообществ волонтерами.

Эффективная профилактика требует перманентной адаптации правовой базы к технологиям, адресной деятельности с группами риска, обеспечения доступного образования и досуга. Высокая тревожность подавляет критическое мышление, поэтому необходим школьный психологический скрининг и обучение подростков саморегуляции.

Таким образом, противодействие цифровым угрозам выступает приоритетом национальной безопасности, объединяющим обновление законодательства, правовое просвещение, развитие цифровой грамотности и системную психологическую поддержку.

---

[1] Федеральный закон от 25 июля 2002 г. N 114-ФЗ «О противодействии экстремистской деятельности» // Гарант URL: https://base.garant.ru/411232417/?ysclid=ms28576ept225607030 (дата обращения: 26.07.2026).

[2] Теоретико-правовые проблемы информатизации (цифровизации) нормотворческой и правоприменительной деятельности органов внутренних дел / А.Ю. Гарашко, Д.С. Давидов, С.В. Зыкова [и др.]. – Москва: Издательский дом «Граница», 2023. – 92 с.

Список источников:

1. Майоров А.В. Виктимологическое противодействие цифровой виктимизации несовершеннолетних, вовлекаемых в экстремистскую и террористическую деятельность / А.В. Майоров // Виктимология. – 2025. – Т. 12, № 3. – С. 363-374.
2. Правкина И.Н. Влияние информационно-телекоммуникационных технологий на правосознание современного общества / И.Н. Правкина, И.В. Правкин // История государства и права. – 2020. – № 10. – С. 77-80.
3. Правкина И.Н. Правовое воспитание в современном обществе / И.Н. Правкина, И.В. Правкин // Вестник Саратовской государственной юридической академии. – 2023. – № 5(154). – С. 188-194.
4. Субботина Р.А. Психологические особенности проявления виктимного поведения в юношеском возрасте / Р.А. Субботина // Путь науки. – 2015. – № 5(15). – С. 118-123.
5. Тарабрина К.С. Виктимное поведение несовершеннолетних в цифровом пространстве / К.С. Тарабрина // Уголовная политика России на современном этапе: состояние, тенденции, перспективы: Сборник научных трудов по материалам международной научно-практической конференции, посвященной 90-летию со дня рождения профессора Г.А. Аванесова. В 2-х частях, Москва, 27 сентября 2024 года. – Москва: Академия управления МВД России, 2024. – С. 291-297.
6. Теоретико-правовые проблемы информатизации (цифровизации) нормотворческой и правоприменительной деятельности органов внутренних дел / А.Ю. Гарашко, Д.С. Давидов, С.В. Зыкова [и др.]. – Москва: Издательский дом «Граница», 2023. – 92 с.

В.А. Прорвич[1]

ДОКТРИНАЛЬНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ ГОСУДАРСТВЕННОЙ ПРОГРАММЫ БОРЬБЫ С КИБЕРЭКСТРЕМИЗМОМ В МОЛОДЕЖНОЙ СРЕДЕ

1. Побудительные мотивы к разворачиванию научных исследований и разработок по борьбе с киберэкстремизмом в Московской академии Следственного комитета России.

Результаты анализа содержательных особенностей нормативных актов концептуально-стратегического и доктринального уровня, раскрывающих особенности обеспечения национальной безопасности России, показывают, что среди основных направлений уголовно-правовой политики государства большое

[1] Прорвич Владимир Антонович – профессор-исследователь Департамента уголовного права, процесса и криминалистики Национального исследовательского университета «Высшая школа экономики», доктор юридических наук, доктор технических наук, профессор, Почетный профессор Московской академии Следственного комитета имени А.Я. Сухарева.

внимание уделяется борьбе с проявлениями экстремизма и терроризма. Уже в Стратегии национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента РФ от 12 мая 2009 г. № 537, констатировалось усиление противоборства в глобальном информационном пространстве, стремление некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории. Соответственно, среди главных направлений обеспечения государственной и общественной безопасности было указано на усиление роли государства в качестве гаранта безопасности личности и прав собственности, совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма.

Обеспечение государственной и общественной безопасности осуществляется путем повышения эффективности деятельности правоохранительных органов и специальных служб, органов государственного контроля (надзора), совершенствования единой государственной системы профилактики преступности, в первую очередь среди несовершеннолетних, и иных правонарушений (включая мониторинг и оценку эффективности правоприменительной практики), разработки и использования специальных мер, направленных на снижение уровня криминализации общественных отношений.

К факторам, влияющими на национальную безопасность в области науки и образования, были отнесены, в том числе, и повышение роли школы в воспитании молодежи как ответственных граждан России на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, а также в профилактике экстремизма и радикальной идеологии.

Среди главных направлений государственной политики в сфере обеспечения государственной и общественной безопасности на долгосрочную перспективу были выделены усиление роли государства в качестве гаранта безопасности личности, прежде всего детей и подростков, совершенствование нормативного правового регулирования предупреждения и борьбы с преступностью, коррупцией, терроризмом и экстремизмом. Для этого была признана необходимость повышения эффективности деятельности правоохранительных органов и спецслужб, создания единой государственной системы профилактики преступности (в первую очередь среди несовершеннолетних) и иных правонарушений, включая мониторинг и оценку эффективности правоприменительной практики, разработки и использования мер, направленных на противодействие глобальным вызовам, включая международный и национальный терроризм, политический и религиозный экстремизм, национализм и этнический сепаратизм, предупреждение социальных и межнациональных конфликтов.

Перечисленные выше установки государственной политики были восприняты руководителями Московской академии Следственного комитета России А.М. Багметом и В.В. Бычковым с момента ее создания, как одно из важнейших направлений научных исследований и разработок. Благодаря их энтузиазму, к этим научным исследования подключились многочисленные коллеги, также занимающиеся обучением и воспитанием молодежи, будущих сотрудников

правоохранительных органов, которым предстоит обеспечить выполнение указанных выше установок государства.

В течение нескольких лет было обозначено несколько основных направлений исследований по перечисленной выше тематике, а также по ряду смежных направлений. При этом речь идет не только непосредственно об исследованиях, обобщающих уже существующий опыт выявления, раскрытия и расследования преступлений в сфере экстремизма и терроризма. Законодатель предусмотрел ряд признаков экстремистских проявлений в уголовно-правовых нормах по нескольким десяткам преступлений различного вида, что потребовало организации исследований для поиска критериев, позволяющих создать научно обоснованную систему их классификации.

Это привело и к необходимости выявления также тех новых проблем, которые возникают при методическом и инструментальном обеспечении оперативно-розыскных мероприятий для выявления и фиксации следов таких преступлений. Кроме того, ряд новых научных направлений был направлен на выявление и поиск решений ряда проблем, начиная от получения достаточных данных для возбуждения уголовных дел о преступлениях, связанных с различными проявлениями экстремизма и терроризма, и до надлежащего формирования предмета доказывания и установления пределов доказывания по соответствующим уголовным делам.

Большое внимание уделялось и сбору самого разнообразного эмпирического материала, связанного с преступлениями рассматриваемого вида, включая не только изучение особенностей уголовных дел, завершенных расследованием и рассмотренных судами, но и многочисленные опросы не только следователей, но и различных групп представителей той молодежной среды, на которую и нацеливались организаторы экстремистских преступлений различного вида. Здесь необходимо отметить ту колоссальную организационную работу, которую провел В.В. Бычков, а также неоценимую помощь в организации опросов представителей МВД России, которую оказал профессор А.Ф. Волынский.

2. Расширение направлений исследований и разработок, прямо или косвенно связанных с выполнением государственных задач по борьбе с различными проявлениями экстремизма и терроризма.

В Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 31 декабря 2015 г. № 683, среди угроз государственной и общественной безопасности особое внимание также было обращено на деятельность террористических и экстремистских организаций, направленную на насильственное изменение конституционного строя, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, деятельность радикальных общественных объединений, использующих националистическую и религиозно-экстремистскую идеологию, иностранных и международных неправительственных организаций, финансовых и экономических структур, а также частных лиц, направленная на нарушение единства и территориальной целостности Российской Федерации, дестабилизацию внутриполитической и социальной ситуации в стране,

включая инспирирование «цветных революций», разрушение традиционных российских духовно-нравственных ценностей; деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе.

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, актуализация которой планируется в ближайшее время с учетом новых вызовов и угроз, отмечается что возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Таким образом, в рамках государственной уголовно-правовой политики был обозначен рад новых направлений, связанных с активизацией деятельностью западных спецслужб, в том числе, в информационном пространстве компьютерных сетей. При этом для экстремистских преступлений стал активно использоваться Интернет. К главным направлениям обеспечения государственной и общественной безопасности были отнесены совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции,

терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями, развитие взаимодействия органов обеспечения государственной безопасности и правопорядка с гражданским обществом, повышение доверия граждан к правоохранительной и судебной системам. В том же 2016 г. законодателем был внесен ряд дополнений в Уголовный кодекс РФ по результатам криминализации новых видов экстремистских преступлений, а в 2019 г. в ч. 1 и 2 ст. 282 УК РФ были введены дополнения, раскрывающее особенности совершения экстремистских преступлений с использованием сети Интернет.

В этот период был завершен комплекс наших многолетних совместных исследований по интегрированному применению инструментария всех наук уголовно-правового блока – уголовного права, уголовно-процессуального права, криминалистики, судебной экспертизы и оперативно-розыскной деятельности, следователями по преступлениям в сфере экономики. Их главной особенностью являлось преодоление давно сложившихся проявлений «научного сепаратизма» в системе наук уголовно-правового блока и поиск возможностей для консолидации ученых и специалистов в различных сферах наук уголовно-правового, экономического и информационного блоков в борьбе с современной преступностью – как на доктринальном уровне, так и в практической работе. В них кроме ряда ученых и специалистов Московской академии Следственного комитета РФ во главе с А.Н. Багметом и В.В. Бычковым, приняли участие ведущие ученые из МВД РФ, Генеральной прокуратуры РФ, экспертных организаций.

В результате были изданы под общей редакцией А.И. Бастрыкина два монографических учебных пособия: в 2016 году «Организация и методика расследования отдельных видов экономических преступлений»[1] объемом 80 печатных листов, и в 2018 году «Ошибки при раскрытии и расследовании экономических преступлений»[2] объемом 60 печатных листов. По отзывам многих наших коллег они стали настольной книгой многих следователей, а ряд ученых и специалистов после этого также занялись выявлением и систематизацией следственных ошибок, установлением их причин и совершенствованием соответствующих программ повышения квалификации.

В рамках данных комплексных исследований были разработаны алгоритмы применения в параллельно-последовательном режиме всех имеющихся в распоряжении следователя методик и инструментария, разработанных в рамках всех наук уголовно-правового блока. Базовый вариант этих юридических алгоритмов носил универсальный характер, обеспечивающий возможности для формирования на его основе юридических алгоритмов, сориентированных на формирование комплекса методик и инструментария, предназначенного для выявления, раскрытия и расследования любых других видов преступлений.

Поскольку в указанных выше нормативных правовых актах были поставлены задачи по совершенствованию структуры и деятельности правоохранительных

[1] Организация и методика расследования отдельных видов экономических преступлений: учебно-методическое пособие / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М., Спутник+, 2016.

[2] Ошибки при раскрытии и расследовании экономических преступлений: учебно-методическое пособие / под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М., Спутник+, 2018.

органов, включая выявление, предупреждение и пресечение разведывательной и иной деструктивной деятельности специальных служб и организаций иностранных государств, проявлений религиозного радикализма, национализма, сепаратизма, иных форм экстремизма, организованной преступности и иных преступных посягательств на конституционный строй Российской Федерации, права и свободы человека и гражданина, В.В. Бычков принял решение сосредоточить свое внимание на проблемах, решение которых необходимо для оперативного выявления, своевременного раскрытия и надлежащего расследования преступлений экстремистской направленности, совершаемых с использованием Интернета и других информационно-телекоммуникационных технологий

3. Некоторые особенности диссертационных исследований В.В. Бычкова по разработке научных основ государственной программы борьбы с киберэкстремизмом.

Важно обратить внимание на то, что В.В. Бычкову, как представителю руководства Московской академии Следственного комитета РФ, неоднократно давались поручения о подготовке предложений для разработки определенной части государственной программы борьбы с преступлениями в сфере экстремизма, относящейся к сфере компетенции Следственного комитета России. Поэтому ему пришлось глубоко погрузиться в проблемы не только научного характера, но и организационного, связанного с межведомственным взаимодействием правоохранительных органов, включая подготовку необходимых для этого кадров. Тем не менее, даже в условиях высокой занятости проблемами административного и учебно-воспитательного характера, ему удавалось находить возможности для выполнения обширного комплекса научных исследований по проблемам борьбы с преступлениями в сфере экстремизма, совершенными с использованием информационно-телекоммуникационных технологий, включая Интернет.

Следуя уже отмеченным выше особенностям наших научных исследований и разработок, сфокусированных на формирование комплексного методического обеспечения следователей, на основе того инструментария, который был создан в рамках всех наук уголовно-правового блока, в первую очередь были изучены особенности информационно-правовой структуры развернутых уголовно-правовых характеристик конкретных киберпреступлений в сфере экстремизма различного вида. В результате были идентифицированы обязательные и факультативные признаки 57 различных составов этих преступлений. При этом особое внимание было уделено особенностям совокупностей таких преступлений, совершенных с различными формами соучастия их субъектов. Последующий сопоставительный анализ содержательных особенностей различных групп их признаков позволил разработать их восьмиуровневую классификацию[1].

[1]Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография, под ред. В.А. Прорвича. / М.: Альпен-Принт, 2024, 572 с.; Бычков В.В., Прорвич В.А. Киберэкстремизм: понятие, квалификация, расследование: учебное пособие. / М.: Московская академия Следственного комитета России, 2023 г., 330 с.; Бычков В.В., Прорвич В.А. Особенности формирования алгоритмов выявления, раскрытия и расследования «высокотехнологичных» преступлений экстремистского характера, совершенных с использованием сети «Интернет» // Российский журнал правовых исследований. 2021. Том 8.

Что касается раскрытия тех неопределенностей, которые были связаны с особенностями проявления принципа дополнительности при формировании развернутых уголовно-правовых характеристик киберпреступлений различных видов, то было установлено важное значение правил тех информационных систем, которые были использованы для формализации соответствующих правоотношений в искусственно созданном информационном пространстве компьютерных сетей, включая Интернет, субъектов цифровых прав[1]. Более подробно результаты наших исследований в данной сфере докладывались год назад, на первой всероссийской научной конференции памяти В.В. Бычкова.

С учетом ряда доктринальных аспектов формирования составов преступлений рассматриваемого вида, а также особенностей различных групп их объективных и субъективных, обязательных и факультативных признаков, были раскрыты неразрывные связи уголовного и уголовно-процессуального права. Это позволило перейти от общих рассуждений об особенностях формирования юридического фундамента российского уголовного судопроизводства на основе Уголовного кодекса РФ и Уголовно-процессуального кодекса РФ, к разработке единого информационно-технологического инструментария, необходимого для оперативного выявления, своевременного раскрытия и надлежащего расследования преступлений в сфере киберэкстремизма.

Прежде всего, на основе раскрытия содержательных особенностей признаков составов преступлений рассматриваемого вида были разработаны юридические алгоритмы формирования информационно-правовой структуры доказательств, собираемых при расследовании соответствующих уголовных дел. Это позволило сформировать проблемно-ориентированные юридические алгоритмы с матричными классификаторами и двойными системами юридических тождеств для выполнения надлежащей проверки и оценки доказательств, на основе тех юридических информационных технологий, которые были разработаны совместно с профессором А.М. Новиковым[2].

На основе дальнейшей разработки доктринальных аспектов уголовно-правовой защиты современного общества от различных экстремистских проявлений, в том числе с использованием современных информационных технологий, были разработаны новые подходы к формированию криминалистических методик, развивающие научные представления, сформированные Н.П. Яблоковым и А.А. Бессоновым. Это позволило соединить описанное выше описание роли и места доктринального понятия «состав преступления» не только с первой частью криминалистической методики – криминалистической характеристики

№ 1. С. 1-8; Бычков В.В., Прорвич В.А. Алгоритмы выявления признаков экстремистской и террористической деятельности с использованием Интернета на основе информационных шаблонов возможных составов преступлений данного вида // Расследование преступлений: проблемы и пути их решения. 2022. № 2. С. 43-50.

[1] Прорвич В.А. Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы // Российский журнал правовых исследований. – 2023. – Том 10 – № 3. – С. 7-19.

[2] Новиков А.М., Прорвич В.А. Доказательства и доказывание в следственной практике. М.: Московская академия Следственного комитета России, 2022 г.

расследуемого преступления, но и сформировать новые, циклические алгоритмы практического применения всех ее семи частей.

Важно обратить внимание на то, что с помощью данной юридической информационной технологии, основанной на обновленной структуре и циклическом алгоритме практического применения криминалистической методики, сформировать не только информационно полную совокупность доказательств по расследуемому уголовному делу о конкретном киберпреступлении в сфере экстремизма определенного вида. Поскольку обобщение следственной практики показало, что важную роль приобретает выявление совокупностей преступлений рассматриваемого вида, совершенных с различными формами соучастия их субъектов, данная юридическая информационная технология была нацелена не только на выявление признаков наличия не одного, а нескольких преступлений, но и дифференциацию составов каждого из них.

При этом были показаны и новые возможности применения специальных знаний для получения, проверки и оценки доказательств по уголовным делам о преступлениях рассматриваемого вида, а также особенности применения информационных технологий для оперативного выявления и фиксации следов данных преступлений.

Полученные результаты наших многолетних исследований и разработок позволили к 2023 году сформировать научные основе государственной программы борьбы с киберэкстремизмом, а также подготовить к защите докторскую диссертацию В.В. Бычкова по новой специальности 5.1.4 «уголовно-правовые науки». Ее содержание вызвало большой интерес у большинства ученых и преподавателей не только Московской академии Следственного комитета РФ имени А.Я. Сухарева, но и десятков ведущих ученых из других организаций, давших свои положительные отзывы. Кроме того, были получены акты о внедрении ее положений из 100 организаций, начиная с Московского государственного университета имени М.В. Ломоносова, и заканчивая всеми территориальными управлениями СК РФ.

Предварительные защиты докторской диссертации В.В. Бычкова проводились на совместных заседаниях пяти кафедр Академии и вызвали большой интерес; диссертанту были заданы многочисленные вопросы, на которые он дал исчерпывающие ответы. После единогласного голосования ректор утвердил представление диссертации к защите.

Получив полный комплект необходимых документов для защиты своей докторской диссертации, В.В. Бычков фактически провел еще одно, весьма оригинальное исследование в рамках переговоров с руководителями и членами нескольких диссертационных советов. Выяснилось, что к рассмотрению диссертации, подготовленной в строгом соответствии с паспортом специальности 5.1.4 «Уголовно-правовые науки», многие советы оказались не готовы, а ведущие ученые настойчиво рекомендовали исключить из нее главы и параграфы, связанные с результатами исследований уголовно-правовых и уголовно-процессуальных аспектов борьбы с киберэкстремизмом, и даже упоминания о государственной

программе борьбы с киберэкстремизмом, оставив только исследования и разработки в сфере криминалистики.

То есть, те проявления «научного сепаратизма», которые были описаны А.Ф. Волынским за много лет до этого[1], так и не были преодолены. А наши коллективные научные исследования и разработки по созданию интегрированного методического обеспечения и инструментария, сориентированного на решение проблем, возникающих у следователей, начиная с обоснования решения о возбуждении уголовного дела, формирования развернутой уголовно-правовой характеристики конкретного преступления, идентификации признаков состава преступления, и заканчивая методиками проверки и оценки каждого из доказательств, включая установление пределов доказывания на основе критериев достаточности собранной совокупности доказательств, получившие признание и поддержку следователей, признаются далеко не всеми маститыми учеными.

Поэтому В.В. Бычкову пришлось потратить много своих творческих сил и нервной энергии, чтобы в течение полугода изменить целевую установку нашего исследования – убрать из диссертации даже упоминание о разработке научных основ государственной программы борьбы с киберэкстремизмом, значительные фрагменты которой были направлены руководством Академии для включения в соответствующую государственную программу, и переориентировать ее с научно-методического обеспечения всего спектра следственных действий по борьбе с киберэкстремизмом, на интересы консервативных ученых-криминалистов, заседающих в диссертационных советах.

По результатам данного этапа научных исследований мы пришли к выводу о том, что в науках уголовно-правового блока проявления авторитарного характера уже стали приводить к формированию рисков торможения проблемно-ориентированных исследований и разработок, нацеленных на решение задач, поставленных государством перед правоохранительными органами в приведенных выше нормативных правовых актах. И особенно тревожная ситуация сложилась в сфере подготовки кадров высшей квалификации по специальности 5.1.4 «Уголовно-правовые науки».

Но за получение этих выводов В.В. Бычков отдал свою жизнь… Сердце, ослабленное продолжительной борьбой не только с тяжелой болезнью, но и с непониманием государственных задач многими коллегами, отстаивающими свои личные консервативные взгляды, не выдержало такой нагрузки…

4. Особенности формирования разделов государственной программы борьбы с проявлениями киберэкстремизма в молодежной среде.

При формировании научных основ государственной программы борьбы с киберэкстремизмом большое внимание было уделено различным аспектам, связанным с преступными проявлениями данного вида в молодежной среде – наиболее уязвимой части нашего общества.

Прежде всего, были сформулированы задачи по формированию эмпирической базы для проведения дальнейших научных исследований и разработок. По

[1] Волынский А.Ф. Предмет криминалистики и «Научный сепаратизм»: последствия и возможности их преодоления // Труды Академии управления МВД России. 2018. № 1(45). С. 175-185.

специально разработанным анкетам и опросным листам был выполнен анализ уголовных дел, в том числе, незавершенных расследованием, а также завершившихся приговорами судов, с выделением тех из них, субъектами которых были молодые люди различного возраста. При опросе следователей также выделялись проблемы, связанные с вовлечениями в преступную деятельность молодых людей, а также особенности возрастных характеристик потерпевших.

Кроме того, в отличие от других подобных исследований, были разработаны специальные анкеты и опросные листы для опросов самих молодых людей различного возраста, которые проводились в течение нескольких лет с непосредственным участием В.В. Бычкова и его коллег. Среди них были выделены несколько групп школьников и кадетов различного возраста, а также студентов и курсантов. Среди многочисленных вопросов к ним были сформулированы связанные с тем, насколько они информированы о содержании информации экстремистского характера, распространяемой в каждой из сетей, а также через «темный интернет».

Ряд вопросов был связан с осведомленностью молодых людей с содержанием призывов к противоправным действиям экстремистского характера, участию в несанкционированных демонстрациях, распространению в Интернете призывов к незаконным действиям, и т п. Задавались вопросы и о возможном личном участии в таких противоправных действиях экстремистского характера. Всего было опрошено более тысячи респондентов[1].

Анонимный опрос школьников и кадетов, студентов и курсантов показал, что они не только являются активными пользователями Интернета, хорошо понимают смысл понятий, связанных с информацией экстремистского характера, но и подвергались активному воздействию социальных сетей для их вовлечения в незаконные акции протеста и участие в массовых беспорядках[2]. Подавляющее большинство опрошенных хорошо понимали противоправность подобных акций и отказывалось участвовать в них. Правдивость их ответов подтверждается их полной анонимностью, а также тем, что некоторые из них признались, что не только участвовали в незаконных экстремистских мероприятиях, но и совершали противоправные действия.

Во многих анкетах отражались признаки подчеркнутого свободолюбия, что более характерно для молодежи старших возрастов, с определенными проявлениями нигилизма. Нередко высказывалось возмущение, что «взрослые» считают молодёжь глупой, и «её следует как малое дитя вести за ручку и показывать пальцем на что смотреть и что делать». Однако большая часть опрошенных молодых люди соглашались, что их должны учить взрослые, но не подчинять их своей воле и не навязывать свое мнение. Иначе они начнут воспринимать такое «обучение» в негативном ключе и станут активно препятствовать пропаганде всего хорошего и поддерживать всё плохое назло своим «обидчикам».

---

[1] Бычков В.В. Профилактика молодежного киберэкстремизма // Советская и российская криминалистика: традиции и перспективы: материалы Всероссийской научно-практической конференции с международным участием (Москва, 2.02.2023). М., 2023. С. 294-300.

[2] Бычков В.В. Протестные акции как форма проявления экстремизма // Вестник Московской академии Следственного комитета Российской Федерации. 2021. № 4. С. 57-62.

Анкетирование и опросы показали, что по отношению к экстремистской пропаганде наиболее устойчивыми оказались кадеты и курсанты учебных заведений правоохранительных органов и Министерства обороны РФ, а также обучающиеся в кадетских корпусах и академиях Следственного комитета РФ. Это подтверждает, что воспитательная работа в данных образовательных учреждениях находится на должном уровне, отвечая тем установкам, которые даны в Концепции кадетского образования в Российской Федерации[1]. Следственный комитет России осуществляет комплекс мероприятий в сфере кадетского образования, нацеленный не только на качественное образование детей, но и на воспитание патриотически настроенных граждан, готовых к будущей службе Отечеству[2].

В процессе обработки результатов выполненных опросов и анкетирования было обращено внимание на только на особенности отношения молодых людей к попыткам воздействия на них организаторов киберэкстремистских преступлений, в том числе, зарубежных. Многие из кадетов и курсантов высказывались о том, что они готовы не только игнорировать попытки воздействия на их сознание со стороны иноагентов, но и призывать к этому своих товарищей.

Более того, некоторые из них высказывались о необходимости рассмотреть возможность их дополнительного обучения методам выполнения оперативно-розыскных мероприятий под руководством их старших товарищей, по выявлению признаков экстремистских проявлений в среде школьников и студентов. При этом они высказывались о том, что лучше понимают своих сверстников, и школьники, по их мнению, скорее прислушаются к советам своего сверстника-кадета, чем учителя или следователя. Понимая, что у них недостаточно для самостоятельного выполнения оперативно-розыскных мероприятий специальных знаний и профессиональных компетенций, они предлагали создавать оперативные группы кадетов и курсантов под руководством опытных следователей, для работы среди своих «штатских» сверстников.

Эту часть инициатив наших кадетов и курсантов детально разработать для научно-педагогического и организационного обоснования соответствующего доклада руководству В.В. Бычков не успел. Возможно, организаторы настоящей научной конференции не оставят без внимания эту инициативу нашей молодежи и продолжат научные исследования и разработки, чтобы организовать профилактику киберэкстремизма в молодежной среде и борьбу с его проявлениями с активным участием самих молодых людей, проявивших такую инициативу и заявивших, что они лучше понимают своих сверстников. Соответствующие положения требуют специального обсуждения при формировании государственной программы борьбы с киберэкстремизмом в молодежной среде на основе уже сделанного задела в представленных ниже публикациях.

---

[1] https://mccvu.ru/ads/kontseptsiya-kadetskogo-obrazovaniya.

[2] Концепция развития профильного кадетского образования Следственного комитета Российской Федерации на период до 2018 года, утверждена СК России 10.05.2016 // СПС «КонсультантПлюс».

Список источников

1. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография, под ред. В.А. Прорвича. / М.: Альпен-Принт, 2024, 572 с.
2. Бычков В.В., Прорвич В.А. Киберэкстремизм: понятие, квалификация, расследование: учебное пособие. / М.: Московская академия Следственного комитета России, 2023 г.
3. Новиков А.М., Прорвич В.А. Доказательства и доказывание в следственной практике. М.: Московская академия Следственного комитета России, 2022 г.
4. Прорвич В.А. Компьютерное моделирование преступных проявлений в сфере цифровых прав: основные подходы и алгоритмы. / Российский журнал правовых исследований. – 2023. – Том 10 – № 3. – С. 7-19.
5. Прорвич В.А. Научные и организационные основы государственной программы борьбы с киберэкстремизмом: творческое наследие Василия Васильевича Бычкова // Расследование преступлений: проблемы и пути их решения, № 1, 2024, с. 187-198.

А.Ж. Саркисян[1]

СОСТОЯНИЕ ПРЕСТУПНОСТИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В РОССИИ (2024–2026 ГГ.): ДИНАМИКА, СТРУКТУРА И ПРАВОПРИМЕНИТЕЛЬНЫЕ ТЕНДЕНЦИИ

Аннотация. В статье проводится анализ состояния преступности экстремистской направленности в России в 2024–2026 гг. на основе данных МВД, Генпрокуратуры. Показано, что на фоне снижения общей преступности наблюдается устойчивый рост экстремистских и «террористических» деяний, исключительно в цифровой среде. Выявлены основные тенденции правоприменения: расширение квалификации высказываний, рост числа осуждённых по ст. 205.2 и 354.1 УК, удвоение доли несовершеннолетних.

Ключевые слова: экстремизм; терроризм; преступность; статистика; ст. 205,2 УК; ст. 354,1 УК; цифровая среда; радикализация; правоприменение.

Введение

Экстремистская преступность остается одним из приоритетных объектов государственной политики в сфере национальной безопасности в связи с идеологической мотивацией, сетевой организацией и высоким общественным резонансом. В условиях цифровизации коммуникаций и геополитической напряжённости изменяются как формы экстремистской активности, так и подходы к её криминализации и правоприменению.

[1] Саркисян Армен Жораевич – декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

Цель исследования — описать современное состояние преступности экстремистской направленности в России, характерные структурные сдвиги и правоприменительные тенденции в 2024–2026 гг.

Задачи:

- обратить внимание на динамику зарегистрированных преступлений экстремистской и террористической направленности;
- описать сложные навыки и основную практику;
- оценить социальные и возрастные характеристики вовлечённых лиц;
- сформулировать выводы для профилактической и уголовной политики.
-

Динамика преступности экстремистской и террористической направленности

Таблица 1. Зарегистрированные преступления экстремистской и террористической направленности (2024–2026 гг.)

Показатель	2024	2025	Изменение 2025/2024	9 мес. 2024	9 мес. 2025	Изменение 9 мес.	l кв. 2026 (динамика)
Экстремистские преступники	1719	2241	+30,4%	—	1760	+28,1%	+28,3% (к I квартал 2025 г.)
Преступления «террористического характера»	—	—	—	—	4467	+75% (по состоянию на 9 мес. 2024 г.)	—
Общая преступность (контекст)	—	—	−7,3% (2025)	—	—	−16,7% (криминальные, I кв. 2026 г.)	—

На фоне общей преступности экстремистская ситуация приводит к ациклическому росту: +28–30% в годовом эффекте и до +60% по категориям, согласно статистике Генпрокуратуры.

Судебная статистика: осуждённые и приговоры

Таблица 2. Судебная практика по экстремистским и террористическим статьям (2024–2026 гг.)

Показатель	2024	2025	1 полугодие 2025	1 полугодие 2026	Изменение
Осуждённые по «террористическим» статьям	—	2078	—	—	×2 к 2024
Осуждённые по экстремистским статьям (6 мес.)	—	—	~500	—	+35% к 2024 году (6 мес.)
Поступило дело по экстремистским статьям (6 мес.)	—	—	360	489	+36%

Показатель	2024	2025	1 полугодие 2025	1 полугодие 2026	Изменение
Осуждённые по ст. 205.2 УК (пропаганда/призывы), 1 полугодие	—	—	—	357	почти 1/3 всех «террористических» приговоров
Решения по ст. 354.1 УК (реабилитация нацизма и др.)	63	119	—	—	×1,9

Структура и квалификация: «онлайн-экстремизм» и расширение состава.

- Проходящая часть экстремистских деяний происходит в Интернете.
- Резкий рост последствий «террористического характера» (+75% за 9 мес. 2025 г.).
- В другом варианте растёт доля дел, границ с публичными призывами, оправданием и пропагандой терроризма (ст. 205.2 УК).
- Увеличение применения ст. 354.1 УК: осуждённых высказываний стало примерно в 1,5 раза больше; с учётом покушений на материальные объекты — почти вдвоем.

Социальные и возрастные аспекты

- Генпрокуратура отмечает удвоение числа несовершеннолетних, причастных к экстремистским и террористическим преступникам в 2025 г.
- «Антивоенные акции» носят одиночный, немассовый характер, однако часть экстремистских деяний реализуется онлайн.
- Статья о пропаганде терроризма (ст. 205.2 УК) остается самой распространённой, хотя абсолютное число новых дел по ней в 2025 г. Ниже, чем в 2024 г. (102 против 147).

Обсуждение

Полученные данные указывают на несколько взаимосвязанных процессов:

- Расширение квалификаций и активное использование статей для высказываний и онлайн-контента. Рост осуждённых по ст. 205.2 и 354.1 УК, а также увеличение количества дел, поступающих в суды, приводят к смещению правоприменения в идеологически мотивированных высказываниях.
- Усиление интернета и реестров «террористов и экстремистов». Ежегодно в перечне подключаются тысячи новых записей, что коррелирует с ростом зарегистрированных преступлений.
- Геополитический контекст и рост дела «террористического характера». Рост числа пресечений на стадии подготовки и квалификационных действий как «террористических» влияет на общую статистику.
- Социально-психологические факторы радикализации среди подростков и молодёжи. Удвоение числа несовершеннолетних, причастных к таким преступлениям, требует адресных профилактических мер.

Ациклическая динамика (рост экстремизма при снижении общей преступности) может быть частично следствием изменения практики учёта и квалификации, а не только реальным ростом противоправной активности.

Заключение

- В 2024–2026 гг. в России зафиксирован устойчивый рост последствий экстремистской направленности: +28–30% в годовом эффекте и до +60% по третьим категориям.
- Основная доля таких идей реализуется в Интернете. Одновременно резко растёт число дел «террористического характера» и осуждённых за публичные призывы и пропаганду.
- Правоприменение смещается в сторону криминализации высказываний и онлайн-активности, что отражается в росте приговоров по ст. 205.2 УК и ст. 354,1 УК.
- Особую тревогу вызывает удвоение числа несовершеннолетних, причастных к экстремистским и террористическим преступникам.

Дальнейший риск риска требует не только усиления профилактического контроля, но и адресной профилактики радикализации, особенно в цифровой среде и среди молодёжи.

Список источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
2. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 25.05.2026) "О противодействии терроризму" // КонсультантПлюс.
3. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 27.10.2025) "О противодействии экстремистской деятельности" // КонсультантПлюс.
4. См.: Ф. 492 ГИАЦ МВД России за 2024-2026 гг.
5. Приказ Генпрокуратуры России от 09.12.2022 № 746 "О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре" (вместе с "Положением о государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре", "Инструкцией о порядке предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики", "Правилами заполнения учетных документов, используемых для предоставления первичных статистических данных о состоянии преступности, о сообщениях о преступлениях, следственной работе и дознании в государственную автоматизированную систему правовой статистики") // КонсультантПлюс.
6. Состояние преступности в России за январь-декабрь 2025 года. https://мвд.рф/reports/item/77848182/.

С.Ю. Скобелин[1]

ВИДЫ И ПРИЗНАКИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. Предпринята попытка выяснить ключевые признаки, разновидности и дать понятие киберпреступлениям. Обобщены международные и национальные нормативные акты, декларации, а также мнения ученых, статистические данные и правоприменительная практика раскрытия и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий. На основе выявленных признаков киберпресуплений предлагаются рекомендации по их доказыванию.

Ключевые слова: киберпреступления, сеть «Интернет», электронные устройства, цифровые следы, идентификация, расследование.

Для эффективного противодействия киберпреступлениям, как справедливо отмечал В.В. Бычков, следует разобраться с самим понятием и признаками таких преступлений, определить их разновидности[2]. Только в этом случае возможно выработать способы их выявления и документирования, фиксации следов, определить направления версионной работы и планирования, организации и тактики проведения следственных и иных процессуальных действий, оперативно-разыскных мероприятий, сформулировать задачи и разработать инновационные методики экспертных исследований, наконец представить масштабы этого негативного явления и предложить правоприменителям методики расследования и предупреждения подобных преступлений.

В юридической доктрине и правоприменительной практике единства мнений по этому вопросу нет, по-разному называют как сами данные преступления, так и подразделения, нацеленные на борьбу с ними. Это высокотехнологичные, «киберпреступления», преступления в сфере высоких или информационных технологий (IT), преступления, совершенные с использованием электронных и (или) информационно-телекоммуникационных сетей и (или) технологий и др.

Международные акты традиционно декларативны дают довольно обобщенные понятия таких преступлений. Правы Жданов Ю.Н. и Овчинский В.С., акцентирующие внимание на многочисленных разрозненных и неоднозначных подходах к пониманию киберпреступлений и киберпреступности, когда утверждают, что ни в Конвенции Совета Европы о компьютерных преступлениях, ни в Конвенции Лиги арабских государств, ни в проекте Конвенции Африканского союза нет определения термина «киберпреступность» для целей этих документов[3].

Так, Будапештская Конвенция о преступности в сфере компьютерной информации (23.11.2001) основной целью провозглашается лишь сдерживание

---

[1] Скобелин Сергей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

[2] Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. 2024. № 2. С. 56.

[3] Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. С.72.

действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными.

Хотя далее все-таки называются ряд обобщенных деяний (противозаконный доступ, неправомерный перехват, воздействие на данные, на функционирование системы, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, с нарушением авторского права и смежных прав)[1].

В ст. 2 (Термины) Конвенции ООН против киберпреступности (Принята резолюцией 79/243 Генеральной Ассамблеей от 24 декабря 2024 года, г. Нью-Йорк) понятия данных преступлений отсутствует и лишь в главе 2 «Криминализация» даются некоторые наименования возможных разновидностей таких умышленных преступлений (ст. ст. 7-17 Конвенции)[2]:

1. Незаконный доступ;
2. Незаконный перехват;
3. Воздействие на электронные данные;
4. Воздействие на информационно-коммуникационную систему;
5. Неправомерное использование устройств;
6. Подлог с использованием информационно-коммуникационной системы;
7. Хищение или мошенничество с использованием информационно-коммуникационной системы;
8. Преступления, связанные с размещением в интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации;
9. Домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка;
10. Распространение интимных изображений без согласия;
11. Отмывание доходов от преступлений[3].

В Соглашении о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере информационных технологий стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния в сфере информационных технологий, если они совершены умышленно:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем

---

[1] Конвенция о преступности в сфере компьютерной информации (ETS N 185) (Заключена в г. Будапеште 23.11.2001) // СПС Консультант Плюс (дата обращения 21.07.2026).

[2] https://www.un.org/ru/documents/treaty/A-RES-79-243

[3] Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (Заключена в г. Нью-Йорке 24.12.2024) // СПС Консультант Плюс (дата обращения 20.07.2026).

несанкционированного доступа к охраняемой законом компьютерной информации;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети «Интернет» или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети "Интернет" или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма[1].

В России нормативно терминология и признаки таких преступлений не закреплены, а ежегодно меняющийся в целях формирования статистической отчетности перечень преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации (№ 25) данный вопрос решает не полностью[2].

Генеральная прокуратора РФ и МВД РФ в качестве основного критерия, по которым определенные составы преступлений включают в данный перечень справедливо относит способ их совершения, а именно использование:

---

[1] Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Заключено в г. Душанбе 28.09.2018) // СПС Консультант Плюс (дата обращения 20.07.2026).

[2] Указание Генпрокуратуры России № 67/11, МВД России № 1 от 04.02.2026 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» // СПС Консультант Плюс (дата обращения 20.07.2026).

- сети «Интернет» (в т.ч. Даркнет, социальных сетей, мессенджеров, бот-сетей, DDoS-атак, технологий "Дипфэйк" и т.п.);

- средств мобильной связи (SIP-телефонии, технологии ВАТС);

- фиктивных электронных платежей, операций с цифровыми финансовыми активами операции с цифровой валютой;

- специальных средств и техники, предназначенной для компрометации банковских устройств самообслуживания (банкоматов, терминалов);

- информационной инфраструктуры иностранного государства (или придание такого вида), под которой в т.ч. понимаются зарубежные серверы (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д.

Таким образом, не малую долю киберпреступлений в России составляют кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» ч.3 ст. 158 УК РФ), распространение, публичная демонстрация порнографических материалов или предметов (ст.242.1 УК РФ), мошенничество с помощью простых мобильных телефонов (ст.159 УК РФ) и даже взяточничество (ст.290–291.2 УК РФ). Объективная сторона этих преступлений выражена в том, что лица, нашедшие банковские карты совершают по ним покупки; отправляют друг другу через мессенджеры и социальные сети порнографические фото и видео; дают-получают взятки через электронные кошельки или с помощью переводов на банковские карты.

Удачным выглядит предложение О.Ю. Антонова разделить данные преступления на 4 группы:

– преступления в сфере компьютерной информации (глава 28 УК РФ);

– общеуголовные преступления: склонение к самоубийству, развратные действия и другие преступления против половой неприкосновенности несовершеннолетних и др.;

– преступления экономической направленности: хищения (со счетов, банковских карт), мошенничество (сетевое либо с использованием методов социальной инженерии), незаконные организация и проведение азартных игр, легализация доходов, полученных преступным путем, финансирование терроризма и др.;

– преступления, связанные с распространением противоправной информации: порнографических материалов или деструктивного контента (материалов, дискредитирующих использование Вооруженных Сил РФ, либо экстремистских, либо направленных на реабилитацию нацизма); о продаже или способе изготовления предметов, запрещенных к обороту (огнестрельного оружия и боеприпасов, взрывных устройств, наркотиков, персональных данных, криптовалюты и других цифровых активов, фальсифицированной продукции и др.); информации, нарушающей авторские и смежные права либо

неприкосновенность частной жизни, содержащей инструкции о совершении преступлений и т.п.[1]

Очевидно, что киберпреступления – это умышленные преступления, совершенные с использованием сети «Интернет» или мобильной связи, которые имеют различные объекты и мотивы посягательства, совершаются общим субъектом (порой обладающим специальными познаниями в области информационных технологий) путем использования специализированных программ, информационных сетей либо написания (изготовления), отправки (выкладывания), копирования текста, фотографий, видео файлов, продуктов нейросетей.

Основными признаками киберпреступности, как представляется, являются:

1) Использование для совершения преступления сети «Интернет» (в том числе средств анонимизации - прокси серверов, VPN, TOR а также теневых цифровых ресурсов типа «Kraken», «Mega», «BlackSprut» и др.) или мобильной телефонии.

2) Услуги «Интернет» и мобильной телефонии оказываются компаниями провайдерами, хостинг-провайдерами, операторами сотовой связи, администрацией социальной сети, мессенджера, компьютерной игры, админом группы, VPN сервиса за определенную плату;

3) В качестве средства доступа к сети используются различные цифровые устройства: смартфоны, ноутбуки, моноблоки, планшеты и иные компьютеры;

4) Общественно опасное деяние выражено в использовании специализированных программ, сетей, либо написании (изготовлении) и отправке (выкладывании), копировании, текста, фотографий, видео файлов, продуктов нейросетей.

Это означает, во-первых, что при выявлении, раскрытии и расследовании таких преступлений чаще всего необходимо осуществлять взаимодействие (запросы, поручения требования, ходатайства в суд в порядке ч.4 ст.21, ч.7 ст.185. ст.186 УПК РФ, ч.2 ст.7 Закона «О Следственном комитете») с указанными агрегаторами связи, специалистами в области кибербезопасности, IT компаниями, банками. Данные юридические и физические лица помогут определить место и время совершения преступления, идентифицировать устройство и порой самого преступника, новые эпизоды и соучастников, жертв, его транзакции, активность в сети, мета данные, трафик и пр.

Проблема в том, что офисы, оборудование, серверы ряда агрегаторов расположены в недружественных для России странах.

Несмотря на своевременные направления иностранным провайдерам соответствующих запросов, в том числе в порядке ст.453 УПК РФ о правовой помощи в рамках международного сотрудничества, с просьбой сохранения криминалистически значимой цифровой информации, ее предоставления следователю для выяснения всех обстоятельств преступления, такие запросы

[1] Антонов О.Ю. Общие положения методики расследования преступлений, совершенных с использованием информационных технологий // Расследование преступлений: проблемы и пути их решения. № 1.2026. С.43-44.

остаются не исполненными. Особенно это касается видеохостинга YouTube, иных сервисов и инструментов компании Google, мессенджеров Facebook, Skype, WhatsApp и других.

Во-вторых, в ходе проведения следственных, иных процессуальных действий, оперативно-розыскных мероприятий всегда следует обращать внимание на способ подключения к сети и сохранение криминалистически-значимой цифровой информации в памяти перечисленных устройств (смартфонов, компьютеров), внешних накопителей, данных реестров, лог-файлов сетевого оборудования (маршрутизаторов, шлюзов, карт и др.), установленных программ для совершения или сокрытия преступлений, облачных хранилищах, а главное - изымать и исследовать компьютеры преступников и жертв, сохраняя изначальный дамп памяти и исключая дистанционное вмешательство[1].

В -третьих, преступник может тщательно готовиться и препятствовать его изобличению и возможному исследованию его устройств;

В- четвертых, территориально преступник, его соучастники и жертва могут располагаться где угодно.

В этом случае зачастую возникают спорные моменты с определением следственного органа и следователя, который будет возбуждать и принимать к производству уголовное дело. Даже если установлено место совершения преступления, преступление раскрыто и личность преступника установлена, возникают трудности с допросами и привлечением соучастников, потерпевших, свидетелей, проведением иных следственных действий в других субъектах страны или за рубежом [1, с. 10; 2-5; 6, с. 20].

Следователям приходится готовить многочисленные поручения в другие регионы для выполнения соответствующих следственных действий, выезжать самим в командировки либо проводить некоторые следственные действия дистанционно с использованием систем видео-конференц-связи (ст. 189.1. УПК РФ)

Список источников

1. Антонов О.Ю. Общие положения методики расследования преступлений, совершенных с использованием информационных технологий // Расследование преступлений: проблемы и пути их решения. № 1.2026. С.43-44.
2. Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. 2024. N 2. С. 56.
3. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография. М.: Альпен-Принт, 2024. С.464.
4. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. С.72.

[1] Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография. М.: Альпен-Принт, 2024. С.464.

Л.А. Скобелина[1]

ПРЕДУПРЕЖДЕНИЕ МОЛОДЕЖНОГО КИБЕРЭКСТРЕМИЗМА

Аннотация. Рассмотрены уголовно-правовые, административные и обще-социальные меры предупреждения преступлений и правонарушений экстремистского характера несовершеннолетними. Обобщены нормативные акты, декларации, а также мнения ученых, статистические данные и правоприменительная практика раскрытия и расследования подобных преступлений, их разновидности и причины. Предлагаются меры различного уровня и направлений по их предупреждению.

Ключевые слова: киберэкстремизм, сеть «Интернет», несовершеннолетние, предупреждение, ответственность.

В Концепции информационной безопасности детей в РФ 2023 г. справедливо говорится о том, что современные дети – это первое поколение, чье взросление происходит на фоне стремительно развивающихся информационно-коммуникационных технологий. В своих привычках, ценностях и поведении в сети «Интернет» эта группа принципиально отличается от представителей более старшей аудитории (18 - 45 лет). Их основными интересами являются общение в социальных сетях, просмотр видео и онлайн-игры. Несформированность критического мышления обусловливает особую уязвимость детей перед воздействием такой информации, оказывает на несовершеннолетних психотравмирующее воздействие, способствует их виктимизации, вовлечению в деструктивную деятельность, усвоению ими антисоциальных ценностей и норм, побуждает их к совершению общественно опасных действий, способных причинить вред как самому ребенку, так и его окружению[2].

Президентом РФ в п. 22 Стратегии противодействия экстремизму в России отмечается: «Участились случаи привлечения в ряды экстремистских организаций несовершеннолетних лиц, поскольку они не только легче поддаются идеологическому и психологическому воздействию, но и при определенных обстоятельствах не подлежат уголовной ответственности»[3].

Согласно российской энциклопедическому словарю А.М. Прохорова, слово экстремизм (от лат. extremus - «крайний, чрезмерный») означает приверженность крайним и радикальным взглядам, методам действий[4].

---

1 Скобелина Людмила Анатольевна - доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук.

2 Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // СПС Консультант Плюс (дата обращения 12.07.2026).

3 Указ Президента РФ от 28.12.2024 № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации» // СПС Консультант Плюс (дата обращения 12.07.2026).

4 Российский энциклопедический словарь / Гл. ред. А. М. Прохоров. М.: Научное изд-во «Большая Российская энциклопедия», 2000. Т. 2. С. 1832. 1023 с.

Безусловно, несовершеннолетним, находящимся в поиске себя и желающим заявить о себе такие взгляды и методы интересны и привлекательны, а доступность и некая защищенность домашней обстановки придает смелости в ознакомлении с подобными материалами в сети Интернет, вступлении в социальные группы, обсуждении и комментировании различных фото, видео, текстовых материалов.

Так называемый физический экстремизм (насильственное изменение основ конституционного строя, применение насилия по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы; нарушение территориальной целостности Российской Федерации и пр.) несовершеннолетним не свойственен, что подтверждается статистическими данными[1].

Чаще всего дети совершают интеллектуальные экстремистские действия. Осуществляют поиск в сети Интернет экстремистских материалов, дают согласие стать членом определенной группы, обсуждают, высказываются путем печатной речи или голосом, репостят в сети Интернет (распространяют публично) видео, фотоматериалы; выкладывают (демонстрируют) нацистскую атрибутики или символику (сходную с нацистской атрибутику или символику до степени смешения)[2].

Причем, как отмечает Скобликов П.А., изучивший практику привлечения к административной ответственности лиц, совершивших пропаганду либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами (ч.1 ст. 20.3.КоАП РФ), суды зачастую в своих итоговых постановлениях не устанавливают форму вины, не выясняют цели и мотивы деяния, осведомленность фигуранта дела о наличии юридического запрета. Лица в поисках снисхождения, чаще всего признают себя виновными, не прибегают к помощи защитников[3].

При этом повторное совершение подобных действий (или бездействий в случае не удаления символики со страницы социальной сети либо использование запрещенных сетей в течении года влечет уже уголовную ответственность по ст.282.4 УК РФ).

Вряд ли несовершеннолетние осведомлены о существовании федерального списка экстремистских материалов (свыше 5500 материалов), перечня организаций, признанных в соответствии с законодательством Российской Федерации экстремистскими (около 150), нацистской атрибутики или

1 Состояние преступности в России за январь-декабрь 2025 года file:///C:/Users/user/Downloads/Sbornik_dlya_UOS.pdf.

2 Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография. М.: Альпен-Принт, 2024. С.67.

3 Скобликов П.А. Противодействие нацизму и экстремизму: выборочное исследование судебной практики по ч. 1 ст. 20.3 КоАП РФ в контексте действующего законодательства // Актуальные проблемы российского права. 2025. № 1. С. 162 - 179.

символики, размещенных и постоянно пополняющихся на сайте Министерства юстиции РФ.

На сегодняшний день наиболее опасными увлечениями несовершеннолетними в сети Интернет являются такие группы и движения, как:

1. АУЕ («Арестантский уклад един» или «Арестантско-уркаганское единство», пропагандирующее противоправный образ жизни, тюремные понятия, криминальную субкультуру, «воровской закон», «общака» и пр.
2. Колумбайн или скулшутинг - вооруженное нападение на образовательные организации, обучающихся, педагогов внутри образовательного учреждения.
3. Группы смерти («Синий кит», «Разбуди меня в 4.20», «Тихий дом», F57 и др.)
4. Группы националистического, расистского или религиозного толка (Скинхеды, Братья-мусульмане, ИГИЛ, Аль-Каида, Активный клуб, 375 бригада, ЧВК «Редан» и др.)

В стране принято большое количество нормативных актов и создано множество различных организаций, нацеленных на защиту несовершеннолетних от подобного деструктивного влияния, предупреждение совершения ими противоправных деяний, выявления и привлечения виновных к ответственности. Однако основная роль в этом направлении все-таки принадлежит родителям и нам – педагогам.

Безусловно прав Санташов А.Л., когда утверждает, что приоритет нужно отдавать не наказанию детей, а профилактической работе с ними, которая направлена на изменение поведения подростка до совершения преступления. Силы общества должны направляться на ограничение условий, ведущих к преступлению[1].

Минимальные стандартные правила Организации Объединенных Наций, касающихся отправления правосудия в отношении несовершеннолетних (Пекинские правила) закрепили очень важную декларацию: «государства должны стремиться к созданию таких условий, которые обеспечивали бы содержательную жизнь подростка в обществе, чтобы в тот период жизни, когда они наиболее склонны к неправильному поведению, благоприятствовать процессу развития личности, получения образования и отвращению от преступлений и правонарушений»[2].

Также стоит поддержать мнения депутатов Государственной Думы Останиной Н. А. и Яровой И. А., которые неоднократно предлагали исключить меры уголовной ответственности к несовершеннолетним, связанным с изоляцией их от общества за указанные преступления, а также полностью исключить уголовную ответственность несовершеннолетних (имеется в виду освобождение от уголовной ответственности с применением принудительных мер

1 Санташов А.Л. Криминологические и уголовно-правовые аспекты противодействия преступности несовершеннолетних // Российский следователь. 2021. № 6. С. 61 - 63.

2 Минимальные стандартные правила ООН, касающиеся отправления правосудия в отношении несовершеннолетних (Пекинские правила): приняты Резолюцией 40/33 Генеральной Ассамблеи от 29 ноября 1985 г. // СПС "КонсультантПлюс".

воспитательного воздействия – ст.90 УК РФ), совершивших впервые преступления небольшой и средней тяжести (при оставлении исключительных случаев)[1].

Представляется, что коллегам – следователям, оперативным сотрудникам, прокурорам и судьям стоит помнить, что любой человек в возрасте до 18 лет – это ребенок. И не стоит гнаться за пресловутыми служебными показателями, лучше объективно оценивать общественную опасность и вредность совершенного им деяния (мотивы, установить лиц, причастных к его склонению, допустивших упущения в воспитании) и личности самого несовершеннолетнего. Не стоит забывать о таких понятиях, как «малозначительность деяния» (ст.2.9. КоАП РФ и ч.2 ст.14 УК РФ) и возможности выйти в суд с ходатайством о применении к несовершеннолетнему преступнику не карательно-травмирующих мер в виде уголовного наказания, а воспитательных мер (ст.431 УПК РФ, ст.90 УК РФ) и мер социальной реабилитации (а) предупреждение; б) передача под надзор родителей или лиц, их заменяющих, либо специализированного государственного органа; в) возложение обязанности загладить причиненный вред; г) ограничение досуга и установление особых требований к поведению несовершеннолетнего).

Список источников

1. Бычков В.В., Прорвич В.А. Научные основы государственной программы борьбы с киберэкстремизмом: монография. М.: Альпен-Принт, 2024. С.67.
2. Санташов А.Л. Криминологические и уголовно-правовые аспекты противодействия преступности несовершеннолетних // Российский следователь. 2021. № 6. С. 61 - 63.
3. Скобликов П.А. Противодействие нацизму и экстремизму: выборочное исследование судебной практики по ч. 1 ст. 20.3 КоАП РФ в контексте действующего законодательства // Актуальные проблемы российского права. 2025. № 1. С. 162 - 179.

Т.А. Строкова[2]

МОЛОДЕЖНЫЙ КИБЕРЭКСТРЕМИЗМ И ТЕРРОРИЗМ КАК СОВРЕМЕННЫЙ ВЫЗОВ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИИ

Аннотация. В России в последние годы все чаще молодежь становится объектом для вовлечения в преступную деятельность, связанную с киберэкстремизмом и кибертерроризмом, с помощью различных методов воздействия и давления. Используя активно для этого киберпространство и информационные технологии, вражеские силы

1 Путин согласился с идеей смягчения ответственности несовершеннолетних преступников //Известия. https://tass.ru/obschestvo/4765663.

[2] Строкова Татьяна Алексеевна – доцент кафедры гуманитарных и социально-экономических дисциплин Московской академии Следственного комитета им. А.Я. Сухарева, кандидат политических наук, майор юстиции.

вынуждают молодых людей совершать преступления экстремистско-террористического характера. Для сохранения государственности, социальной стабильности и обеспечения национальной безопасности является стратегически важным национальным приоритетом национальной политики защитить современную российскую молодежь от угрозы терроризма и экстремизма.

Ключевые слова: национальная безопасность, киберэкстремизм, кибертерроризм, молодежь, стратегические национальные приоритеты.

Молодежь является будущим любой нации и государства. От ее благополучия и здорового развития в перспективе зависят основы государственности. Обеспечение физической, моральной, духовно-нравственной, психологической, психической, интеллектуальной безопасности современной российской молодежи – одна из приоритетных национальных и политических задач, касающаяся выработки не только грамотной молодежной политики, но и представляющая актуальные, стратегически важные национальные приоритеты для Российской Федерации.

Молодежь в последнее время становится объектом для деструктивного воздействия со стороны различных вражеских, преступных сил, вовлекающих молодых людей, часто несовершеннолетних, в экстремистскую и террористическую деятельность. Молодежный экстремизм и терроризм – широко распространенное явление в современных российских реалиях, которое является угрозой национальной безопасности России. При этом молодежь занимает важное место, как отмечает А.В. Горелкин, среди всех субъектов обеспечения безопасности и стабильности, что связано с двойственностью социального статуса и одновременной ролью и субъекта и объекта социальных отношений, усваивая и транслируя существующие социальные нормы и ценности и при этом выполняет инновационную функцию по ювентизации, т.е., с одной стороны, молодежь обеспечивает сохранение и стабильность социальной системы. С другой стороны, от молодежи зависит общественный прогресс и социальное развитие[1].

Молодежь является наиболее уязвимой социальной группой в силу недостаточности жизненного опыта и знаний, легкой внушаемости, максималистским взглядам, желания быть значимым и хорошо зарабатывать. Эти факторы делают молодых людей объектом для преступного воздействия, чем пользуются деструктивные силы, вовлекая юношей и девушек в экстремистскую и террористическую деятельность. Под экстремисткой деятельностью в соответствии с Федеральным законом от 25.07.2002 № 114-ФЗ (ред. от 27.10.2025) «О противодействии экстремистской деятельности» понимается насильственное изменение конституционного строя; нарушение территориальной целостности РФ; деятельность, связанная с терроризмом или его оправданием; возбуждение социальной, расовой, национальной или религиозной розни, дискриминация или пропаганда превосходства по

[1] См.: Горелкин А.В. Молодежь как субъект обеспечения устойчивого развития российского общества и национальной безопасности // Вестник Кемеровского государственного университета. – № 2-2 (62). – 2015. – С. 25

социальным, национальным, расовым, религиозным признакам, использование нацистской символики, нарушения связанные с реализацией избирательных прав граждан и воспрепятствование законной деятельности органов государственной и местной власти, религиозных и общественных организаций, сопряженные с угрозой применения насилия или насильственными действиями, а также преступные деяния, совершенные на основе политической, идеологической, расовой, национальной или религиозной ненависти или вражды или нетерпимости в отношении какой-либо социальной группы и т.д.[1]. В том числе, как мы видим, в понятие экстремизма входит и террористическая деятельность, к которой в соответствии с Федеральным законом от 06.03.2006 № 35-ФЗ «О противодействии терроризму» относится террористический акт, финансирование, планирование, подготовка, реализация, подстрекательство, вербовка, пособничество, пропаганда и распространение террористических идей, материалов, содержащих информацию, призывы и оправдание терроризма.

Таким образом, мы видим, что экстремизм и терроризм включают в себя широкий спектр деяний, носящих деструктивный, преступный характер и подлежат уголовной ответственности.

С развитием интернета и различных цифровых технологий преступления экстремистско-террористического характера вышли в киберпространство, и получили новую форму киберэкстремизма и кибертерроризма. Под киберэкстремизмом понимается форма экстремистской деятельности, совершаемая в онлайн-среде с использованием социальных сетей, интернет-технологий и цифровых методов. Кибертерроризм часто рассматривается как крайняя и более радикальная форма киберэкстремизма с использованием сети интернет, компьютерных и телекоммуникационных технологий на основе идеологических, политических или религиозных мотивов. Целью кибертерроризма является не только пошатнуть стабильность, но угроза безопасности общества, его дестабилизация, запугивание и устрашение населения, давление на власть. Как отмечают в своей статье В.В. Кудинов и А.В. Минаев, «кибертерроризм – это слияние киберпространства и терроризма, где противозаконная деятельность и угрозы атак в отношении компьютеров, сетей и хранимой информации исполняются с целью запугивания или принуждения государства или его населения к продвижению политических или социальных целей. Кроме того, атака должна привести к насилию по отношению к лицам или имуществу, либо по крайней мере причинить достаточно вреда для порождения страха»[2]. При этом, как считают В.В. Кудинов и А.В. Минаев, «деятельность может считаться кибертерроризмом только при нанесении ущерба конфиденциальности, целостности или доступности компьютеров, сетей и хранимой информации; а также когда ведет к насилию или вреду иного рода»[3]. Данные авторы отмечают, что современные террористы часто используют

[1] См.: ст. 1 ФЗ от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности»

[2] Кудинов В.В., Минаев А.В. Кибертерроризм: основные угрозы и проблемы правового регулирования национальной безопасности Российской Федерации. 2022. № 4.

[3] Там же.

киберпространство как коммуникативные каналы связи, вербовки, сбора информации, получения финансирования и планирования и исполнения атак.

Таким образом, интернет-пространство становится благоприятной средой для распространения экстремисткой идеологии и ведения террористической деятельности, в которую всё чаще вовлекают молодежь, часто не достигшую совершеннолетнего возраста. С помощью социальных сетей, онлайн-игр происходит вербовка молодых людей, насаждение им деструктивных воззрений, даются задания иностранными кураторами, которые с помощью различных способов вынуждают молодых людей, часто несовершеннолетних, совершать диверсионные, подрывные действия на объектах критически важной инфраструктуры, прежде всего железнодорожной. Как отмечают спецслужбы России и ученые, на сегодняшний день ведется массовая, широкомаштабная, целенаправленная деятельность по вовлечению молодежи деструктивными, вражескими силами по средствам сети интернет и цифровой среды в целом с использованием нейросетей и искусственного интеллекта в преступную деятельность экстремистско-террористического характера. Как отмечает ректор Московской академии Следственного комитета им. А.Я. Сухарева А.А. Бессонов в интервью агентству «Интерфакс», «в России каждое пятое преступление в сфере информационных технологий совершено несовершеннолетними»[1].

По данным Росфинмониторинга в 2025 г. существенно выросла доля подростков в возрасте от 14 до 17 лет, числящихся в реестре экстремистов и террористов и причастных к экстремистской или террористической деятельности. Прежде чем завербовать подростка преступники тщательно изучают психологический портрет и личность своей жертвы через информацию, размещенную в социальных сетях, вступают в переписку с подложных, фейковых аккаунтов, чтобы заполучить как можно больше сведений, обработать психологически и подтолкнуть к преступным действиям. Таким образом, идет спланированная атака на молодое поколение россиян, наносящая значительный урон духовно-нравственному, психоэмоциональному, физическому состоянию и развитию, калечат неокрепшую психику молодых людей, ломают судьбы. Часто молодые люди могут вовлекаются в преступную деятельность, связанную с киберэкстремизмом или киберэкстремизмом, и самостоятельно из-за желания заработать легкие и быстрые деньги. Преступники размещают в интернете объявления о сомнительной дистанционной работе, обещая заплатить большие деньги. Молодые люди особенно несовершеннолетние откликаются на подобные объявления, предоставляют свои паспортные данные неизвестным лицам, оформляют на себя сим-карты, с которых осуществляют деятельность украинские террористы, и т.д. За подобную деятельность российское уголовное законодательство предусматривает серьезные наказания. Наши спецслужбы оперативно отслеживают и пресекают подобную преступную деятельность.

[1] Каждое пятое киберпреступление в РФ совершено подростками - статистика СКР // Агенство «Интерфакс». Электронный ресурс (режим доступа: https://www.interfax-russia.ru/northwest/main/kazhdoe-pyatoe-kiberprestuplenie-v-rf-soversheno-podrostkami-statistika-skr).

Молодые люди, которые занимались подобной трудовой деятельностью, получают наказания в виде лишения свободы вне зависимости, знали ли они о преступности своей работы или были «использованы в слепую».

Таким образом, в последнее время проблема вовлеченности молодежи в экстремистскую и террористическую деятельность особенно с использованием кибертехнологий, сети интернет, социальных сетей, цифровровой среды и искусственного интеллекта становится острой и требующей незамедлительного реагирования со стороны действующей власти, законодательных и правоохранительных органов. Вовлечение молодых людей в возрасте от 14 до 30 лет и особенно несовершеннолетних подростков в киберэкстремистскую и кибертеррористическую деятельность является современным вызовом национальной безопасности Российской Федерации и наносит ей значительный урон. Требуются законодательно разработанные меры по защите молодых людей, эффективный комплекс профилактических мероприятий и практические механизмы реализации установленных мер и алгоритмов действий по предотвращению вовлеченности молодежи данными видами преступной деятельности.

Список источников

1. Бычков В.В., Прорвич В.А. Информационная модель криминалистической характеристики киберэкстремизма // Вестник Московской академии Следственного комитета Российской Федерации. 2023. № 3. С. 113 - 120.
2. Бычков В.В., Прорвич В.А. Киберэкстремизм в системе киберпреступности // Российский следователь. 2015. № 2. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=153402#1rruKPVYNmR2CSzJ (дата обращения: 24.05.2026).
3. Горелкин А.В. Молодежь как субъект обеспечения устойчивого развития российского общества и национальной безопасности // Вестник Кемеровского государственного университета. 2015. № 2-2 (62). С. 23-26.
4. Каждое пятое киберпреступление в РФ совершено подростками - статистика СКР // Агенство «Интерфакс». Электронный ресурс. – URL: https://www.interfax-russia.ru/northwest/main/kazhdoe-pyatoe-kiberprestuplenie-v-rf-soversheno-podrostkami-statistika-skr (дата обращения: 23.05.2026).
5. Кудинов В.В., Минаев А.В. Кибертерроризм: основные угрозы и проблемы правового регулирования национальной безопасности Российской Федерации. 2022. № 4
6. Макашова В.Н., Чернова Е.В. Информационные технологии как фактор распространения идей киберэкстремизма в молодежной среде // Современные информационные технологии и ИТ-образование. 2013. № 9. С. 328-335
7. Ситникова М.В. Противодействие экстремизму в молодежной среде: уголовно-правовой и криминологический аспекты: по материалам Приволжского федерального округа : диссертация ... кандидата

юридических наук : 5.1.4. / Ситникова Марина Петровна; [Место защиты: «Балтийский федеральный университет имени Иммануила Канта» ; Диссовет 99.2.127.02]. — Калининград, 2026. — 232 с.
8. Федеральный закон от 25.07.2002 №114-ФЗ «О противодействии экстремистской деятельности». URL: https: //consultantplus.
9. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму». URL: https: //consultantplus.

А.Д. Цыплакова[1]

МЕТОДЫ ВЫЯВЛЕНИЯ ДЕСТРУКТИВНЫХ МАТЕРИАЛОВ В СЕТИ ИНТЕРНЕТ В ОТДЕЛЬНЫХ ИНОСТРАННЫХ ГОСУДАРСТВАХ

Аннотация. В настоящей работе рассматриваются зарубежные подходы к выявлению деструктивного контента в информационно-коммуникационной сети «Интернет». Соответствующие меры обычно формируются применительно к отдельным видам онлайн-вреда, включая террористический и насильственно-экстремистский контент, материалы сексуальной эксплуатации несовершеннолетних, разжигание ненависти, преследование, склонение к самоповреждению и иные формы вредоносного цифрового воздействия. Выделяются основные методы выявления: пользовательские и экспертные уведомления, хэш-сопоставление, перцептивное хэширование, автоматизированная классификация текста, мультимодальный анализ изображений и видео, поведенческая аналитика, кризисные протоколы и риск-ориентированная оценка платформ. Эффективная зарубежная модель представляет собой гибридную систему, соединяющую автоматическое техническое выявление, экспертную проверку, правовые критерии, отчётность платформ и процедуры обжалования. В статье обозначены проблемы и некоторые пути их решения.

Ключевые слова: деструктивный контент, Интернет, цифровые платформы, автоматизированная модерация, хэш-сопоставление, террористический контент, материалы сексуальной эксплуатации несовершеннолетних, доверенные уведомители, риск-ориентированный подход, зарубежный опыт.

Распространение деструктивного контента в Интернете относится к числу значимых вызовов современной уголовно-правовой, криминологической и информационно-правовой политики. Цифровые платформы позволяют быстро тиражировать запрещённые материалы и требуют алгоритмической модерации для эффективного противодействия неправомерному контенту[2].

Методы выявления можно поделить на две большие группы: сигнатурное сопоставление и прогностическая классификация, в том числе с использованием достижений в сфере искусственного интеллекта (ИИ) для целей автоматизации — и шесть подгрупп.

Во-первых, *реактивные методы* выявления: *жалобы пользователей, обращения государственных органов, сообщения неправительственных*

[1] Цыплакова Алёна Дмитриевна – старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики МГИМО МИД России, кандидат юридических наук.

[2] Gorwa R., Binns R., Katzenbach C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance // Big Data & Society. 2020. Vol. 7. № 1. P. 1–15.

организаций, специализированные горячие линии и уведомления доверенных субъектов — зависят от активности заявителей и последующей обработки сообщений, однако позволяют учитывать контекст, особенно когда вредоносность материала зависит от адресата, ситуации распространения, языка или скрытой символики. Так, например, Регламентом ЕС 2022/2065 о цифровых услугах[1] предусмотрен институт доверенных уведомителей, который предоставляется субъектам, обладающим специальной компетенцией в выявлении и уведомлении о незаконном контенте, независимостью от платформ и способностью действовать добросовестно, точно и объективно[2]. Регламентом ЕС 2021/784 о противодействии распространению террористического контента онлайн[3] предусмотрена обязанность хостинг-провайдеров удалять террористический контент или блокировать доступ к нему в течение одного часа после получения распоряжения компетентного органа. Примечательно, что в государствах-членах ЕС данный срок распространим на явно незаконный контент (примером служит Германия[4]), в то время как остальной вредоносный должен быть удалён в течение 7 дней.

Зарубежный институт доверенных уведомителей может быть интересен как модель профессионализации первичных сообщений о вредоносном контенте, если такая модель сопровождается критериями компетентности, независимости и ответственности уведомителя. Схожий опыт реализуется в рамках казахстанского проекта «Кибернадзор»[5]: более 20 министерств и агентств наряду с гражданами могут направить жалобу на рассмотрение Министерству культуры и информации Республики. Вовлечение гражданского общества в противодействие преступности представляется важным направлением её профилактики.

При этом ряд государств Глобального Севера и Глобального Юга на законодательном уровне возлагает обязанность на цифровые платформы выявлять и блокировать незаконный контент, анализировать риски незаконного контента, поддерживать актуальность такой оценки, внедрять меры снижения рисков, обеспечивать понятные пользовательские правила и процедуры жалоб[6].

---

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) // Official Journal of the European Union. 2022. L 277. P. 1–102.

[2] European Commission. Trusted flaggers under the Digital Services Act // European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa (дата обращения: 15.06.2026).

[3] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29.04.2021 on addressing the dissemination of terrorist content online // Official Journal of the European Union. 2021. L 172. P. 79–109.

[4] Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz — NetzDG) 01.09.2017 // Bundesgesetzblatt. 2017. Teil I. S. 3352.

[5] Кибернадзор: официальный сайт. URL: kibernadzor.kz (дата обращения: 15.06.2026).

[6] Цыплакова А. Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: диссертация на соискание ученой степени кандидата юридических наук / Цыплакова Алёна Дмитриевна. Москва, 2025. 368 с.; Online Safety Act 2023 // legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2023/50 (дата обращения: 15.06.2026); Ofcom. Statement:

При этом проблематика состоит в различных подходах к перечню запрещённого и множественности компетентных органов в данной сфере[1]. В Великобритании, например, выделяется 17 групп неправомерного контента, включая терроризм, сексуальную эксплуатацию несовершеннолетних, груминг, материалы сексуального насилия над детьми, разжигание ненависти, преследование, угрозы, незаконный оборот наркотиков, мошенничество и иные формы цифрового вреда[2]. В связи с этим можно выделить ещё одну группу: *организационно-комплаенсные методы*: оценка риска, аудит, отчёты прозрачности, внутренние регламенты модерации, процедуры апелляции.

В рамках Европейского союза и Великобритании функционируют институциональные механизмы по типу «Counter Terrorism Internet Referral Unit»[3], в рамках которых сообщения о террористическом материале проходят оценку специалиста, после чего возможны расследование и обращение к провайдеру об удалении, а также формируются банки изображений, видео и электронных файлов формата «.pdf», связанных с террористической и насильственно-экстремистской активностью, по типу «TCO-DETECT». На глобальном уровне аналогом можно считать базу данных Глобального Интернет-форума для противодействия терроризму[4]. При этом существенное значение имеют критерии отнесения к террористическому или экстремистскому контенту, доступ малых платформ к таким инструментам, возможность независимой проверки, а также возможность апеллирования решения о включении материала в базу для соблюдения минимальных стандартов прав человека в виртуальной среде.

Для отдельных категорий материалов может быть полезен опыт верифицированных баз цифровых отпечатков и использование их в отечественной практике.

В связи с обозначенным можно выделить ещё одно направление — *сигнатурные методы, основанные на сопоставлении* с уже известным вредоносным материалом, особенно эффективны в отношении повторного

Protecting people from illegal harms online // Ofcom. 16.12.2024. URL: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/statement-protecting-people-from-illegal-harms-online (дата обращения: 15.06.2026).

[1] Цыплакова А. Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: современное состояние, проблемы и перспективы // Право и управление. XXI век. 2025. Т. 21, № 3(76). С. 62-75; Цыплакова А. Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности // Российский следователь. 2025. № 10. С. 62-66.

[2] Ofcom. Illegal content duties under the Online Safety Act // Ofcom. 18.02.2026. URL: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/illegal-content-duties-under-the-online-safety-act (дата обращения: 15.06.2026).

[3] Counter Terrorism Policing. Together, We’re Tackling Online Terrorism // Counter Terrorism Policing. 19.12.2018. URL: https://www.counterterrorism.police.uk/news/together-were-tackling-online-terrorism/ (дата обращения: 15.06.2026); Report online material promoting terrorism or extremism // GOV.UK. URL: https://www.gov.uk/report-terrorism (дата обращения: 15.06.2026).

[4] GIFCT. GIFCT’s Hash-Sharing Database // Global Internet Forum to Counter Terrorism. URL: https://gifct.org/hsdb/ (дата обращения: 15.06.2026).

распространения материалов сексуальной эксплуатации несовершеннолетних и террористических видеозаписей, однако они ограниченно применимы к новому, видоизменённому или контекстно неоднозначному контенту. К ним относятся криптографические хэши, перцептивные хэши, «PhotoDNA» (проект компании «Microsoft»)[1], «CSAI Match» (применяется «Google»[2], «Youtube») базы цифровых отпечатков изображений, видео и URL-ссылок. После теракта в Крайстчерче стали распространяться т.н. кризисные протоколы для координации действий государств, платформ и гражданского общества при распространении террористического и насильственно-экстремистского контента в реальном времени[3].

В-четвертых, *методы обработки естественного языка и глубокого обучения* (машинное обучение) применяются для выявления разжигания ненависти, угроз, преследования, вербовочных сообщений, суицидального контента, «криминальных» инструкций и иных текстовых форм вреда, однако всё ещё остаются зависимыми от языка, обучающих данных, культурного контекста и качества разметки[4]. Важно закладывать подобное ещё на этапе проектирования (принцип «safety by design»)[5], а не удалять *ad hoc*. Выстраивание соответствующей архитектуры должно учитывать хэштеги, сигналы, иносказательную лексику, культурные и религиозные особенности, которые обычно обходят прямолинейные формально-логические (алгоритмические) выявления[6], а также различные форматы контента. Научные модели нередко работают с узкими корпусами данных, тогда как платформы сталкиваются с многоязычной, мультимодальной и быстро меняющейся средой[7].

---

[1] Microsoft. PhotoDNA // Microsoft. URL: https://www.microsoft.com/en-us/photodna (дата обращения: 15.06.2026); Microsoft. Digital Safety Content Report // Microsoft Corporate Social Responsibility. URL: https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report (дата обращения: 15.06.2026).

[2] Google. Google’s Efforts to Combat Online Child Sexual Abuse Material // Google Transparency Report. URL: https://support.google.com/transparencyreport/answer/10330933 (дата обращения: 15.06.2026).

[3] Christchurch Call. Responding to Crises // Christchurch Call. URL: https://www.christchurchcall.org/responding-to-crises/ (дата обращения: 15.06.2026); EU Internet Forum committed to an EU-wide Crisis Protocol // European Commission. 06.10.2019. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009 (дата обращения: 15.06.2026).

[4] Jahan M.S., Oussalah M. A systematic review of hate speech automatic detection using natural language processing // Neurocomputing. 2023. Vol. 546. Article 126232.

[5] Подобный подход заложен в австралийском правовом регулировании. Online Safety Act 2021 (Cth). No. 76, 2021 // Federal Register of Legislation. URL: https://www.legislation.gov.au/C2021A00076/latest (дата обращения: 15.06.2026).

[6] Lookingbill V., Le K. “There’s Always a Way to Get Around the Guidelines”: Nonsuicidal Self-Injury and Content Moderation on TikTok // Social Media + Society. 2024. Vol. 10. № 2. DOI: 10.1177/20563051241254371.

[7] Arora A., Nakov P., Hardalov M., Sarwar S.M., Nayak V., Dinkov Y., Zlatkova D., Dent K., Bhatawdekar A., Bouchard G., Augenstein I. Detecting Harmful Content on Online Platforms: What Platforms Need vs. Where Research Efforts Go // ACM Computing Surveys. 2023. Vol. 56. № 3. Article 72. P. 1–37.

В связи с этим целесообразно выделять ещё одно направление — *мультимодальные методы*, предполагающие одновременный анализ текста, изображения, видео, звука, символики, метаданных и иных признаков, важны для выявления мемов, зашифрованной пропаганды, экстремистской символики и контента[1]. Подобный подход наиболее логичен, хотя и труден в реализации. В ноябре 2020 г. Центр ИИ и робототехники Исследовательского института УНП ООН совместно с Министерством внутренних дел ОАЭ запустили инициативу «ИИ для более безопасных детей» (англ. «Artificial Intelligence for Safer Children»)[2] для разработки инструмента по эффективному мониторингу и выявлению запрещённого контента, а также жертв торговли людьми среди несовершеннолетних. В июле 2022 г. была издана онлайн-платформа, которая активно используется не только сотрудниками Департамента по защите детей МВД ОАЭ, но и правоохранительными органами других стран Глобального Юга.

Наконец, отдельно отметим *поведенческие и сетевые методы*, включающие повторяющиеся паттерны размещения, координация аккаунтов, миграция сообществ между платформами, массовое тиражирование ссылок, всплески активности в кризисные периоды, важны при выявлении радикализирующих сетей, организованной травли, распространения террористической символики и кампаний по тиражированию вредоносных материалов[3]. В этой связи представляют интерес проекты с использованием технологий ИИ: Федеральная полиция разрабатывает и обучает систему, которая могла бы распознавать и интерпретировать эмодзи и сленг, используемый поколениями «Альфа»[4] и «Зумеры»[5], для выявления так называемых криминальных инфлюенсеров (англ. «crimefluencers»), тяготеющих к насильственному экстремизму, нигилизму, садизму, нацизму и сатанизму[6]. Более широкого профиля база разрабатывается в Германии — дата-сеты из изъятых данных, систематизированные для дальнейшего обучения нейросетей[7].

Несмотря на развитие технологий, автоматизированное выявление деструктивного контента не может рассматриваться как самодостаточный правовой механизм. Во-первых, алгоритмические системы сталкиваются с

---

[1] Kiela D., Firooz H., Mohan A., Goswami V., Singh A., Ringshia P., Testuggine D. The Hateful Memes Challenge: Detecting Hate Speech in Multimodal Memes // Advances in Neural Information Processing Systems. 2020. Vol. 33. P. 2611–2624.

[2] AI for Safer Children // UNICRI. URL: https://unicri.org/topics/AI-for-Safer-Children (дата обращения: 15.06.2026).

[3] Govers J., Feldman P., Dant A., Patros P. Down the Rabbit Hole: Detecting Online Extremism, Radicalisation, and Politicised Hate Speech // ACM Computing Surveys. 2023. Vol. 55. № 14s. DOI: 10.1145/3583067.

[4] С 2010-е по 2025 гг.

[5] Примерно со второй половины 1990-х по 2010-е гг.

[6] Sharwood S. Australian police building AI to translate emoji used by ‘crimefluencers’ // The Register. 29.10.2025. URL: https://www.theregister.com/2025/10/29/afp_ai_commissioner_barrett_speech/ (дата обращения: 15.06.2026).

[7] Berlin: Police can secretly enter homes for state trojan installation // Heise online. 05.12.2025. URL: (дата обращения: 15.06.2026).

проблемой контекста. Во-вторых, сохраняется языковая и культурная зависимость моделей. Системы, обученные на англоязычных корпусах, не всегда корректно работают с малораспространёнными языками, диалектами, сленгом, мемами и кодовыми обозначениями. Вдобавок, для обучения нейросетей на восточных языках требуется значительно больше времени, объёма и мощностей, поскольку английский более компактен и занимает меньшее количество токенов. В-третьих, существует риск ложноположительных и ложноотрицательных решений. Первые ведут к необоснованному удалению правомерного контента, вторые — к сохранению вредоносного материала в сети. В правовом отношении обе ошибки значимы: первая затрагивает свободу выражения мнения, вторая — безопасность личности, общества и государства. В-четвёртых, автоматизация способна усиливать непрозрачность. Наконец, блокировка или удаление запрещённого контента не всегда подразумевает привлечение конкретного пользователя к уголовной ответственности. В перспективе представляется целесообразной система подобная по интеллектуальному управлению дорожным движением в Китае, которая осуществляет генерацию правил дорожного движения и контроль их исполнения, вплоть до идентификации правонарушителя, выписывания административного штрафа и первичного сбора доказательственной информации для последующего возбуждения уголовного дела[1]. Фактически на данный момент функционируют только административно-правовые и цифровые механизмы: замораживание аккаунта или полное удаление, а также частичное или полное прекращение доступа, однако сохраняется проблематика идентификации и установления аффилиации личности в рамках уголовного судопроизводства. Правоохранительные органы получают сведения *ad hoc* по запросу в рамках конкретного уголовного дела, тогда как было бы целесообразным рассмотреть аналог с сообщениями о подозрительных операциях от подразделений финансовой разведки, которая в свою очередь получает их от центрального банка страны, установленных нефинансовых предприятий и профессий, а также кредитных организаций согласно рекомендациям ФАТФ.

Также отметим проблематику того, что и как блокируется: в то время в Российской Федерации зачастую осуществляется блокировка доступа к Интернет-ресурсу[2], в зарубежных странах больший упор сделан на удаление непосредственно запрещённого контента.

Зарубежный опыт показывает, что выявление деструктивного контента в Интернете развивается как гибридная система. В её основе лежит сочетание нескольких элементов: технического обнаружения, экспертной проверки, правового критерия, риск-оценки платформы, межплатформенного обмена

[1] Атабеков А.Р. Применение искусственного интеллекта в рамках реализации административной функции правоохранительных органов: опыт, перспективы, регламентация // Теория и практика общественного развития. 2023. № 4 (182). С. 122-127.

[2] Роскомнадзор. Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено // Роскомнадзор. URL: https://eais.rkn.gov.ru/ (дата обращения: 15.06.2026).

сигналами, кризисного реагирования и процедур защиты пользователей от ошибочного удаления. Она должна включать в себя классификацию видов деструктивного контента, критерии правовой оценки, проверяемые технические инструменты, участие компетентных субъектов, отчётность платформ, процедуры обжалования и гарантии сохранения правомерного контента. Подобное может быть реализуемо в том числе в рамках Дополнительного протокола к Конвенции ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

Список источников

1. Атабеков А.Р. Применение искусственного интеллекта в рамках реализации административной функции правоохранительных органов: опыт, перспективы, регламентация // Теория и практика общественного развития. 2023. № 4 (182). С. 122-127.
2. Цыплакова А. Д. Международное сотрудничество в борьбе с киберпреступлениями: некоторые правовые проблемы в свете принятия Конвенции ООН против киберпреступности // Российский следователь. 2025. № 10. С. 62-66.
3. Цыплакова А. Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: диссертация на соискание ученой степени кандидата юридических наук / Цыплакова Алёна Дмитриевна. Москва, 2025. 368 с.
4. Цыплакова А. Д. Противодействие киберпреступлениям в отдельных странах Глобального Юга: современное состояние, проблемы и перспективы // Право и управление. XXI век. 2025. Т. 21, № 3(76). С. 62-75.
5. Arora A., Nakov P., Hardalov M., Sarwar S.M., Nayak V., Dinkov Y., Zlatkova D., Dent K., Bhatawdekar A., Bouchard G., Augenstein I. Detecting Harmful Content on Online Platforms: What Platforms Need vs. Where Research Efforts Go // ACM Computing Surveys. 2023. Vol. 56. № 3. Article 72. P. 1–37.
6. Gorwa R., Binns R., Katzenbach C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance // Big Data & Society. 2020. Vol. 7. № 1. P. 1–15.
7. Jahan M.S., Oussalah M. A systematic review of hate speech automatic detection using natural language processing // Neurocomputing. 2023. Vol. 546. Article 126232.
8. Kiela D., Firooz H., Mohan A., Goswami V., Singh A., Ringshia P., Testuggine D. The Hateful Memes Challenge: Detecting Hate Speech in Multimodal Memes // Advances in Neural Information Processing Systems. 2020. Vol. 33. P. 2611–2624.

9. Lookingbill V., Le K. “There’s Always a Way to Get Around the Guidelines”: Nonsuicidal Self-Injury and Content Moderation on TikTok // Social Media + Society. 2024. Vol. 10. № 2. DOI: 10.1177/20563051241254371.

А.А. Шибанова[1]

ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ: ОЦЕНКА ЗАТРАТ, РИСКОВ И ВЛИЯНИЯ НА ФИНАНСОВУЮ УСТОЙЧИВОСТЬ

Аннотация. В статье рассматриваются экономические аспекты обеспечения кибербезопасности предприятий в условиях ускоренной цифровизации хозяйственной деятельности. Обосновано, что расходы на защиту информационных систем перестают быть исключительно технической статьей бюджета и приобретают значение элемента финансовой устойчивости, поскольку информационные атаки способны вызывать простой производственных процессов, потерю данных, нарушение договорных обязательств, снижение выручки, рост внеплановых расходов и ухудшение деловой репутации. На основе статистических данных Росстата проанализирована динамика затрат организаций на внедрение и использование цифровых технологий, структура расходов по видам экономической деятельности, распространенность угроз информационной безопасности и применяемых защитных средств. Сделан вывод о необходимости риск-ориентированного планирования затрат на кибербезопасность предприятий, при котором расходы соотносятся не только с текущими потребностями, но и с ожидаемым экономическим ущербом от возможных угроз, параметрами ликвидности, долговой нагрузки и устойчивости денежных потоков предприятия.

Ключевые слова: кибербезопасность, экономическая безопасность, финансовая устойчивость, затраты, информационная безопасность, риск-менеджмент, финансовая безопасность.

Цифровая трансформация предприятий сопровождается не только ростом производительности, автоматизацией управленческих процедур и расширением каналов взаимодействия с контрагентами, но и увеличением зависимости бизнеса от информационной инфраструктуры. Глубокая интеграция цифровых технологий в процессы закупки, сбыта, бухгалтерского учета, логистики, кадрового администрирования, производственного контроля повышает экономическую значимость нарушений их нормального функционирования. Киберугрозы в таких условиях выражаются не только в технических сбоях, но и в прямых финансовых потерях, нарушении обязательств, падении доверия партнеров, возникновении регуляторных рисков и росте расходов на восстановление.

В научной литературе проблема кибербезопасности все чаще рассматривается через категорию экономической безопасности предприятия. Отдельные авторы связывают развитие концепции экономической безопасности с цифровой трансформацией, подчеркивая необходимость учета новых угроз, возникающих

[1] Шибанова Анна Анатольевна – старший преподаватель кафедры гуманитарных и социально-экономических дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат экономических наук, майор юстиции.

в информационной среде[1]. Другие исследователи применительно к промышленным предприятиям показывают, что цифровая экономика меняет не только технологический уклад, но и систему рисков, влияющих на финансовую стабильность, рентабельность и непрерывность деятельности[2].

Ученые также выделяют киберугрозы в числе значимых рисков цифровой трансформации, поскольку уязвимости информационной инфраструктуры способны преобразовываться в ущерб для экономической системы[3]. Встречается мнение, что кибератаки являются самостоятельной угрозой финансовой безопасности компании, что позволяет связать информационную защиту с устойчивостью денежных потоков, сохранностью активов и деловой репутацией[4].

Современные предприятия вынуждены одновременно решать две взаимосвязанные задачи: увеличивать цифровые инвестиции и ограничивать вероятность ущерба от киберрисков. При недостаточных вложениях организация остается уязвимой перед вредоносными программами, несанкционированным доступом, утечками данных и остановкой информационных ресурсов. При избыточных и плохо обоснованных расходах возникает иной риск: средства отвлекаются от основной деятельности, ухудшается структура затрат, снижается рентабельность, а финансовая устойчивость не получает сопоставимого положительного эффекта. Поэтому экономическая оценка кибербезопасности должна строиться не по принципу «чем больше расходов, тем выше защищенность», а через сопоставление стоимости защитных мер, вероятности угроз, размера потенциального ущерба и способности предприятия сохранять платежеспособность при наступлении неблагоприятного события.

Экономическая сущность затрат на кибербезопасность предприятия, оценка статистических тенденций цифровых расходов и информационных угроз, а также определении влияния киберрисков на финансовую устойчивость хозяйствующих субъектов является актуальной темой для научных дискуссий[5].

Экономическая безопасность предприятия традиционно связывается со способностью организации сохранять устойчивое функционирование,

---

[1] Докукина А.А. Теоретические основы концепции экономической безопасности предприятия в контексте цифровой трансформации // Экономика, предпринимательство и право. 2023. Т. 13. № 4. С. 1105–1124.

[2] Кобышева М.С., Володин А.А., Иванов М.В., Феофилова Т.Ю., Манасерян Т.М. Риски и угрозы экономической безопасности России в условиях цифровой трансформации // Вестник Алтайской академии экономики и права. 2021. № 2. С. 53–60.

[3] Клыков Д.А. О некоторых вопросах экономической безопасности предприятия в условиях цифровизации. В сборнике «За нами будущее: взгляд молодых ученых на инновационное развитие общества». Сборник научных статей 2-й Всероссийской молодежной научной конференции. Курск, 2021. С. 131-134.

[4] Мамий Е.А., Рябовол Е.А. Кибератаки как угроза финансовой безопасности компании. В сборнике «Кластеризация цифровой экономики: Глобальные вызовы» Сборник трудов национальной научно-практической конференции с зарубежным участием. 2020. С. 541-546.

[5] Кобышева М.С., Володин А.А., Иванов М.В., Феофилова Т.Ю., Манасерян Т.М. Риски и угрозы экономической безопасности России в условиях цифровой трансформации // Вестник Алтайской академии экономики и права. 2021. № 2. С. 53–60.

противостоять внутренним и внешним угрозам, обеспечивать платежеспособность, рентабельность, ресурсную автономию и развитие. В условиях цифровизации эта способность зависит не только от финансовых, производственных и кадровых факторов, но и от надежности информационных систем. Цифровая инфраструктура становится средой, в которой создаются, передаются и хранятся ключевые управленческие данные, сведения о клиентах, договорах, платежах, производственных процессах, интеллектуальной собственности и коммерческих планах.

Кибербезопасность предприятия в экономическом смысле представляет собой систему организационных, технических, правовых и финансовых мер, направленных на предотвращение ущерба от нарушения конфиденциальности, целостности и доступности информации. Ее отличие от узкого технического понимания состоит в том, что объектом защиты выступают не только серверы, рабочие станции, сети и программное обеспечение, но и финансовый результат предприятия. Неэффективная информационная система приводит к потенциальной потере доходов, выручки и в конечном счете прибыли. Утеря или искажение данных приводит к увеличению расходов на восстановление, аудит и претензионную работу. Утечка конфиденциальной информации в большинстве случаев способствует убыткам, связанным с потерей клиентов, дополнительными требованиями контрагентов, репутационными потерями и санкциями со стороны регулирующих органов. В этом проявляется связь кибербезопасности с финансовой устойчивостью.

В работах, посвященных финансовой безопасности и устойчивости предприятия, подчеркивается значение ликвидности, платежеспособности, структуры капитала, способности финансировать текущую деятельность и противостоять неблагоприятным воздействиям. Киберугрозы способны одновременно ухудшить несколько указанных параметров: сократить входящий денежный поток, увеличить срочные расходы, создать непредвиденные обязательства и снизить доверие кредиторов или инвесторов. Следовательно, расходы на кибербезопасность должны рассматриваться в том числе как инвестиции в снижение волатильности финансового результата и поддержание непрерывности бизнеса.

В экономическом анализе целесообразно разделять затраты на кибербезопасность на четыре группы. Первая группа может включать превентивные расходы, связанные с внедрением средств аутентификации, разграничением прав доступа, антивирусной защитой, резервным копированием, шифрованием, обучением сотрудников, аудитом защищенности, разработкой внутренних регламентов. Вторая группа может представлять расходы на выявление угроз, например, мониторинг событий, системы обнаружения вторжений, анализ журналов, услуги центра мониторинга, внутренние проверки. Третья группа, предполагается, включает расходы на реагирование и восстановление финансовой стабильности: расследование инцидента, восстановление данных, замена оборудования, юридическое сопровождение, уведомление заинтересованных лиц, работа с претензиями. Четвертая группа может включать потери от последствий, например, в результате простоя,

недополученной выручки, штрафов, компенсаций, снижения рыночной стоимости, ухудшения условий кредитования, оттока клиентов.

Такое деление позволяет перейти от формального учета расходов к оценке экономического эффекта. Предприятие должно стремиться не к максимальному набору инструментов, а к такому уровню защиты, при котором предельное снижение ожидаемого ущерба превышает предельные затраты на соответствующие меры. Иными словами, экономически обоснованная кибербезопасность – это не абсолютная защищенность, которая практически недостижима, а управляемое снижение риска до уровня, совместимого с финансовыми возможностями, отраслевой спецификой и критичностью бизнес-процессов.

По данным Росстата[1] валовые внутренние затраты на развитие цифровой экономики в России увеличились с 3324 млрд рублей в 2017 г. до 6673 млрд рублей в 2024 г. В текущих ценах показатель за рассматриваемый период вырос примерно в два раза. При этом отношение данных затрат к ВВП изменялось менее равномерно: 3,6% в 2017 г., 3,8% в 2020 г., 3,1% в 2023 г. и 3,3% в 2024 г. Такая динамика показывает, что цифровизация остается значимым направлением экономического развития, однако ее интенсивность относительно масштаба экономики зависит от макроэкономической конъюнктуры, инвестиционной активности и структуры расходов.

Особое значение для анализа предприятий имеют затраты организаций на внедрение и использование цифровых технологий и связанных с ними товаров и услуг. В 2019 г. их совокупный объем составлял 2742 млрд руб., в 2020 г. - 2882 млрд руб., в 2021 г. - 3797 млрд руб., в 2022 г. - 4171 млрд руб., в 2023 г. - 4617 млрд руб., в 2024 г. - 5915 млрд руб. Так, за 2019–2024 гг. показатель увеличился примерно на 115,7%, то есть более чем в 2,1 раза. Только за 2024 г. прирост относительно 2023 г. составил около 28,1%. Это подтверждает, что цифровые расходы становятся устойчивой и быстрорастущей частью корпоративных бюджетов.

Таблица 1. Динамика затрат организаций на внедрение и использование цифровых технологий, млрд руб.

Год	Всего	Внутренние затраты	Внешние затраты
2019	2742	2164	578
2020	2882	2051	831
2021	3797	2836	961
2022	4171	3017	1154
2023	4617	3153	1464
2024	5915	4087	1828

[1] Использование цифровых технологий организациями по Российской Федерации, субъектам Российской Федерации и видам экономической деятельности : статистические данные. Федеральная служба государственной статистики Российской Федерации официальный сайт. URL:https://rosstat.gov.ru/ storage/mediabank/ikt_org.xlsx (дата обращения: 16.06.2026).

Анализ структуры затрат предприятий (Табл.1) показывает, что в 2024 г. внутренние затраты организаций составили 4087 млрд руб., внешние - 1828 млрд руб. По сравнению с 2023 г. внутренние расходы выросли с 3153 до 4087 млрд руб., то есть примерно на 29,6%, а внешние - с 1464 до 1828 млрд руб., или на 24,9%. Преобладание внутренних затрат указывает на стремление организаций формировать собственные цифровые компетенции, развивать внутренние ИТ-подразделения, адаптировать информационные системы под специфику бизнеса и снижать зависимость от внешних подрядчиков. Вместе с тем рост внешних расходов свидетельствует о сохранении спроса на специализированные услуги: внедрение программных решений, сопровождение инфраструктуры, облачные сервисы, аудит, консалтинг и техническую поддержку.

Применительно к кибербезопасности эта структура имеет двойственное значение. С одной стороны, развитие внутренних компетенций повышает управляемость защитных процессов и позволяет быстрее реагировать на инциденты. С другой стороны, не каждая организация способна содержать квалифицированную команду информационной безопасности. Поэтому экономически оправданной часто является смешанная модель: критически важные функции контроля, доступа, регламентирования и принятия решений остаются внутри предприятия, а специализированный мониторинг, тестирование защищенности, реагирование на сложные инциденты и экспертный аудит передаются профессиональным поставщикам услуг.

Структура затрат крупных и средних организаций по видам экономической деятельности также демонстрирует существенную неоднородность. В 2024 г. общий объем затрат крупных и средних организаций на внедрение и использование цифровых технологий составил 5244,1 млрд руб. На сектор информации и связи пришлось 1883,2 млрд руб., или около 35,9% совокупного объема. Финансовый сектор сформировал 1223,1 млрд руб., то есть примерно 23,3%. Обрабатывающая промышленность обеспечила 459,2 млрд руб., профессиональная, научная и техническая деятельность - 311,6 млрд руб., транспортировка и хранение - 276,1 млрд руб., государственное управление и социальное обеспечение - 275,4 млрд руб., оптовая и розничная торговля - 256,4 млрд руб.

Таблица 2. Затраты крупных и средних организаций на цифровые технологии в 2024 г. по отдельным видам деятельности

Вид экономической деятельности	Затраты, млрд руб.	Доля в общем объеме, %
Информационные услуги и услуги связи	1883,2	35,9
Финансовый сектор	1223,1	23,3
Обрабатывающая промышленность	459,2	8,8
Профессиональная, научная и техническая деятельность	311,6	5,9

Вид экономической деятельности	Затраты, млрд руб.	Доля в общем объеме, %
Транспортировка и хранение	276,1	5,3
Государственное управление и социальное обеспечение	275,4	5,3
Оптовая и розничная торговля	256,4	4,9

Организации, чей основной вид деятельности связан с информацией и связью, а также с финансовой деятельностью - аккумулировали около 59,2% затрат крупных и средних организаций на цифровые технологии. Такая концентрация закономерна: именно эти отрасли опираются на высоконагруженные цифровые платформы, обработку больших массивов данных, дистанционное обслуживание клиентов, платежные и коммуникационные сервисы. Однако высокая доля цифровых расходов не означает автоматического снижения киберрисков. Напротив, чем сложнее цифровая инфраструктура и шире поверхность атаки, тем выше требования к управлению доступом, непрерывности, резервированию, мониторингу и защите данных.

Важна и структура самих расходов. В 2024 г. среди затрат крупных и средних организаций на цифровые технологии 36,3% приходилось на программные средства, 30,2% - на машины и оборудование, 5,1% - на телекоммуникационные услуги, 2,1% - на цифровой контент и базы данных, 0,2% - на обучение сотрудников, 26,1% - на прочие направления. Низкая доля затрат на обучение персонала является экономически значимым индикатором. Наличии современных программных и технических средств не исключает уязвимости предприятий, если сотрудники не умеют распознавать фишинг, нарушают правила работы с паролями, передают данные через незащищенные каналы, не соблюдают регламенты доступа и не реагируют на признаки инцидента. Следовательно, малая доля образовательных расходов может снижать отдачу от более капиталоемких вложений в оборудование и программное обеспечение.

По данным за 2024 г., 17,0% крупных и средних организаций - пользователей интернета сталкивались с несанкционированными вторжениями в информационные системы, заражениями вредоносными программами или компьютерными атаками. Из них 5,0% организаций сообщили о последствиях в виде блокирования или сбоя информационных ресурсов и оборудования, 3,4% - о полном или частичном уничтожении либо повреждении данных, 2,7% - о нарушении конфиденциальности, то есть об утечке данных.

Практически каждая шестая крупная или средняя организация сталкивается с киберугрозами, следовательно, риск нельзя рассматривать как редкое исключительное событие. Он должен включаться в систему регулярного финансового планирования наряду с валютными, кредитными, рыночными, операционными и правовыми рисками. При этом последствия отличаются по экономической природе. Блокирование ресурсов прежде всего влияет на выручку и производственный цикл. Уничтожение или повреждение данных увеличивает восстановительные затраты и может нарушить учет, складскую логистику, договорное сопровождение и управленческую отчетность. Утечка

конфиденциальной информации несет репутационный, правовой и конкурентный ущерб, который часто проявляется с временным лагом.

Особого внимания заслуживает показатель утечки данных. В гостиницах и общественном питании доля организаций, сообщивших о нарушении конфиденциальности, составила 10,1%, в телекоммуникациях - 9,6%, при среднем уровне 2,7%. Так, для отдельных отраслей риск раскрытия информации может быть более существенным, чем риск физического повреждения данных или сбоя оборудования. Экономические последствия утечки включают не только расходы на устранение инцидента, но и потерю клиентской лояльности, необходимость уведомления заинтересованных лиц, усиление контроля со стороны партнеров, возможное снижение продаж и затраты на репутационное восстановление.

Анализ применяемых средств защиты показывает, что в 2024 г. 64,6% крупных и средних организаций использовали средства строгой аутентификации, 54,7% - программные и аппаратные средства, препятствующие несанкционированному доступу и распространению вредоносных программ, 51,6% - антиспамовые фильтры, 51,0% - шифрование, 42,5% - системы обнаружения вторжений, 37,7% - автоматизированные средства анализа и контроля защищенности информационных систем, 35,8% - корпоративную виртуальную сеть, 31,4% - резервное копирование данных вне территории организации, 7,4% - биометрические средства аутентификации.

Данные свидетельствуют о том, что базовые меры защиты распространены заметно шире, чем инструменты восстановления и углубленного контроля. Между тем именно резервное копирование за пределами территории организации, автоматизированный анализ защищенности и системы обнаружения вторжений особенно важны для сокращения экономического ущерба после атаки.

Финансовая устойчивость организации отражает способность предприятия своевременно исполнять обязательства, поддерживать нормальный оборот капитала, финансировать развитие и сохранять платежеспособность при изменении внешних условий.

Для предприятий целесообразно формировать бюджет для обеспечения информационной и кибербезопасности не по остаточному принципу, а на основе карты рисков. Такая карта должна включать критичные бизнес-процессы, используемые информационные системы, виды обрабатываемых данных, вероятные сценарии угроз, потенциальный ущерб, действующие контрольные процедуры, ответственных лиц и сроки совершенствования защиты.

Проведенный анализ показывает, что обеспечение кибербезопасности предприятий требует междисциплинарного подхода. С одной стороны, оно опирается на технические решения, стандарты защиты, программные средства и инфраструктурные меры. С другой стороны, его экономический смысл раскрывается через снижение вероятности убытков, сохранение ликвидности, защиту денежных потоков, устойчивость договорных отношений и поддержание стоимости бизнеса.

Кибербезопасность предлагается рассматривать как элемент экономической безопасности, который влияет на платежеспособность, рентабельность и риск-профиль организации. Практическая значимость заключается в возможности использования предложенного подхода при формировании бюджета информационной безопасности, оценке целесообразности защитных мероприятий, подготовке карты рисков и разработке внутренних регламентов.

Цифровизация российских предприятий сопровождается существенным ростом затрат на внедрение и использование цифровых технологий. По данным Росстата, в 2019-2024 гг. совокупные затраты организаций на эти цели увеличились более чем вдвое, достигнув 5915 млрд руб. Одновременно статистика угроз показывает, что киберриски имеют массовый характер: в 2024 г. 17,0% крупных и средних организаций - пользователей интернета сталкивались с несанкционированными вторжениями, вредоносными программами или компьютерными атаками, а отдельные отрасли имели значительно более высокий уровень инцидентов.

Экономическая проблема состоит не только в росте расходов на цифровые технологии, но и в необходимости их правильного распределения. Значительная доля затрат направляется на программные средства и оборудование, тогда как обучение сотрудников занимает крайне малое место в структуре расходов. Такой подход создает риск несбалансированной защиты, при которой техническая инфраструктура развивается быстрее, чем организационная культура безопасности и способность персонала предотвращать инциденты и грамотно реагировать на окружающие угрозы.

Кибербезопасность оказывает прямое влияние на финансовую устойчивость предприятия через выручку, расходы, активы, обязательства, стоимость капитала и репутацию. Поэтому ее финансирование должно строиться на риск-ориентированной основе. Оптимальный подход предполагает оценку ожидаемого ущерба, приоритизацию критичных бизнес-процессов, внедрение базового контура защиты, регулярное обучение сотрудников, резервное копирование, мониторинг, готовность к реагированию и включение киберрисков в финансовое стресс-тестирование.

Кибербезопасность предприятия является не вспомогательной ИТ-функцией, а экономическим механизмом сохранения устойчивости предприятия. Ее эффективность определяется не количеством приобретенных технических средств, а способностью снижать вероятность ущерба, обеспечивать непрерывность деятельности и поддерживать финансовую стабильность даже при реализации неблагоприятных цифровых сценариев.

Список источников

1. Докукина А.А. Теоретические основы концепции экономической безопасности предприятия в контексте цифровой трансформации // Экономика, предпринимательство и право. 2023. Т. 13. № 4. С. 1105–1124.
2. Кобышева М.С., Володин А.А., Иванов М.В., Феофилова Т.Ю., Манасерян Т.М. Риски и угрозы экономической безопасности России в условиях

цифровой трансформации // Вестник Алтайской академии экономики и права. 2021. № 2. С. 53–60.
3. Клыков Д.А. О некоторых вопросах экономической безопасности предприятия в условиях цифровизации. В сборнике «За нами будущее: взгляд молодых ученых на инновационное развитие общества». Сборник научных статей 2-й Всероссийской молодежной научной конференции. Курск, 2021. С. 131-134.
4. Мамий Е.А., Рябовол Е.А. Кибератаки как угроза финансовой безопасности компании. В сборнике «Кластеризация цифровой экономики: Глобальные вызовы» Сборник трудов национальной научно-практической конференции с зарубежным участием. 2020. С. 541-546.
5. Оборин М.С. Экономическая безопасность промышленных предприятий в условиях цифровой экономики // Вестник Самарского государственного экономического университета. 2022. № 1 (207). С. 44–54.
6. Шибанова А.А. Информация как производительная сила современного общества/ Журнал прикладных исследований. 2022. Т. 4. № 11. С. 323-326.
7. Использование цифровых технологий организациями по Российской Федерации, субъектам Российской Федерации и видам экономической деятельности : статистические данные. Федеральная служба государственной статистики Российской Федерации официальный сайт. URL:https://rosstat.gov.ru/ storage/mediabank/ikt_org.xlsx (дата обращения: 16.06.2026).

А.В. Штефан[1]

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ КИБЕРАТАКАМ В ШКОЛЬНОЙ СРЕДЕ

Аннотация. В статье раскрывается, как общегосударственные меры противодействия киберпреступности (закреплённые, в частности, в Доктрине информационной безопасности РФ и законодательстве о персональных данных) реализуются непосредственно в школьной среде. Особое внимание уделено практическим аспектам обеспечения информационной безопасности в школе: техническим мерам (антивирусная защита, сегментация сети, резервное копирование), организационным решениям (назначение ответственного, регламенты, аудит) и педагогическим инструментам (обучение цифровой гигиене, адаптация просветительских форматов под разные возрастные группы). В статье приведены типичные для школы сценарии киберугроз (фишинг, заражение через внешние носители, утечки данных) и соответствующие меры защиты.

Ключевые слова: кибертерроризм, противодействие кибертерроризма в школьной среде, дети – жертвы кибертерроризма.

[1] Штефан Алёна Владимировна – доцент кафедры уголовно-правовых дисциплин Федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный университет», кандидат юридических наук, доцент.

Интенсивная цифровизация образовательной среды обусловливает возрастание уязвимости образовательных учреждений к кибератакам, что обусловлено расширением поверхности атаки за счёт интеграции информационных систем (электронных журналов, платформ дистанционного обучения, корпоративных сетей и др.), а также наличием значительного объёма обрабатываемых персональных данных субъектов образовательного процесса.

По мнению В.Н. Сигитовой и И.А. Погодиной, в школьной цифровой среде чаще всего встречаются следующие типы киберугроз:

1. Фишинг и социальная инженерия. Злоумышленники рассылают письма или сообщения якобы от администрации школы или техподдержки, чтобы выманить логины, пароли, данные учётных записей. Ученики и даже педагоги могут неосознанно передать конфиденциальную информацию.

2. Вредоносное программное обеспечение и вирусы. Вредоносные файлы могут попасть в школьную сеть через флешки, письма, непроверенные загрузки. Последствия — от блокировки компьютеров до утечки данных.

3. DDoS-атаки. Массированные запросы к школьным информационным системам могут привести к их недоступности, срыву экзаменов или невозможности вести электронный журнал.

4. Утечки персональных данных. Из-за слабой защиты или ошибок персонала в открытый доступ могут попасть сведения об учениках, родителях, сотрудниках. Это нарушает требования законодательства о персональных данных и несёт репутационные риски.

5. Компрометация учётных записей. Если пароли слабые или используются повторно, злоумышленник может получить доступ к почте, электронным дневникам, внутренним ресурсам школы.

6. Кибербуллинг и манипуляции в цифровой среде. Хотя это не «атака на инфраструктуру», такие явления создают токсичную цифровую атмосферу и требуют профилактических мер со стороны педагогов и психологов[1].

В российских образовательных учреждениях за 2025 год количество утечек увеличилось на 20% - с 15 до 18 инцидентов. Объем скомпрометированных персональных данных также возрос - с 1,4 млн в первом полугодии 2024 года до 1,7 млн в первом полугодии 2025 года[2]

Для защиты школьной цифровой инфраструктуры применяют следующие технические решения: обязательная установка и регулярное обновление антивирусов на всех компьютерах и серверах; разделение школьной сети на сегменты (например, отдельный сегмент для административных систем, отдельный — для учебных классов) снижает риски распространения заражений; регулярные бэкапы журналов, баз данных, важных документов позволяют

[1] Сигитова В. Н., Погодина И. А. Кибербезопасность в школе. анализ угроз в сети интернет и методы защиты персональной информации // Вестник науки. 2025. №1 (82). URL: https://cyberleninka.ru/article/n/kiberbezopasnost-v-shkole-analiz-ugroz-v-seti-internet-i-metody-zaschity-personalnoy-informatsii (дата обращения: 21.05.2026).

[2] Количество утечек в образовательной сфере России выросло. // URL: https://www.comnews.ru/content/241000/2025-0-w36/1008/kolichestvo-utechek-obrazovatelnoy-sfere-rossii-vyroslo (дата обращения: 25.05.2026).

быстро восстановиться после атаки; ограничение прав пользователей и внедрение двухфакторной аутентификации для администраторов и педагогов снижает риск компрометации учётных записей; своевременная установка обновлений операционных систем, браузеров и прикладного ПО закрывает известные уязвимости; ограничение доступа к потенциально опасным сайтам, контроль использования флешек и внешних накопителей.

В 2026 году для защиты цифровой инфраструктуры школ в России применяют целый комплекс технических решений:

1. Видеонаблюдение. Камеры располагают на входах в здания, чтобы контролировать доступ и фиксировать инциденты. В некоторых проектах (например, при оснащении школ в рамках нацпроекта «Цифровая экономика») внедряют системы с видеоаналитикой: нейросети автоматически отслеживают подозрительное поведение — например, попытки проноса запрещённых предметов или выноса материалов. При этом важно: такие системы часто настроены так, чтобы не вести съёмку персональных данных и ответов учеников.

2. Защищённый Wi-Fi. Школы оснащают беспроводными сетями с шифрованием трафика и разграничением прав доступа. Это нужно, чтобы обеспечить безопасный доступ к образовательным платформам и одновременно блокировать подключение неавторизованных устройств.

3. Антивирусная защита и межсетевые экраны. Специализированное ПО сканирует устройства и блокирует вредоносное ПО. Межсетевые экраны фильтруют сетевой трафик, блокируя попытки несанкционированного доступа к внутренним ресурсам.

4. Системы контентной фильтрации. Программное обеспечение блокирует доступ к ресурсам, которые содержат информацию, причиняющую вред здоровью и развитию детей, либо не соответствующую задачам образования. Часто такие системы настраивают на основе реестров безопасных образовательных сайтов.

5. Средства криптографической защиты. Для безопасной передачи данных (например, при интеграции с государственными системами вроде ФГИС «Моя школа» или электронными журналами) применяют средства шифрования.

6. Средства контроля доступа. Реализуют разграничение прав: у разных категорий пользователей (учителя, ученики, технический персонал) разный уровень доступа к ресурсам. Используют системы контроля и управления доступом (СКУД).

7. Централизованное управление учётными записями. Позволяет администраторам легко управлять паролями и правами, а также оперативно отзывать доступ при увольнении сотрудника.

8. Резервное копирование. Критически важные данные регулярно копируют на носители, которые физически отключены от основной сети — это помогает быстро восстановиться в случае атаки или сбоя.

9. Сертификация средств защиты. По требованиям ФСТЭК России средства защиты должны иметь соответствующую сертификацию в зависимости от класса защищённости информационной системы школы[1].

Представленные технические средства работают только в сочетании с продуманной организацией процессов, например, в школе должен быть утверждённый документ, регламентирующий правила работы с данными, использование устройств, действия при инцидентах; регламент чёткие инструкции, кто и как должен действовать при обнаружении подозрительной активности, утечке данных или заражении вирусом; периодические проверки состояния защиты, тестирование на проникновение, анализ журналов событий; своевременное отключение доступа уволенным сотрудникам и выпускникам, запрет на передачу паролей; взаимодействие с внешними экспертами и государственными структурами, а также при необходимости — привлечение специалистов по кибербезопасности и соблюдение требований регуляторов.

В связи с тем, что ученики и педагоги — важное «слабое звено» в защите, необходимы меры по формированию цифровой культуры такие как: 1) регулярные занятия и инструктажи по безопасному поведению в сети: как создавать надёжные пароли, распознавать фишинг, защищать личные данные; 2) интеграция основ кибербезопасности в учебный процесс, то есть введение занятий по информационной безопасности на уроках информатики, обществознания, ОБЖ; 3) использование квестов, симуляций, деловых игр, где учащиеся учатся выявлять угрозы и правильно на них реагировать (например, разбор «кейсов» с подозрительными письмами); 4) информирование родителей о рисках и способах защиты детей в цифровой среде, рекомендации по настройке родительского контроля и обсуждению правил безопасного поведения.

Важно, чтобы ученики не боялись сообщать о подозрительных сообщениях, взломах аккаунтов или случаях травли в сети, для этого можно организовать анонимные каналы обратной связи.

В России хорошим примером просветительской работы является проект «Урок цифры», где школьники разных возрастов знакомятся с основами кибербезопасности в доступной форме[2].

На национальном уровне предупреждение преступности состоит из стратегий и мероприятий, направленных на снижение риска совершения преступлений и нейтрализацию потенциально вредных последствий для частных лиц и общества. Так, в Доктрине информационной безопасности РФ подчёркивается, что информационные технологии стали частью всех сфер жизни, в том числе и образования. Для школы это значит, что цифровая среда (электронный журнал,

[1] Информационная безопасность в образовательных организациях: как выстроить защиту правильно. // URL: https://www.klerk.ru/blogs/fedresurs/678491/ (дата обращения: 25.05.2026).
[2] Урок цифры — всероссийский профориентационный проект в сфере цифровых технологий. // URL: https://урокцифры.рф// (дата обращения: 26.05.2026).

чаты, школьный сайт, Wi-Fi, компьютеры в классах) должна быть защищена так же серьёзно, как и любые другие важные системы[1].

К числу основных мер относятся: принятие законов, стратегий противодействия киберпреступности, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно-просветительская деятельность, создание прочной базы знаний, сотрудничество между органами государственного управления и частным сектором. Безусловно, немаловажным фактором является надлежащее отношение к соответствующей компьютерной информации, которая представляет собой определенный интерес для другого субъекта, ограничение доступа к такой информации при помощи использования лицензированных компьютерных программ и антивирусных софтов для защиты компьютера от незаконного взлома.

Итак, к законодательным мерам противодействия кибератакам в школьной среде необходимо отнести следующее:

1. Федеральный закон № 152-ФЗ «О персональных данных»[2] обязывает школу защищать сведения об учениках и сотрудниках. На практике это выражается в конкретных действиях: в школе есть положение об обработке персональных данных, доступ к базам строго ограничен, а любые утечки должны фиксироваться и расследоваться. Школы как операторы персональных данных обязаны обеспечивать их защиту, вести учёт инцидентов, информировать о нарушениях.

2. Согласно требованиям ФСТЭК и ФСБ для информационных систем, обрабатывающих персональные данные, действуют технические и организационные требования по защите.

3. На уровне учреждения разрабатывают положения об обработке персональных данных, инструкции по информационной безопасности, приказы о назначении ответственных лиц.

Несоблюдение вышеперечисленных мер может привести к административной ответственности и штрафам.

Итак, противодействие кибератакам в школьной среде — это комплексная задача, требующая сочетания технических, организационных, педагогических и правовых мер. Школа должна не только защищать свою цифровую инфраструктуру, но и формировать у учеников навыки безопасного поведения в интернете. Только системный подход, включающий обучение, регламенты, современные технологии и взаимодействие всех участников образовательного процесса, позволит минимизировать риски и создать безопасную цифровую среду для обучения и развития.

---

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.

[2] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 26.07.2026) // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.

Сведения об авторах

Бычкова Екатерина Игоревна – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

Васюков Виталий Федорович – главный научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета имени А.Я. Сухарева, доктор юридических наук, профессор.

Вепрев Сергей Борисович – профессор Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, доктор технических наук, профессор.

Долусов Арсений Андреевич – следователь Демидовского Межрайонного Следственного отдела Следственного Управления Следственного комитета Российской Федерации по Смоленской области, лейтенант юстиции.

Зинуров Максим Рафаэлевич – магистрант Президентской академии (РАНХиГС).

Золотухина Наталья Валерьевна – доцент кафедры управления и психологии следственной деятельности (Высшие академические курсы) факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева.

Зуева Ольга Владимировна – заведующий кафедрой гуманитарных и социально-экономических дисциплин факультета подготовки следователей Московской академии Следственного комитета имени А.Я. Сухарева, кандидат социологических наук, доцент.

Клименко Алексей Иванович – начальник кафедры теории государства и права Московского университета МВД России имени В.Я. Кикотя, ведущий научный сотрудник сектора философии права, истории и теории государства и права Института государства и права РАН, доктор юридических наук профессор.

Лебедева Анна Андреевна – заведующая кафедрой информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева кандидат юридических наук, доцент, полковник юстиции.

Леонтьев Егор Дмитриевич – курсант 1 курса факультета подготовки следователей Московской академии Следственного комитета имени А.Я. Сухарева.

Нестерович Сергей Александрович – доцент кафедры информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества Российского государственного социального университета, кандидат технических наук, доцент.

Опальский Александр Павлович – профессор Института государственной службы и управления Президентской академии (РАНХиГС), д-р экономических наук, профессор.

Османова Надежда Валерьевна – декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент.

Правкина Ирина Николаевна – доцент кафедры правовых дисциплин Московского экономического института, кандидат юридических наук, доцент.

Прорвич Владимир Антонович – профессор-исследователь Департамента уголовного права, процесса и криминалистики НИУ ВШЭ, доктор юридических наук, доктор технических наук, профессор, почётный профессор Московской академии Следственного комитета имени А.Я. Сухарева.

Саркисян Армен Жораевич – декан факультета повышения квалификации Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент, подполковник юстиции.

Скобелин Сергей Юрьевич – доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии Следственного комитета имени А.Я. Сухарева, кандидат юридических наук, доцент полковник юстиции.

Скобелина Людмила Анатольевна – доцент кафедры государственно-правовых дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат исторических наук, капитан юстиции.

Строкова Татьяна Алексеевна – доцент кафедры гуманитарных и социально-экономических дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат политических наук, майор юстиции.

Титов Андрей Александрович – начальник отдела УРОПД Следственного департамента МВД России, кандидат юридических наук.

Фурсова Софья Равилевна – курсант 5 курса факультета подготовки следователей Московской академии Следственного комитета имени А.Я. Сухарева.

Цыплакова Алёна Дмитриевна – старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Московского государственного университета международных отношений МИД России (МГИМО), научный сотрудник Центра ИИ МГИМО МИД России.

Шибанова Анна Анатольевна – старший преподаватель кафедры гуманитарных и социально-экономических дисциплин Московской академии Следственного комитета имени А.Я. Сухарева, кандидат экономических наук, майор юстиции.

Штефан Алена Владимировна – доцент кафедры уголовно-правовых дисциплин Института права Челябинского государственного университета, кандидат юридических наук, доцент.

Оглавление

ПРАВОВЫЕ АСПЕКТЫ БОРЬБЫ С ПРОЯВЛЕНИЯМИ КИБЕРЭКСТРЕМИЗМА И ТЕРРОРИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Всероссийский круглый стол, посвященный памяти почетного профессора Московской академии Следственного комитета имени А.Я. Сухарева, почетного сотрудника Следственного комитета Российской Федерации Василия Васильевича Бычкова

Москва, 29 мая 2026 г.

Подписано в печать: 25.08.2026
Формат 60x90 1/16
Усл. печ. л. 6,4
Тираж 100 экз.
Компьютерная верстка, техн. редактирование –
А.Ж. Саркисян, И.Д. Нестерова
Заказ № 552

Отпечатано в типографии Московской академии
Следственного комитета имени А.Я. Сухарева,
ул. Врубеля, д. 12