УДК 34 **DOI: 10.34670/AR.2025.40.47.029**

К вопросу о минимизации последствий преступности в традиционной и цифровой образовательной среде

Сидорова Екатерина Закариевна

Кандидат юридических наук, доцент,
заместитель начальника кафедры уголовного права и криминологии,
Восточно-Сибирский институт МВД России,
664074, Российская Федерация, Иркутск, ул. Лермонтова, 110;
e-mail: ketrik6@mail.ru

Аннотация

Современная образовательная экосистема, одновременно функционирующая в офлайн- и онлайн-режимах, сталкивается с трансформацией преступности и ростом латентной виктимизации, что делает минимизацию последствий противоправных посягательств междисциплинарной задачей, выходящей за рамки «физической охраны» учреждений. Целью статьи является выявление направлений совершенствования законодательства и правоприменения для снижения ущерба от преступности в традиционной и цифровой образовательной среде. Эмпирическую и нормативную основу исследования составили положения УК РФ, Федерального закона «Об образовании в Российской Федерации» и подзаконных актов о безопасности объектов образования, данные МВД РФ и Генеральной прокуратуры РФ о преступности несовершеннолетних и преступлениях в отношении несовершеннолетних за 2018–2023 гг., материалы судебной практики по уголовным и гражданским делам о возмещении вреда, а также результаты опросов участников образовательного процесса; применены диалектический метод, формально-юридический и сравнительно-правовой анализ, контент-анализ судебных решений, криминологическое прогнозирование рисков, связанных с цифровизацией и использованием ИИ. Показано, что угрозы приобретают гибридный характер: офлайн-конфликты эскалируют в цифровых коммуникациях, а онлайн-травля и вовлечение в деструктивные сообщества материализуются в насильственных инцидентах; в «традиционном» сегменте сохраняются кражи, вымогательства и причинение вреда здоровью, но они все чаще сопряжены с доступом к устройствам и шантажом персональными данными. Отдельно анализируется риск вооруженных нападений на учебные заведения и значение квалификации в террористическом контексте, а также ограничения профилактики, основанной только на металлодетекторах и ЧОП без мониторинга цифровой среды. В цифровом контуре доминируют кибербуллинг и посягательства на честь и достоинство, однако отсутствие специального состава в УК РФ осложняет доказывание и повышает безнаказанность; существенную опасность представляют утечки персональных данных с последующим мошенничеством, «инфоцыганские» схемы и цифровизация коррупционных практик. Делается вывод о необходимости перехода от реактивной модели к проактивной: закрытия правовых лакун (в том числе в части онлайн-надзора школ), усиления требований к операторам данных,

развития служб медиации, обучения цифровой гигиене и выстраивания межведомственного обмена информацией при соблюдении режима персональных данных.

Для цитирования в научных исследованиях

Сидорова Е.З. К вопросу о минимизации последствий преступности в традиционной и цифровой образовательной среде // Вопросы российского и международного права. 2025. Том 15. № 11А. С. 248-258. DOI: 10.34670/AR.2025.40.47.029

Ключевые слова

Преступность в образовательной среде, кибербезопасность, кибербуллинг, персональные данные, виктимологическая профилактика.

Введение

Современная образовательная среда, представляющая собой сложный социокультурный механизм, в последние десятилетия претерпевает фундаментальные трансформации, обусловленные не только педагогическими инновациями, но и глобальной цифровизацией общества, что неизбежно влечет за собой видоизменение структуры преступности и требует переосмысления подходов к обеспечению безопасности участников образовательного процесса. Традиционно учебные заведения воспринимались как зоны повышенной социальной ответственности и относительной безопасности, однако криминологическая статистика последних лет свидетельствует о тревожной тенденции роста девиантного и делинквентного поведения, причем вектор угроз смещается от банальных имущественных посягательств к сложным формам насилия и киберпреступности. Актуальность исследования детерминирована необходимостью комплексного анализа правовых и криминологических аспектов защиты личности обучающихся и педагогов в условиях гибридной реальности, где физическое пространство школы или университета неразрывно связано с виртуальными коммуникациями [Гареев, 2021]. Проблема минимизации последствий преступности в данной сфере перестала быть исключительно задачей правоохранительных органов и перешла в плоскость междисциплинарного дискурса, затрагивающего вопросы конституционного права на образование, безопасных условий обучения и защиты персональных данных. Следует отметить, что виктимизация участников образовательных отношений в цифровом пространстве часто носит латентный характер, что затрудняет своевременное выявление и пресечение противоправных деяний, создавая иллюзию безнаказанности для правонарушителей [Измайлова, 2020].

Вместе с тем, стремительное развитие дистанционных образовательных технологий, ставшее безальтернативным ответом на пандемические вызовы, обнажило серьезные пробелы в нормативно-правовом регулировании кибербезопасности образовательных платформ и этике цифрового взаимодействия. Если в традиционной среде основными криминогенными факторами выступали недостатки охраны, слабая воспитательная работа и социально-бытовая неустроенность, то в цифровой среде на первый план выходят анонимность, трансграничность и возможность автоматизированного распространения деструктивного контента. Государственная политика в сфере противодействия преступности должна учитывать эту дуальность, разрабатывая механизмы, способные эффективно функционировать как в офлайн, так и в онлайн-режимах [Диева, Магомедова, 2025]. Игнорирование специфики цифровой виктимности может привести к необратимым психологическим и социальным последствиям для

подрастающего поколения, что подтверждается ростом числа суицидальных проявлений и случаев вовлечения молодежи в экстремистскую деятельность через сеть Интернет. Таким образом, цель настоящей работы заключается в выявлении ключевых направлений совершенствования правоприменительной практики и законодательства для минимизации ущерба от преступных посягательств в образовательной экосистеме, что требует глубокого погружения в сущность криминогенных процессов [Сидорова, 2024].

Материалы и методы исследования

Методологическую основу настоящего исследования составил диалектический метод познания социально-правовых явлений, позволивший рассмотреть преступность в образовательной среде как динамично развивающуюся систему, детерминированную комплексом социальных, экономических и технологических факторов. В работе широко использовались формально-юридический и сравнительно-правовой методы, благодаря которым был проведен детальный анализ положений Уголовного кодекса Российской Федерации, Федерального закона «Об образовании в Российской Федерации», а также ряда подзаконных актов, регламентирующих вопросы безопасности и антитеррористической защищенности объектов образования. Особое внимание уделялось контент-анализу судебной практики по уголовным и гражданским делам, связанным с возмещением вреда, причиненного в стенах учебных заведений или в ходе дистанционного обучения, что позволило выявить реальные проблемы квалификации деяний и доказывания вины ответственных лиц [Четверикова, 2020]. Эмпирическую базу исследования составили статистические данные Министерства внутренних дел РФ и Генеральной прокуратуры РФ о состоянии преступности несовершеннолетних и в отношении несовершеннолетних за период с 2018 по 2023 год, а также результаты социологических опросов участников образовательного процесса относительно их восприятия уровня безопасности.

Кроме того, для достижения объективности выводов применялся метод криминологического прогнозирования, направленный на выявление потенциальных угроз, связанных с внедрением искусственного интеллекта и нейросетей в образовательный процесс. Были изучены материалы правоприменительной практики, касающиеся случаев кибербуллинга, скулшутинга и мошенничества в образовательной сфере, что позволило систематизировать типичные способы совершения преступлений и выработать рекомендации по их профилактике [Комаров, 2020]. Анализ нормативной базы включал в себя оценку эффективности действующих санитарно-эпидемиологических требований и стандартов информационной безопасности, применяемых в школах и вузах, с точки зрения их способности противостоять современным криминальным вызовам. Важным элементом методологии стало изучение зарубежного опыта правового регулирования безопасности в школах, что позволило сопоставить отечественные подходы с международными стандартами и выявить возможности для рецепции наиболее успешных правовых институтов, адаптированных к российским реалиям.

Результаты и обсуждение

Анализ современного состояния преступности в образовательной среде позволяет констатировать наличие устойчивой тенденции к гибридизации угроз, когда конфликт, зародившийся в стенах учебного заведения, находит свое продолжение и эскалацию в

виртуальном пространстве, и наоборот, что создает значительные трудности для правовой квалификации деяний. Традиционные формы преступности, такие как кражи (ст. 158 УК РФ), вымогательства (ст. 163 УК РФ) и причинение вреда здоровью различной степени тяжести, по-прежнему составляют значительную долю в структуре правонарушений, совершаемых на территории образовательных организаций, однако их характер претерпевает изменения под воздействием фактора цифровизации [Поломошнов, Колышкина, 2024]. Например, хищение имущества все чаще сопряжено с неправомерным доступом к электронным устройствам жертвы и последующим шантажом с использованием личной информации, хранящейся на гаджетах. Это актуализирует вопрос о необходимости более широкого применения совокупности норм уголовного права, охватывающих как имущественные составы, так и преступления против неприкосновенности частной жизни и тайны переписки. Судебная практика показывает, что правоприменители зачастую сталкиваются с проблемой разграничения мелкого хулиганства и преступлений экстремистской направленности, совершаемых молодежными группировками на территории школ, что требует четких разъяснений со стороны высших судебных инстанций.

Особую озабоченность вызывает феномен вооруженных нападений на учебные заведения, известный как «скулшутинг», который, к сожалению, перестал быть исключительно зарубежной проблемой и приобрел черты системной угрозы для российской образовательной системы. Правовая оценка таких действий требует не только применения статей об убийстве (ст. 105 УК РФ), но и квалификации деяний как террористических актов (ст. 205 УК РФ) в случаях, когда целью нападения является дестабилизация деятельности органов власти или устрашение населения [Анцупов, Тимофеев, Акимов, 2020]. Верховный Суд РФ признал движение «Колумбайн» террористическим, что дало правоохранительным органам дополнительные инструменты для пресечения деятельности организаторов и подстрекателей подобных атак на стадии приготовления. Однако, как показывает анализ уголовных дел, профилактические меры, основанные исключительно на усилении физической охраны (металлодетекторы, ЧОП), оказываются недостаточно эффективными без глубокой оперативной работы в цифровой среде, где формируются деструктивные сообщества. Важно отметить, что ответственность за обеспечение безопасности лежит не только на правоохранителях, но и на администрации учебных заведений, чье бездействие или халатность (ст. 293 УК РФ) нередко становятся условиями, способствующими совершению тяжких преступлений.

В цифровом сегменте образовательной среды доминирующее положение занимают преступления против чести и достоинства, а также половой неприкосновенности несовершеннолетних, совершаемые с использованием информационно-телекоммуникационных сетей. Кибербуллинг, или травля в Интернете, представляет собой серьезную проблему, которая, несмотря на высокую общественную опасность, не имеет прямого закрепления в Уголовном кодексе РФ как отдельный состав преступления, что вынуждает юристов прибегать к нормам о клевете (ст. 128.1 УК РФ) или угрозе убийством (ст. 119 УК РФ) [Хамидуллин, Чуб, 2023]. Однако специфика цифрового следа и возможность анонимного воздействия делают процесс доказывания по таким делам крайне затруднительным, требующим проведения сложных лингвистических и компьютерно-технических экспертиз. Отсутствие специального состава «киберпреследования» приводит к тому, что значительная часть виновных лиц избегает уголовной ответственности, ограничиваясь мерами дисциплинарного или административного воздействия, которые не способны в полной мере восстановить нарушенные права жертвы и компенсировать моральный вред. Необходимо также учитывать, что психологическое насилие

в сети часто становится прелюдией к доведению до самоубийства (ст. 110 УК РФ), расследование которых требует особого профессионализма и понимания психологии подросткового возраста.

Еще одним значимым аспектом является защита персональных данных участников образовательного процесса, массовая утечка которых стала реальностью в условиях перехода на дистанционное обучение и использование облачных сервисов. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание вредоносных программ (ст. 273 УК РФ) в контексте образовательных платформ могут привести не только к срыву учебного процесса, но и к использованию полученных данных для совершения мошеннических действий в отношении родителей и педагогов [Новиков, 2025]. Практика показывает, что многие образовательные учреждения не уделяют должного внимания технической защите информации, используя уязвимое программное обеспечение и пренебрегая правилами цифровой гигиены. Это создает благоприятную почву для фишинговых атак и социальной инженерии, жертвами которых становятся наименее защищенные участники образовательных отношений. Введение административной ответственности за нарушение законодательства в области персональных данных (ст. 13.11 КоАП РФ) является лишь первым шагом, требующим дополнения в виде ужесточения требований к операторам данных в сфере образования и введения оборотных штрафов за утечки информации.

Правовой анализ ситуаций, связанных с вовлечением несовершеннолетних в совершение противоправных действий через образовательную среду, выявляет проблему недостаточной эффективности института профилактики безнадзорности и правонарушений. Существующая система профилактического учета часто носит формальный характер и не охватывает группы риска, которые не проявляют явной девиантности в реальной жизни, но активно участвуют в деструктивных интернет-сообществах [Рыбокитова, Польшиков, 2024]. Законодатель предпринимает попытки криминализации действий, направленных на склонение к потреблению наркотических средств или совершению действий, опасных для жизни, через Интернет (ст. 230, 151.2 УК РФ), однако правоприменительная практика сталкивается с проблемой экстерриториальности преступников. Многие организаторы «групп смерти» или наркомагазинов находятся за пределами юрисдикции РФ, что делает невозможным их привлечение к ответственности без эффективного международного сотрудничества, которое в настоящее время затруднено геополитической обстановкой. В этой связи возрастает роль внутринациональных механизмов блокировки контента и превентивной работы с молодежью на уровне образовательных организаций.

Вопросы гражданско-правовой ответственности образовательных учреждений за вред, причиненный обучающимся в результате преступных посягательств, также требуют детального рассмотрения через призму ст. 1068 и 1073 ГК РФ. Суды, как правило, исходят из презумпции вины образовательного учреждения в случае причинения вреда малолетнему во время нахождения под надзором школы, если не будет доказано, что вред возник не по их вине [Чекушов и др., 2020]. Однако в условиях цифрового обучения границы «надзора» размываются: несет ли школа ответственность за кибербуллинг, происходящий в школьном чате во внеучебное время? Судебная практика по данному вопросу пока не сформировала единого подхода, что создает правовую неопределенность. Некоторые суды полагают, что образовательное учреждение обязано модерировать созданные им ресурсы, другие же считают, что ответственность полностью лежит на законных представителях несовершеннолетних. Представляется, что необходимо законодательное закрепление статуса официальных каналов

коммуникации образовательной организации и регламентация обязанностей по их администрированию.

Проблема распространения криминальной субкультуры (АУЕ и прочие) в образовательной среде, несмотря на запрет соответствующих движений, остается острой и трансформируется в новые формы подражания криминальным авторитетам через социальные сети. Популяризация тюремной романтики и насилия среди школьников подрывает основы правосознания и способствует формированию правового нигилизма [Вифлеемский, 2020]. Борьба с этим явлением не может ограничиваться только репрессивными мерами; необходима системная работа по дегероизации преступного мира и предложению альтернативных социальных лифтов. Важную роль здесь играют школьные службы медиации (примирения), которые, согласно Федеральному закону № 273-ФЗ, должны способствовать урегулированию конфликтов и профилактике правонарушений. Однако на практике такие службы часто существуют лишь на бумаге или не обладают достаточным авторитетом и профессиональными компетенциями для разрешения серьезных конфликтов, перерастающих в уголовно наказуемые деяния.

Отдельного внимания заслуживает вопрос квалификации мошенничества в сфере образовательных услуг, когда под видом обучающих курсов или программ повышения квалификации реализуются так называемые «инфоцыганские» продукты, не имеющие образовательной ценности, или выдаются документы государственного образца без соответствующих лицензий (ст. 159, 327 УК РФ). Подобные действия наносят ущерб не только финансовому благосостоянию граждан, но и репутации системы образования в целом, девальвируя значимость дипломов и сертификатов [Бабушкина, 2023]. Сложность расследования таких преступлений заключается в разграничении гражданско-правовых отношений, связанных с ненадлежащим исполнением договора оказания услуг, и уголовно наказуемого обмана. Правоприменителю необходимо доказывать наличие умысла на хищение средств еще на стадии заключения договора, что требует анализа финансово-хозяйственной деятельности организации и содержания образовательных программ.

Следует также отметить латентность коррупционных преступлений в образовательной среде, которые, хотя и не сопряжены с насилием, создают предпосылки для деградации качества образования и формирования у молодежи искаженных представлений о социальной справедливости. Взяточничество (ст. 290, 291 УК РФ) и мелкое взяточничество (ст. 291.2 УК РФ) при сдаче экзаменов и зачетов переходят в цифровой формат: передача средств осуществляется через криптовалюты или электронные кошельки, что усложняет фиксацию преступления [Сморгунова, 2023]. Минимизация последствий такой преступности требует внедрения прозрачных цифровых систем контроля знаний и процедур поступления, исключающих субъективный фактор. Вместе с тем, чрезмерная цифровизация контроля не должна нарушать права обучающихся на личную тайну, что требует соблюдения баланса интересов.

В рамках анализа мер по минимизации последствий преступности нельзя не упомянуть о необходимости совершенствования института необходимой обороны (ст. 37 УК РФ) применительно к ситуациям нападения на образовательные учреждения. Педагоги и сотрудники охраны часто оказываются в ситуации правовой неопределенности относительно пределов допустимой самообороны при отражении групповых или вооруженных нападений подростков. Страх превышения пределов необходимой обороны может парализовать волю к сопротивлению, что приводит к увеличению числа жертв. В юридической литературе обоснованно поднимается вопрос о необходимости специальной подготовки персонала школ к

действиям в чрезвычайных ситуациях и правовой регламентации их действий по защите жизни и здоровья обучающихся [Степанова, 2025]. Судебная практика должна более четко ориентировать суды на оправдательный уклон в случаях, когда действия обороняющегося были направлены на спасение детей от реальной угрозы.

Таким образом, анализ правовых аспектов преступности в образовательной среде показывает, что действующее законодательство, хотя и содержит необходимый инструментарий для борьбы с преступностью, требует точечной настройки под реалии цифрового общества. Пробелы в регулировании кибербуллинга, недостаточная эффективность профилактических мер и сложности с квалификацией гибридных угроз создают риски для безопасности образовательного пространства. Минимизация последствий преступности невозможна без интеграции правовых, технических и педагогических мер в единую стратегию безопасности. Необходимо переходить от реактивной модели борьбы с преступностью, основанной на наказании виновных постфактум, к проактивной модели, ориентированной на раннее выявление криминогенных факторов и устранение причин виктимизации.

Важно подчеркнуть, что ответственность за преступления, совершенные несовершеннолетними в образовательной среде, не должна рассматриваться изолированно от ответственности родителей за неисполнение обязанностей по воспитанию (ст. 5.35 КоАП РФ, ст. 156 УК РФ). Практика показывает прямую корреляцию между семейным неблагополучием и криминальной активностью подростков. В то же время, чрезмерное ужесточение санкций в отношении родителей без предоставления им реальной помощи и поддержки со стороны государства может иметь обратный эффект. Нужен баланс карательных и восстановительных мер правосудия, особенно когда речь идет о впервые оступившихся подростках, для которых клеймо судимости может стать фактором, толкающим на путь рецидива.

Завершая раздел анализа и обсуждения, стоит указать на значимость межведомственного взаимодействия. Разрозненность действий полиции, комиссий по делам несовершеннолетних, органов опеки и администраций школ часто приводит к тому, что тревожные сигналы о поведении подростка игнорируются до момента совершения им тяжкого преступления. Создание единых цифровых платформ обмена информацией о детях, находящихся в социально опасном положении, при строгом соблюдении законодательства о защите данных, могло бы стать эффективным инструментом ранней профилактики [Саруханян, Вячистов, 2025]. Юридическая наука должна предложить оптимальные правовые модели такого взаимодействия, исключающие бюрократические проволочки и дублирование функций.

Заключение

Подводя итог проведенному исследованию проблем минимизации последствий преступности в традиционной и цифровой образовательной среде, следует констатировать, что современная парадигма безопасности образовательного пространства требует кардинального пересмотра подходов к правовому регулированию и правоприменению. Очевидно, что существующая нормативная база, сформированная преимущественно в доцифровую эпоху, испытывает определенные трудности в адаптации к высокотехнологичным рискам и гибридным угрозам, характеризующимся трансграничностью, латентностью и высокой скоростью распространения. Проведенный анализ позволяет утверждать, что эффективность противодействия преступным посягательствам в учебных заведениях и на образовательных онлайн-платформах напрямую зависит от способности государства и общества выстроить

комплексную систему защиты, в которой императивные нормы уголовного права органично сочетаются с гибкими инструментами предупредительного воздействия, техническими средствами защиты информации и методами виктимологической профилактики. При этом ключевым вектором развития должно стать не столько ужесточение репрессивного аппарата, сколько создание правовых условий для неизбежности ответственности и своевременного купирования криминогенных факторов на ранних стадиях их возникновения.

Безусловно, решение обозначенных проблем лежит в плоскости гармонизации законодательства, регламентирующего образовательную деятельность, информационную безопасность и уголовное судопроизводство, с целью устранения правовых лакун, позволяющих правонарушителям избегать ответственности за деяния, совершаемые в цифровой среде. Необходимо признать, что человеческий фактор, выражающийся в правовой грамотности педагогов, бдительности родителей и уровне правосознания обучающихся, остается фундаментальным элементом системы безопасности, который невозможно полностью заменить техническими средствами контроля или алгоритмическими решениями. Следовательно, стратегической задачей является формирование культуры безопасности и цифровой гигиены, подкрепленной четкими и понятными правовыми механизмами реагирования на любые проявления насилия, дискриминации или мошенничества. Только системный, научно обоснованный и практически ориентированный подход, учитывающий динамику изменения преступности, позволит минимизировать негативные последствия криминальных проявлений и обеспечить конституционные гарантии на безопасное и качественное образование для будущих поколений.

Библиография

1. Четверикова О.Н. Интеллектуальный регресс как оборотная сторона «цифровой школы» // Народное образование. 2020. № 1 (1478). С. 31-44.
2. Чекушов А.А., Гордеевцев Е.И., Чирков М.А., Чистяков М.С. Преступность в цифровой среде как фактор, ограничивающий развитие информационных технологий // Вестник Владимирского юридического института. 2020. № 1 (54). С. 125-133.
3. Гареев М.Ф. Правовой и криминологический анализ внедрения и реализации "цифровой биографии" школьника // Юридическая мысль. 2021. № 2 (122). С. 90-100.
4. Новиков Д.О. Цифровая культура и цифровая грамотность личности как элементы личной, общественной и национальной безопасности: постановка проблемы // Вестник Прикамского социального института. 2025. № 1 (100). С. 129-139.
5. Сидорова Е.З. Об особенностях политики в сфере предупреждения преступности в образовательной среде // Академическая мысль. 2024. № 3 (28). С. 55-58.
6. Вифлеемский А.Б. Обнуление школы // Народное образование. 2020. № 6 (1483). С. 21-33.
7. Анцупов И.С., Тимофеев В.А., Акимов А.Н. О проблемах повышения цифровой грамотности молодежи: генезис проблемы, подходы психолого-педагогической науки // Проблемы современного педагогического образования. 2020. № 67-4. С. 31-34.
8. Диева М.Г., Магомедова З.А. Особенности детерминации преступности среди учащихся образовательных учреждений в условиях цифрового мира // Вестник Чеченского государственного университета им. А.А. Кадырова. 2025. № 2 (58). С. 154-161.
9. Комаров И.М. Проблемы цифровизации в криминалистике (печатается в продолжение исследования: Комаров И.М. Цифровая криминалистика - давно назревшая проблема // Библиотека криминалиста. Научный журнал. М.: МГУ им. М.В. Ломоносова. 2(37) 2018. С. 161-171) // Экономические и социально-гуманитарные исследования. 2020. № 4 (28). С. 87-90.
10. Бабушкина П.А. Роль кибер-криминалистики в образовании // Научный аспект. 2023. Т. 7. № 9. С. 793-797.
11. Хамидуллин Р.С., Чуб Д.С. Политика кибербезопасности современного образования // Право и политика. 2023. № 4. С. 48-60.
12. Измайлова М.А. Цифровая зависимость и цифровая культура: поиск решений в образовании // Инновации в образовании. 2020. № 4. С. 50-64.

13. Сморгунова В.Ю. Цифровая трансформация образования и проблемы информационной безопасности детей и подростков // Ежегодник российского образовательного законодательства. 2023. Т. 18. № 23. С. 40-56.
14. Рыбокитова Ж.И., Польшиков А.В. Студенческая преступность в сфере информационных и телекоммуникационных технологий: состояние, тенденции и меры предупреждения // Вестник Воронежского института МВД России. 2024. № 2. С. 256-261.
15. Поломошнов А.Ф., Колышкина М.С. Цифровизация образования как тренд: за и против // Вестник Калмыцкого университета. 2024. № 4 (64). С. 153-160.
16. Степанова Н.К. Зарубежный опыт эффективной профилактики киберпреступности в отношении несовершеннолетних правоохранительными органами // Управление образованием: теория и практика. 2025. № 8-1. С. 281-293.
17. Саруханян Е.О., Вячистов В.М. Влияние внедрения информационных технологий в вузах на психологическое благополучие преподавателей высшей школы // Управление образованием: теория и практика. 2025. № 9-2. С. 78-87.

On the Question of Minimizing the Consequences of Crime in Traditional and Digital Educational Environments

Ekaterina Z. Sidorova

PhD in Legal Sciences, Associate Professor,
Deputy Head of the Department of Criminal Law and Criminology,
East Siberian Institute of the Ministry of Internal Affairs of Russia,
664074, 110, Lermontova str., Irkutsk, Russian Federation;
e-mail: ketrik6@mail.ru

Abstract

The modern educational ecosystem, simultaneously functioning in offline and online modes, faces the transformation of crime and an increase in latent victimization, making the minimization of the consequences of unlawful acts an interdisciplinary task that extends beyond the "physical security" of institutions. The aim of the article is to identify directions for improving legislation and law enforcement to reduce the damage from crime in traditional and digital educational environments. The empirical and normative basis of the study consisted of provisions of the Criminal Code of the Russian Federation, the Federal Law "On Education in the Russian Federation" and subordinate acts on the security of educational facilities, data from the Ministry of Internal Affairs of Russia and the Prosecutor General's Office of Russia on juvenile delinquency and crimes against minors for 2018–2023, materials of judicial practice on criminal and civil cases regarding compensation for harm, as well as results from surveys of participants in the educational process; the dialectical method, formal-legal and comparative-legal analysis, content analysis of court decisions, criminological forecasting of risks associated with digitalization and the use of AI were applied. It is shown that threats acquire a hybrid character: offline conflicts escalate in digital communications, while online bullying and involvement in destructive communities materialize in violent incidents; in the "traditional" segment, theft, extortion, and harm to health persist, but they are increasingly associated with access to devices and blackmail using personal data. The risk of armed attacks on educational institutions and the significance of qualification in a terrorist context are separately analyzed, as well as the limitations of prevention based solely on metal detectors and private security companies without monitoring the digital environment. In the digital realm, cyberbullying and attacks on honor and dignity dominate; however, the absence of a specific

criminal offense in the Criminal Code of the Russian Federation complicates proof and increases impunity; significant dangers are posed by personal data leaks followed by fraud, "infogypsy" schemes, and the digitalization of corrupt practices. It is concluded that a transition from a reactive model to a proactive one is necessary: closing legal gaps (including regarding online supervision of schools), strengthening requirements for data operators, developing mediation services, teaching digital hygiene, and building interagency information exchange while complying with personal data regulations.

For citation

Sidorova E.Z. (2025) K voprosu o minimizatsii posledstviy prestupnosti v traditsionnoy i tsifrovoy obrazovatel'noy srede [On the Question of Minimizing the Consequences of Crime in Traditional and Digital Educational Environments]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (11A), pp. 248-258. DOI: 10.34670/AR.2025.40.47.029

Keywords

Crime in the educational environment, cybersecurity, cyberbullying, personal data, victimological prevention.

References

1. Chetverikova, O.N. (2020). Intellektual'nyi regress kak oborotnaia storona «tsifrovoi shkoly» [Intellectual regression as the flip side of the "digital school"]. *Narodnoe obrazovanie* [Public Education], (1 (1478)), 31–44.
2. Chekushov, A.A., Gordeevtsev, E.I., Chirkov, M.A., & Chistiakov, M.S. (2020). Prestupnost' v tsifrovoi srede kak faktor, ogranichivaiushchii razvitie informatsionnykh tekhnologii [Crime in the digital environment as a factor limiting the development of information technologies]. *Vestnik Vladimirskogo iuridicheskogo instituta* [Bulletin of the Vladimir Law Institute], (1 (54)), 125–133.
3. Gareev, M.F. (2021). Pravovoi i kriminologicheskii analiz vnedreniia i realizatsii "tsifrovoi biografii" shkol'nika [Legal and criminological analysis of the introduction and implementation of a "digital biography" of a schoolchild]. *Iuridicheskaia mysl'* [Legal Thought], (2 (122)), 90–100.
4. Novikov, D.O. (2025) Tsifrovaia kul'tura i tsifrovaia gramotnost' lichnosti kak elementy lichnoi, obshchestvennoi i natsional'noi bezopasnosti: postanovka problemy [Digital culture and digital literacy of an individual as elements of personal, public and national security: problem statement]. *Vestnik Prikamskogo sotsial'nogo instituta* [Bulletin of the Prikamsky Social Institute], (1 (100)), 129–139.
5. Sidorova, E.Z. (2024). Ob osobennostiakh politiki v sfere preduprezhdeniia prestupnosti v obrazovatel'noi srede [On the features of policy in the field of crime prevention in the educational environment]. *Akademicheskaia mysl'* [Academic Thought], (3 (28)), 55–58.
6. Vifleemskii, A.B. (2020). Obnulenie shkoly [Zeroing out the school]. *Narodnoe obrazovanie* [Public Education], (6 (1483)), 21–33.
7. Antsupov, I.S., Timofeev, V.A., & Akimov, A.N. (2020). O problemakh povysheniia tsifrovoi gramotnosti molodezhi: genezis problemy, podkhody psikhologo-pedagogicheskoi nauki [On the problems of increasing digital literacy of youth: genesis of the problem, approaches of psychological and pedagogical science]. *Problemy sovremennogo pedagogicheskogo obrazovaniia* [Problems of Modern Pedagogical Education], (67-4), 31–34.
8. Dieva, M.G., & Magomedova, Z.A. (2025) Osobennosti determinatsii prestupnosti sredi uchashchikhsia obrazovatel'nykh uchrezhdenii v usloviiakh tsifrovogo mira [Features of the determination of crime among students of educational institutions in the digital world]. *Vestnik Chechenskogo gosudarstvennogo universiteta im. A.A. Kadyrova* [Bulletin of the Chechen State University named after A.A. Kadyrov], (2 (58)), 154–161.
9. Komarov, I.M. (2020). Problemy tsifrovizatsii v kriminalistike (pechataetsia v prodolzhenie issledovaniia: Komarov I.M. Tsifrovaia kriminalistika – davno nazrevshaia problema // Biblioteka kriminalista. Nauchnyi zhurnal. M.: MGU im. M.V. Lomonosova. 2(37) 2018. S. 161-171) [Problems of digitalization in forensics (published as a continuation of the study: Komarov I.M. Digital forensics – a long-overdue problem // Library of a Criminalist. Scientific Journal. M.: Lomonosov Moscow State University. 2(37) 2018. Pp. 161-171)]. *Ekonomicheskie i sotsial'no-gumanitarnye issledovaniia* [Economic and Socio-Humanitarian Research], (4 (28)), 87–90.

10. Babushkina, P.A. (2023). Rol' kiber-kriminalistiki v obrazovanii [The role of cyber-forensics in education]. *Nauchnyi aspekt* [Scientific Aspect], 7(9), 793–797.
11. Khamidullin, R.S., & Chub, D.S. (2023). Politika kiberbezopasnosti sovremennogo obrazovaniia [Cybersecurity policy of modern education]. *Pravo i politika* [Law and Politics], (4), 48–60.
12. Izmailova, M.A. (2020). Tsifrovaia zavisimost' i tsifrovaia kul'tura: poisk reshenii v obrazovanii [Digital addiction and digital culture: searching for solutions in education]. *Innovatsii v obrazovanii* [Innovations in Education], (4), 50–64.
13. Smorgunova, V.Iu. (2023). Tsifrovaia transformatsiia obrazovaniia i problemy informatsionnoi bezopasnosti detei i podrostkov [Digital transformation of education and problems of information security of children and adolescents]. *Ezhegodnik rossiiskogo obrazovatel'nogo zakonodatel'stva* [Yearbook of Russian Educational Legislation], 18(23), 40–56.
14. Rybokitova, Zh.I., & Polishikov, A.V. (2024). Studencheskaia prestupnost' v sfere informatsionnykh i telekommunikatsionnykh tekhnologii: sostoianie, tendentsii i mery preduprezhdeniia [Student crime in the field of information and telecommunication technologies: state, trends and prevention measures]. *Vestnik Voronezhskogo instituta MVD Rossii* [Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia], (2), 256–261.
15. Polomoshnov, A.F., & Kolyshkina, M.S. (2024). Tsifrovizatsiia obrazovaniia kak trend: za i protiv [Digitalization of education as a trend: pros and cons]. *Vestnik Kalmytskogo universiteta* [Bulletin of the Kalmyk University], (4 (64)), 153–160.
16. Stepanova, N.K. (2025) Zarubezhnyi opyt effektivnoi profilaktiki kiberprestupnosti v otnoshenii nesovershennoletnikh pravookhranitel'nymi organami [Foreign experience of effective prevention of cybercrime against minors by law enforcement agencies]. *Upravlenie obrazovaniem: teoriia i praktika* [Education Management: Theory and Practice], (8-1), 281–293.
17. Sarukhanyan, E.O., & Viachistov, V.M. (2025) Vliianie vnedreniia informatsionnykh tekhnologii v vuzakh na psikhologicheskoe blagopoluchie prepodavatelei vysshei shkoly [The impact of the introduction of information technologies in universities on the psychological well-being of higher education teachers]. *Upravlenie obrazovaniem: teoriia i praktika* [Education Management: Theory and Practice], (9-2), 78–87.