УДК 343.9 **DOI: 10.34670/AR.2026.88.23.050**

Характеристика угроз, посягающих на криминологическую безопасность цифровой образовательной среды

Сидорова Екатерина Закариевна

Кандидат юридических наук, доцент,
Восточно-Сибирский институт Министерства
внутренних дел Российской Федерации,
664074, Российская Федерация, Иркутск, ул. Лермонтова, 110;
e-mail: ketrik6@mail.ru

Аннотация

В статье рассматривается цифровая образовательная среда как самостоятельный объект криминологической безопасности современного общества. Автор выявляет и систематизирует комплекс современных угроз криминального и криминогенного характера, посягающих на цифровую образовательную среду на технологическом, информационно-психологическом и ценностно-смысловом уровнях. В заключении обосновывается необходимость перехода от фрагментарных технических решений к разработке целостной концептуальной модели криминологической безопасности образовательной среды, в том числе цифровой, которая должна включать нормативно-правовой, организационно-технический, педагогический и ценностно-ориентационный компоненты.

Для цитирования в научных исследованиях

Сидорова Е.З. Характеристика угроз, посягающих на криминологическую безопасность цифровой образовательной среды // Вопросы российского и международного права. 2026. Том 16. № 1А. С. 418-423. DOI: 10.34670/AR.2026.88.23.050

Ключевые слова

Криминологическая безопасность образования, криминальные угрозы, образовательный суверенитет, национальная безопасность, цифровизация образования.

Введение

Цифровая трансформация образования, ускоренная глобальными вызовами последних лет, привела к формированию гибридной цифровой образовательной среды. Цифровая образовательная среда представляет собой результат объединения традиционных и дистанционных образовательных отношений, возникших в связи с развитием и доступностью различных технологических платформ, сервисов и цифровых данных. Став неотъемлемым элементом отечественной системы образования, цифровая образовательная среда превратилась не только в инструмент дидактики, но и в стратегически значимый объект, требующий комплексной криминологической защиты от криминальных угроз. Под криминологической безопасностью цифровой образовательной среды можно понимать состояние защищенности объектов, субъектов образовательной среды и образовательных отношений, возникающих между участниками данных отношений в цифровом пространстве, от преступных и иных противоправных посягательств, гарантирующее сохранение национальных образовательных и воспитательных приоритетов, ценностей и интересов.

Исходя из предложенного определения можно заключить, что цифровая образовательная среда должна рассматриваться как объект криминологической безопасности системы образования.

Основная часть

Цифровая образовательная среда является сложным системным элементом сферы образования, включающим:

1) технико-технологическую инфраструктуру (серверы, сети, платформы, устройства);

2) информационно-образовательный контент;

3) субъектов образовательных отношений (обучающихся, педагогов, администрацию образовательных организаций, родителей несовершеннолетних обучающихся и других);

4) цифровые персональные данные и иную информацию об участниках образовательных отношений.

Именно эта комплексность делает ее уязвимой для разнообразных криминальных проявлений. Киберугрозы носят не только прямой преступный характер (например, взлом цифровых хранилищ персональных данных о несовершеннолетних обучающихся; хищение информации о работе образовательной организации), но и опосредованный криминогенный характер, создавая условия для девиантного поведения и формирования антиобщественных установок (например, кибербуллинг одного из учащихся в той или иной социальной сети, что может в дальнейшем спровоцировать совершение таким учащимся акта скулшутинга). Таким образом, цифровая образовательная среда выступает одновременно как объект криминологической защиты и как среда, способная породить новые формы противоправной деятельности в сфере образования.

Поскольку криминальные угрозы, посягающие на криминологическую безопасность цифровой образовательной среды, носят системный и многоуровневый характер, одновременно воздействуя на ее различные компоненты, можно выделить многоуровневую систему таких угроз:

1. Технологический уровень угроз криминологической безопасности цифровой образовательной среды. На этом уровне проявляются традиционные, но от этого не менее

опасные киберугрозы:

– атаки на доступность образования, например, DDoS-атаки на образовательные платформы и порталы (это онлайн-атаки на цифровую систему образовательной организации, при которой злоумышленники посылают огромное число запросов), парализующие учебный процесс в определенные периоды, например, для срыва учебной сессии или проведения приемной кампания по поступлению на обучение в образовательную организацию (Как школьники срывают уроки с помощью DDoS-атак – и чем это для них оборачивается // Дзен: сайт. URL: https://dzen.ru/a/aM2dczjYHyujgy_y?ysclid=ml8qqf6w44886355865);

– атаки на конфиденциальность информации об участниках образовательных отношений и целостность образовательной системы. Речь идет о киберпреступлениях, связанных с хищением, уничтожением или подменой данных. Особую опасность представляет компрометация массивов персональных данных (включая биометрические) обучающихся и педагогов, а также несанкционированный доступ к результатам интеллектуальной деятельности (уникальным методикам, курсам, исследованиям) (Хакеры украли данные 4468 пользователей сайта Алтайского госуниверситета // Рамблер Новости: сайт. URL: https://news.rambler.ru/internet/50061653-hakery-ukrali-dannye-4468-polzovateley-sayta-altayskogo-gosuniversiteta/?ysclid=ml8r1ewdka160727153);

– внедрение вредоносного программного обеспечения. В качестве метода воздействия на образовательные организации в ряде случае выступает использование вирусов-шифровальщиков, шпионского программного обеспечения, ботнетов и другие средства для осуществления атак на инфраструктуру образовательных организаций или использования ее ресурсов в противоправных целях (УФСБ выявило опасный вирус в информационной системе РАНХиГС // Континент Сибирь онлайн: сайт. URL: https://ksonline.ru/565433/ufsb-vyyavilo-opasnyj-virus-v-informatsionnoj-sisteme-ranhigs/?ysclid=ml8r7oqma555633742).

2. Информационно-психологический уровень. Данный уровень угроз направлен непосредственно на личность участников образовательных отношений:

– кибербуллинг и кибертроллинг. Это систематические оскорбления участников образовательных отношений, угрозы в их адрес, распространение порочащей честь и достоинство информации о них в цифровом пространстве, ведущие к психологическим травмам, десоциализации, а в крайних случаях – к суицидальным последствиям(Из-за травли в Интернете девочка покончила собой // Российская газета: сайт. URL: https://rg.ru/2015/04/08/travlya.html?ysclid=ml8rdf7uzm410523738&utm_referrer=https%3A%2F%2Fya.ru%2F);

– фишинг и социальная инженерия. Речь идет о манипулятивных техниках, нацеленных, в том числе, на детей, подростков и педагогов с целью получения обманным путем конфиденциальных данных, вовлечения в противоправную деятельность или деструктивные онлайн-сообщества (Мошенники атаковали учителей от имени руководства школ // Газета.ru: сайт. URL: https://www.gazeta.ru/social/news/2021/01/14/n_15485054.shtml?ysclid=ml8rr7wlpj317627089);

– пропаганда девиантного и суицидального поведения. В ряде случаев в цифровых образовательных и сопряженных с ними коммуникационных пространствах (чаты, социальные сети) распространяется информация, направленная на склонение школьников и студентов к потреблению наркотических средств, насилию, участию в экстремистских группах или совершению суицида (так называемые «группы смерти») (В Петербурге школьницы создали «группу смерти» и решили покончить с собой // Regions.ru: сайт. URL: https://regions.ru/bezopasnost/moshenniki-atakovali-uchiteley-ot-imeni-rukovodstva-shkol).

3. Ценностно-смысловой (идеологический) уровень. Это наиболее латентный и крайне опасный уровень угроз, посягающий на фундаментальность образовательного суверенитета страны:

– идеологическое и ценностное воздействие на участников образовательных отношений. Речь идет о целенаправленном распространении через образовательный контент (содержание отдельных учебников или образовательных программ), массовую культуру и медиапространство, интегрированные в цифровую образовательную среду, идеологий, чуждых традиционным российским ценностям (культ потребления, радикальный индивидуализм, обесценивание нравственных норм, фальсификация истории страны). Подобные действия направлены именно на размывание культурно-нравственной российской традиционной идентичности у молодого поколения;

– подмена образовательной парадигмы. Данный вид угрозы может проявиться при полной цифровизации образовательной среды и отказе от традиционного формата образования, где цифровой инструмент заменяет живого педагога-наставника; при отказе от реализации воспитательного компонента образовательных программ; при полном переходе к оказанию только платных цифровых образовательных услуг и формированию знаний у обучающихся только на платной основе (полная коммерциализация сферы образования). Специалисты подчеркивают, что в таких случаях может «усилиться неравенство в возможностях получения образования: хорошее фундаментальное образование – это дорогое «человеческое», для остальных – дешевое дистанционное, онлайн» [Стариченко, 2020, с. 18]. Именно поэтому отечественные правоведы считают необходимым преодолевать проблему цифрового неравенства [Бегишев, Жарова, Залоило, Филипова, Шутова, 2024, с. 736].

Уязвимость цифровой образовательной среды порождается как техническими несовершенствами данной сферы общественных отношений, так и социально-психологическими рисками, к которым относятся:

1) внешние факторы, такие как деятельность транснациональных киберпреступных групп, действия иностранных хакеров и спецслужб, а также идеологическое давление со стороны ряда зарубежных цифровых платформ и производителей цифрового продукта;

2) внутренние факторы, такие как цифровое неравенство и низкая цифровая грамотность. Значительная часть участников образовательных отношений, в особенности представители педагогического сообщества и родительской общественности, еще не обладает достаточными навыками кибергигиены и медиабезопасности для эффективного противодействия криминальным угрозам, проявляющимся в цифровом образовательном пространстве. Также в качестве внутреннего фактора следует рассматривать девиантное поведение самих участников образовательных отношений. Речь идет о так называемых внутрисредовых рисках, создаваемых самими обучающимися, в том числе кибербуллинг, плагиат в цифровом пространстве, приводящий к нарушению авторских прав, распространение запрещенного контента среди школьников и студентов и другое. Следует отметить и определенное отставание нормативно-правовой базы от динамики технологических изменений, недостаточное финансирование мер обеспечения кибербезопасности, отсутствие единых стандартов защиты для всех участников цифровой образовательной среды.

Таким образом, проведенный анализ позволяет утверждать, что угрозы криминологической безопасности цифровой образовательной среды представляют собой сложный феномен, сочетающий в себе технические киберугрозы, психологические манипуляции и попытки идеологического вмешательства в образовательную среду. Ключевой вывод заключается в том, что большую опасность для цифрового образования представляют как прямые, видимые атаки,

так и латентные угрозы ценностно-смыслового уровня, способные негативно отразиться на уровне защищенности национального образовательного и культурного суверенитета страны.

Заключение

В связи с этим можно обоснованно утверждать, что защита цифровой образовательной среды не может ограничиваться исключительно техническими мерами (например, установкой антивирусов и фаерволов; файрвол – это программно-аппаратный комплекс, предназначенный для проверки и фильтрации сетевого трафика [Супрунов, 2008, с. 50]; он позволяет контролировать поток данных, проходящих через сеть, и принимать решения о разрешении или блокировке соединений на основе заранее заданных правил; файервол – это некий «щит» или «фильтр», обеспечивающий безопасность передачи данных). Как справедливо отмечается в литературе, требуется именно системный подход к обеспечению безопасности образовательной среды [Сидорова, 2025, с. 187]. Комплексная криминологическая модель безопасности образовательной среды, в том числе цифровой, должна включать:

1) нормативно-правовой компонент, подразумевающий совершенствование законодательства в сфере криминологической защиты системы образования, в частности обеспечение защиты персональных сведений, принадлежащих участникам образовательных отношений и хранящихся в цифровых базах данных, от так называемой «утечки» и утраты; обеспечение кибербезопасности образовательных организаций; более детальное регулирование отношений, связанных с использованием цифрового образовательного контента;

2) организационно-технический компонент, представленный в виде внедрения стандартов кибербезопасности для участников образовательных отношений, обеспечения цифрового суверенитета через использование отечественного программного обеспечения и отечественных цифровых образовательных платформ;

3) педагогический и воспитательный компонент, в рамках которого предполагается интеграция в образовательные программы положений по цифровой и медиаграмотности, кибергигиене, основам правовой культуры в цифровой среде, при этом ключевая роль отводится подготовке и переподготовке педагогов в данной сфере;

4) ценностно-ориентационный компонент, подразумевающий формирование у обучающихся критического мышления, ценностного иммунитета к деструктивному контенту, распространяемому в информационно-телекоммуникационной среде, воспитание ответственной цифровой гражданской позиции.

Только такой системный междисциплинарный подход, рассматривающий цифровую образовательную среду как пространство формирования будущего нации, позволит обеспечить ее криминологическую безопасность, защитить права личности участников образовательных отношений и укрепить национальный образовательный суверенитет Российской Федерации.

Библиография

1. Бегишев, И. Р., Жарова, А. К., Залоило, М. В., Филипова, И. А., & Шутова, А. А. (2024). Технологические трансформации: рост возможностей и правовой ответ на возникающие риски. Journal of Digital Technologies and Law, 2(4), 735-740.
2. Сидорова, Е. З. (2025). Цифровая, антиэкстремистская и иные виды криминологической безопасности образовательной среды. Вестник Восточно-Сибирского института МВД России, (4(115)), 181-189.
3. Стариченко, Б. Е. (2020). Цифровизация образования: реалии и проблемы. Педагогическое образование в России, (4), 16-26.
4. Супрунов, С. (2008). О пользе файерволов. Системный администратор, (3(64)), 50-52.

Characteristics of Threats Encroaching on the Criminological Security of the Digital Educational Environment

Ekaterina Z. Sidorova

PhD in Law, Associate Professor,
East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation,
664074, 110, Lermontov str., Irkutsk, Russian Federation;
e-mail: ketrik6@mail.ru

Abstract

The article examines the digital educational environment as an independent object of criminological security in modern society. The author identifies and systematizes a complex of contemporary threats of a criminal and criminogenic nature that encroach upon the digital educational environment at the technological, informational-psychological, and value-meaning levels. In conclusion, the necessity of transitioning from fragmented technical solutions to the development of a holistic conceptual model of criminological security of the educational environment, including the digital one, is substantiated. This model should include regulatory-legal, organizational-technical, pedagogical, and value-orientation components.

For citation

Sidorova E.Z. (2026) Kharakteristika ugroz, posyagayushchikh na kriminologicheskuyu bezopasnost' tsifrovoy obrazovatel'noy sredy [Characteristics of Threats Encroaching on the Criminological Security of the Digital Educational Environment]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (1A), pp. 418-423. DOI: 10.34670/AR.2026.88.23.050

Keywords

Criminological security of education, criminal threats, educational sovereignty, national security, digitalization of education.

References

1. Begishev, I. R., Zharova, A. K., Zaloilo, M. V., Filipova, I. A., & Shutova, A. A. (2024). Tekhnologicheskiye transformatsii: rost vozmozhnostey i pravovoy otvet na voznikayushchiye riski [Technological transformations: growth of opportunities and legal response to emerging risks]. Journal of Digital Technologies and Law, 2(4), 735-740.
2. Sidorova, E. Z. (2025). Tsifrovaya, antiekstremistskaya i inyye vidy kriminologicheskoy bezopasnosti obrazovatelnoy sredy [Digital, anti-extremist and other types of criminological security of the educational environment]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii, (4(115)), 181-189.
3. Starichenko, B. E. (2020). Tsifrovizatsiya obrazovaniya: realii i problemy [Digitalization of education: realities and problems]. Pedagogicheskoye obrazovaniye v Rossii, (4), 16-26.
4. Suprunov, S. (2008). O polze fayervolov [On the benefits of firewalls]. Sistemnyy administrator, (3(64)), 50-52.