УДК 343.9

КУЛЬТУРА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ — ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И КУЛЬТУРАЛЬНАЯ КРИМИНОЛОГИЯ

CYBERCRIME COUNTERACTION CULTURE — DIGITAL TRANSFORMATION AND CULTURAL CRIMINOLOGY

Т. И. Вишневская
Могилевский институт МВД Республики Беларусь,
доцент кафедры общеюридических и уголовно-правовых дисциплин
факультета повышения квалификации и переподготовки кадров,
кандидат юридических наук, доцент

Аннотация. *В статье рассматриваются особенности современной киберпреступности. Автор приводит примеры инновационных киберпреступлений, совершающихся в условиях цифровой трансформации, предлагает перспективные направления по противодействию киберпреступности, обращает внимание на важность развития культуры противодействия киберпреступности.*

Ключевые слова: *культура, цифровизация, киберпреступность, противодействие.*

Annotation. *This article examines the characteristics of modern cybercrime. The author cites examples of innovative cybercrimes occurring amidst digital transformation, proposes promising avenues for combating cybercrime, and highlights the importance of fostering a culture of countering cybercrime.*

Keywords: *culture, digitalization, cybercrime, counteraction.*

Цифровая трансформация окружающего мира, обеспечиваемая внедрением цифровых технологий во все аспекты человеческой жизни, качественно изменяет социальную реальность. Закономерно, что усиливающаяся цифровизация неизбежно порождает как положительные, так и отрицательные последствия — киберпреступность. Приоритетной задачей каждого современного государства является формирование культуры противодействия киберпреступности в условиях расширяющейся технологизации, информатизации, кибернетизации и интернетизации.

Киберпреступность постоянно трансформируется, принимает различные противоправные формы: криминальная активность в интернет-торговле; мошенничество с использованием информационно-коммуникационных технологий; киберворовство как хищение программных продуктов, конфиденциальной информации; киберсталкерство и кибербуллинг, обращенные на преследование, запугивание через цифровые ресурсы; кибертерроризм; кибер-секс-бизнес (виртуальная порнография); цифровая наркопреступность и др. С появлением

новых технологических возможностей киберпреступность становится сложнее и разнообразнее.

В настоящее время в Республике Беларусь уже фиксируются случаи преступлений, совершенных с помощью виртуальных персон (аватаров) в виртуальной реальности компьютерных игр. Примером хищения виртуальных предметов может быть преступление, совершенное белорусским несовершеннолетним геймером, который похитил виртуальный танк в игре World of Tanks и продал его за 30 тыс. белорусских рублей [1]. Подобное преступление совершил и участник игры Counter-Strike, который похитил виртуальный нож [2]. Кроме того, в стране зарегистрированы преступления, основанные на технологии deepfake, когда мошенники с помощью нейросетей генерируют голоса, видеообличия цифровых двойников (родственника, руководителя, представителя бизнеса и др.) и рассылают видеоаудиообращения с целью получения денежных средств [3].

Заметим, что в некоторых зарубежных странах уже есть факты совершения виртуальных изнасилований и цифровых убийств. В Великобритании цифровой персонаж 16-летней девочки-подростка подвергся «групповому изнасилованию» виртуальными героями других игроков в компьютерной игре, и, хотя физического нападения не было, правоохранительные органы посчитали, что она получила такие же психологические травмы, как и жертва реального преступления [4]. Примером цифрового убийства может быть случай в Соединенных Штатах Америки, когда хакеры взломали сервер больницы и изменили алгоритм программы кардиостимулятора, что привело к смерти пациента [5]. Кроме того, вызывает беспокойство появление киберфизических преступных систем (роботов, дронов и прочее), специально созданных в преступных целях, которые могут действовать как под управлением оператора, так и автономно [6, с. 29]. Уместно привести прецедент с «умным роботом», который запрограммирован на действия без связи с оператором. Так, в Ливии боевой робот осуществил выслеживание и уничтожение человека «по собственной инициативе и без участия оператора» [7].

В Республике Беларусь на протяжении последних лет наблюдается снижение преступности в целом [8, с. 135] и киберпреступности в частности [9]. Необходимо обратить внимание на то, что к преступлениям, подлежащим учету подразделениями Министерства внутренних дел Республики Беларусь, осуществляющими противодействие киберпреступности, относятся: хищения путем модификации компьютерной техники (ст. 212 Уголовного кодекса Республики Беларусь (далее — УК)); незаконный оборот платежных инструментов, средств платежа и их реквизитов (ст. 222 УК); преступления против информационной безопасности (ст. 349–355 УК); вымогательство (ст. 208 УК);

мошенничество (ст. 209 УК); заведомо ложные сообщения об опасности (ст. 340 УК), если их совершение сопряжено с использованием информационно-коммуникационных технологий; причинение имущественного ущерба без признаков хищения (ст. 216 УК), если ущерб в результате преступления причинен путем модификации компьютерной информации; принуждение (ст. 185 УК); угроза убийством, причинением тяжких телесных повреждений или уничтожением имущества (ст. 186 УК); насилие либо угроза применения насилия в отношении сотрудника органов внутренних дел (ст. 364 УК); насилие либо уроза в отношении должностного лица, выполняющего служебные обязанности, или иного лица, выполняющего общественный долг (ст. 366 УК); угроза в отношении судьи или народного заседателя (ст. 389 УК), если ее совершение сопряжено с совершением преступлений, предусмотренных главой 31 УК, или с использованием вредоносных программ, несанкционированным доступом к компьютерной информации, модификацией компьютерной информации, приведением компьютерной информации в непригодное для использования состояние, использованием поддельных интернет-ресурсов и ссылок на них, блокированием компьютерной информации, использованием неправомерно полученных платежных реквизитов и (или) реквизитов доступа, использованием устройств для считывания данных банковской платежной карты, использованием программного или аппаратного средства [10; 11].

Анализ структуры зарегистрированных киберпреступлений в 2025 г. в Беларуси показывает, что абсолютное большинство всех киберпреступлений составляют мошенничества, совершаемые с использованием информационно-коммуникационных технологий (55 %), и хищения имущества путем модификации компьютерной информации (36 %) [12]. Более чем 96 % всех киберпреступлений связаны с противоправным завладением денежными средствами или информацией для последующего получения кредитов [9], они осуществляются посредством звонков от имени банковских работников, правоохранительных органов, сотовых операторов, коммунальных служб и т. д. Среди наиболее распространенных мошеннических киберсхем можно выделить подложные продажи товаров, оказание поддельных услуг (декларирование средств, внесение денежных средств на безопасный счет, вклады в криптовалюту и др.).

Уменьшение числа рассматриваемых преступлений связано в первую очередь с эффективной работой правоохранительных органов Республики Беларусь в сфере противодействия киберпреступности. Вместе с тем интенсивные технологические изменения в обозримом будущем требуют дальнейшего непрерывного совершенствования мер национальной и международной кибербезопасности.

Эволюционные изменения порождают необходимость развития культуры противодействия киберпреступности. Культура противодействия преступности представляет способ (тип) правоохранительной деятельности, присущий государству, сложившийся в конкретных социально-исторических условиях [13, с. 119]. Как отмечает С. Я. Лебедев, «по своему содержанию культура противодействия преступности отражает свойственную правоохранительной системе государства стратегию антикриминальной деятельности» [14, с. 16]. В практике антикриминальной деятельности существует два взаимосвязанных и взаимообусловленных типа противодействия преступности, определяющих содержание культуры противодействия преступности. Первый из них образует традиционную форму правоохранительной деятельности, содержанием которой выступает уголовная репрессия. Второй формат составляет предупреждение преступности [13, с. 119–120]. В контексте совершенствования культуры противодействия киберпреступности видим перспективу в развитии цифрового законодательства. Нам представляется интересным опыт принятия Цифрового кодекса Кыргызской Республики, который устанавливает правовые основы создания, использования и функционирования информационных технологий, государственных информационных систем, электронного управления, защиты персональных и биометрических данных, использования искусственного интеллекта [15]. Актуальным направлением считаем развитие цифрового уголовного права, а также принятие Кодекса кибербезопасности [6]. В векторе предупреждения киберпреступности видим необходимость цифровой модернизации, а именно создания и внедрения инновационных достижений современных нано-, био-, информационных, когнитивных и социальных технологий (НБИКС-технологий) в предупредительной деятельности [16, с. 63]. Чрезвычайно важным является снижение рисков цифровой виктимности населения через повышение цифровой грамотности, понимание возможностей современных цифровых угроз, развитие массовой и индивидуальной культуры цифровой безопасности, цифрового этикета.

В условиях масштабных информационно-технологических преобразований мир находится на пороге формирования новой системы противодействия киберпреступности. Культуральная криминология рассматривается как одно из последних достижений криминологической теории, как исходное начало для выработки эффективных мер предупреждения преступности.

---

1. Белорусская милиция две недели искала угонщика виртуального танка [Электронный ресурс] // Татар-информ : [сайт]. URL: https://www.tatar-inform.ru/news/belorusskaya-militsiya-dve-nedeli-iskala-ugonschika-virtualnogo-tanka-359067 (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

2. Кражей виртуального ножа в игре Counter-Strike занялся СК Беларуси. Что произошло [Электронный ресурс] // БрестСити : [сайт]. URL: https://brestcity.com/blog/krazha-virtualnogo-nozha (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

3. Ловушки цифровой эпохи: как мошенники воссоздают голос и внешность ваших знакомых [Электронный ресурс] // Следств. ком. Респ. Беларусь : [сайт]. URL: https://sk.gov.by/ru/news-ru/view/lovushki-tsifrovoj-epoxi-kak-moshenniki-vossozdajut-golos-i-vneshnost-vashix-znakomyx-15467/ (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

4. Полиция Британии расследует первое изнасилование в виртуальной реальности [Электронный ресурс] // Редакция «Российской газеты» : [сайт]. URL: https://rg.ru/amp/2024/01/03/policiia-britanii-rassleduet-pervoe-iznasilovanie-v-virtualnoj-realnosti.html (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

5. Борисов Т. Управление «К»: Интернет начал убивать [Электронный ресурс] // Редакция «Российской газеты» : [сайт]. URL: https://rg.ru/2005/02/08/e-prestupnost.html?utm_referrer=https%3A%2F%2Fwww.google.com%2F (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

6. Лебедев С. Я., Джафарли В. Ф. Цифровое уголовное право : моногр. М. : Проспект. 309 с. Вернуться к статье

7. Отчет ООН: Впервые в истории боевой робот выследил и ликвидировал бойца без команды оператора [Электронный ресурс] // Военное обозрение : [сайт]. URL: https://topwar.ru/183548-otchet-oon-vpervye-v-istorii-boevoj-robot-vysledil-i-likvidiroval-bojca-bez-komandy-operatora.html (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

8. Статистический ежегодник Республики Беларусь / Нац. стат. ком. Респ. Беларусь ; редкол.: И. В. Медведева (пред.) [и др.]. Минск : Нац. стат. ком. Респ. Беларусь, 2025. 305 с. Вернуться к статье

9. МВД: количество киберпреступлений в Беларуси снизилось почти на 6 % в 2025 году [Электронный ресурс] // БЕЛТА : [сайт]. URL: https://belta.by/society/view/mvd-kolichestvo-kiberprestuplenij-v-belarusi-snizilos-pochti-na-6-v-2025-godu-762446-2026/ (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

10. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. в ред. от 20 окт. 2025 г. № 101-З. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

11. О преступлениях, подлежащих учету по направлениям деятельности органов внутренних дел [Электронный ресурс] : приказ М-ва внутр. дел Респ. Беларусь от 31 марта 2021 г. № 92 : в ред. от 6 февр. 2025 г. № 33. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

12. Киберпреступность — 2025: что происходит на самом деле [Электронный ресурс] // Следств. ком. Респ. Беларусь : [сайт]. URL: https://sk.gov.by/ru/news-ru/view/kiberprestupnost-2025-chto-proisxodit-na-samom-dele-15685/ (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

13. Симоненко А. В., Грибанов Е. В. Культура противодействия преступности в деятельности органов внутренних дел // Вестн. Моск. ун-та МВД России. 2015. № 4. С. 119–124. Вернуться к статье

14. Лебедев С. Я. Стратегия предупреждения преступности органами внутренних дел // Криминол. журн. 2005. № 2 (8). С. 16–20. Вернуться к статье

15. Цифровой кодекс Кыргызской Республики [Электронный ресурс] : 31 июля 2025 г. № 178 // Законодательство стран СНГ : [сайт]. URL: https://base.spinform.ru/show_doc.fwx?rgn=168581 (дата обращения: 02.02.2026). Перейти к источнику Вернуться к статье

16. Стальбовский В. В., Вишневская Т. И. НБИКС-технологии в противодействии преступности эпохи метамодерна // Юстиция Беларуси. 2026. № 2. С. 63–72. Вернуться к статье