12. France plans internet ombudsman to safeguard free speech. — URL: https://www.theguardian.com/technology/2016/dec/19/france-plans-internet-ombudsman-to-safeguard-free-speech (дата обращения: 30.01.2026).

13. UK considers internet ombudsman to deal with abuse complaints. — URL: https://www.theguardian.com/technology/2017/aug/22/uk-considers-internet-ombudsman-to-deal-with-abuse-complaints (дата обращения: 15.02.2026).

14. Мочалов, А.Н. Об учреждении в России должности уполномоченного по защите прав человека в сфере информационно-телекоммуникационных технологий / А.Н. Мочалов // Правовое государство: теория и практика. — 2022. — № 2(68). — URL: https://cyberleninka.ru/article/n/ob-uchrezhdenii-v-rossii-dolzhnosti-upolnomochennogo-po-zaschite-prav-cheloveka-v-sfere-informatsionno-telekommunikatsionnyh (дата обращения: 12.01.2026).

15. Гуляев, Д. Защита прав в онлайн-среде: как подать обращение Молодежному цифровому омбудсмену / Д. Гуляев. — URL: https://www.gazeta.ru/comments/2021/10/21_a_14118931.shtml?utm_auth=false (дата обращения: 13.02.2026).

16. Sossin, L. Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act: An Effectiveness Study: Prepared for the Canadian Privacy Commission, 2010 / L. Sossin, F. Houle. — URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1911272 (дата обращения: 16.02.2026).

## КРИМИНОГЕННЫЕ ПОСЛЕДСТВИЯ РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

*В.Г. Стаценко*

Криминологические исследования последних лет свидетельствуют о том, что характер и содержание преступности в сегодняшних условиях претерпевают серьезные изменения, криминальная деятельность приобретает черты и свойства, обусловленные, главным образом, переходом к качественно новому этапу цивилизационного развития, определяемого внедрением во все сферы жизни общества информационно-коммуникационных цифровых технологий.

Интегрированный итог криминологического анализа современных тенденций преступности представлен в Киотской декларации «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению Повестки дня в области устойчивого развития на период до 2030 года», принятой 14 Конгрессом ООН по предупреждению преступности и уголовному правосудию 7–12 марта 2021 г. в г. Киото, Япония. В разделе «Новые, появляющиеся и видоизменяющиеся формы преступности» Киотской декларации выделяются конкретные криминальные деяния, наиболее подверженные трансформациям. Так, обращается внимание на важность борьбы со следующими из них: организованная преступность; торговля людьми; незаконный ввоз мигрантов; незаконный оборот огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему; наркоторговля; эксплуатация,

торговля, насилие и пытки в отношении детей, включая сексуальную эксплуатацию детей; незаконный оборот объектов дикой живой природы, в том числе флоры и фауны; фальсификация медицинской продукции; незаконный оборот культурных ценностей и другие преступления против культурных ценностей; контрабанда коммерческих товаров; преступления на почве ненависти; киберпреступность [1].

Практически все приведенные криминальные явления представляют собой отдельный сегмент криминального рынка, имеющего обширную транснациональную распространенность. Кроме того, почти каждое из содержащихся в приведенном перечне преступное деяние способно нанести вред не только общественной, но и национальной безопасности страны.

Очевидно, что в каждом государстве перечисленные выше тенденции развиваются по-разному в зависимости от уровня развития страны, социально-экономического состояния, численности и национального состава населения, географического расположения, уровня преступности и иных криминологически значимых обстоятельств.

В Республике Беларусь эти криминальные проявления также обладают специфическими характеристиками. Структура преступности в стране в последние годы существенно изменяется: происходит определенное сокращение объема и удельного веса традиционных уголовных преступлений, таких как кражи, угон автомобилей и некоторых других. Одновременно фиксируется увеличение в структуре преступности криминальных деяний, связанных с использованием информационно-коммуникационных технологий, причем это относится и к таким видам преступлений, как мошенничество, вымогательство, наркопреступления, преступления экстремистской направленности и др.

Все это с очевидностью определяет актуальность, а также научную и практическую значимость рассматриваемой проблемы.

Материал: эмпирические данные, в частности, международные и официальные статистические источники Республики Беларусь, позволяющие провести сравнительный анализ официальных количественных и качественных показателей киберпреступности в стране, научные публикации по теме исследования.

Общей теоретической и методологической базой для решения поставленных задач послужили общенаучные методы познания (описание, сравнение, анализ, синтез). В зависимости от конкретных задач исследования в работе использовались описательно-аналитический, сравнительно-правовой, статистический, логический и системно-структурный методы.

Противодействие преступности в сфере информационно-коммуникационных технологий и совокупность мер по ее предупреждению — составная часть как международной, так и национальной безопасности. В Концепции национальной безопасности Республики Беларусь, утвержденной Решением Всебелорусского народного собрания 25.04.2024 № 5, подчеркивается,

что «в условиях глобальной цифровизации кибербезопасность критической инфраструктуры и больших данных приобрела исключительное значение для обеспечения устойчивости всех сфер жизнедеятельности», а «дальнейшее развитие безопасной информационной среды и информационного общества», включая превенцию преступлений в сфере информационно-коммуникационных технологий, следует рассматривать как важнейший национальный интерес в информационной сфере» [2].

Вместе с тем борьба с преступностью в сфере информационно-коммуникационных технологий существенно осложняется тем обстоятельством, что современные технологии внедряются в преступную среду и используются ею существенно быстрее, чем развивается соответствующее законодательство, определяющее меры противодействия криминальным проявлениям в области информационно-коммуникационных технологий, а также реакция на развитие т.н. киберпреступности со стороны правоохранительных органов. Все это значительно затрудняет процессы выявления преступлений и сбора доказательственной базы.

Понятие «киберпреступность» хотя и активно применяется в последние десятилетия в качестве доктринального, прежде всего, термина, тем не менее законодательного закрепления во многих странах, да и на международном уровне, почти не имеет. Так, по оценке ООН, из 200 актов законодательства различных стран, относящихся к области противодействия преступности в сфере информационно-коммуникационных технологий (ИКТ), термин «киберпреступность» использовался лишь примерно в 5% случаев [3, с. 68]. Создает проблему и то обстоятельство, что указанное понятие имеет различающуюся содержательную трактовку.

Киберпреступность — в соответствии с определением его содержания, данным на 10 Конгрессе ООН по предупреждению преступности 2000 года (неофициальная трактовка справочного характера) [4], — это родовое понятие, охватывающее как компьютерную преступность в узком значении этого слова (где компьютер является предметом, а информационная безопасность — объектом преступления), так и иные посягательства (широкое значение киберпреступности), когда компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности (например, компьютерное мошенничество и т.п.).

В соответствии с рекомендациями экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде.

Согласно Европейской Конвенции о киберпреступности (в русском переводе показательно — «Конвенция о компьютерных преступлениях»)

выделены два вида киберпреступлений: 1) компьютерные преступления против данных и систем (offences against the confidentiality, integrity and availability of computer data and systems); 2) преступления, связанные с компьютером (computer-related offences) [5], т.е. преступления, где компьютерные технологии используются в качестве орудия преступления.

В русскоязычной литературе термин «киберпреступность» чаще всего употребляется наряду с такими понятиями, как компьютерная преступность, преступления в сфере компьютерной информации, Интернет-преступность, преступления в сфере высоких технологий, преступления, сопряженные с компьютерными технологиями.

В законодательстве Республики Беларусь термин «киберпреступность» хотя и используется, например в наименовании главы 19 «Противодействие киберпреступности» Концепции информационной безопасности Республики Беларусь от 18 марта 2019 года [6], тем не менее правового определения также не имеет. В Уголовном кодексе Республики Беларусь применяется понятие «преступления против компьютерной безопасности». Глава 31 Раздела XII УК Республики Беларусь под этим наименованием включает в себя 5 видов преступлений, содержащихся в соответствующих статьях.

Необходимо исходить из того, что объединяющими признаками всех преступлений, входящих в состав киберпреступности, являются средства их совершения — киберпространство, информационно-телекоммуникационные сети и средства компьютерной техники. Соответственно, киберпреступность можно определить как совокупность преступлений, совершенных путем использования средств компьютерной техники и информационно-телекоммуникационных сетей.

Исходя из данной трактовки киберпреступности, составляющие ее противоправные деяния можно — по объекту посягательства — классифицировать следующим образом:

– преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации (посягательства на собственность);

– преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (преступления против информационной безопасности);

– преступления, в которых компьютеры и другие средства компьютерной техники применяются в качестве средства совершения корыстного преступления (хищение путем использования компьютерной техники).

Термин «киберпреступность», таким образом, существенно шире понятия «компьютерные преступления».

Киберпреступность превращается в один из самых крупных вызовов, с которыми человечество столкнется в ближайшие десятилетия.

Согласно «Отчету о рынке кибербезопасности за 2026 год», подготовленному Cybersecurity Ventures, ущерб от киберпреступности обойдется миру в 10,5 трлн долларов США в 2026 году — по сравнению с 6 трлн долларов в 2021 году и 3 трлн долларов в 2015 году, а к 2031 году объем продуктов и услуг в области кибербезопасности достигнет 1 трлн долларов США в год (в 2004 году этот рынок оценивался в 3,5 миллиарда долларов) [7].

Основными правовыми проблемами при расследовании киберпреступлений и судебном преследовании киберпреступников являются: разные правовые системы государств; различия национальных законодательств о киберпреступности; различия в нормах доказательственного права и уголовного судопроизводства (например, в процедурах получения доступа к цифровым доказательствам правоохранительными органами); различия в охвате и географической применимости региональных и многосторонних договоров о борьбе с киберпреступностью; различия в подходах к защите данных и соблюдению прав человека и др.

Европол разделяет киберпреступления на «киберзависимые преступления (т.е. любое преступление, которое может быть совершено только с использованием компьютеров, компьютерных сетей или других форм информационно-коммуникационных технологий)» и преступления, «совершаемые посредством кибертехнологий (т.е. традиционные преступления, совершаемые с помощью Интернета и цифровых технологий)» [8].

Киберпреступность становится все более серьезной проблемой для стран, в которых хорошо развита инфраструктура Интернета и функционируют платежные системы. Согласно последним оценкам Интерпола угрозы киберпреступности, последняя становится все более агрессивной и конфронтационной. Это можно наблюдать в различных формах киберпреступности, включая высокотехнологичные преступления, утечку данных, кибермошенничество, кибербуллинг.

В 2019 году Секретариат ООН предложил государствам-членам представить информацию о проблемах, с которыми они сталкиваются в борьбе с использованием информационно-коммуникационных технологий в преступных целях — для подготовки доклада Генерального секретаря ООН на ее 74 сессии.

В предоставленной Республикой Беларусь информации отмечалось, в частности:

– «принимая во внимание модернизацию современной наркопреступности и использование даркнета и криптовалют в целях незаконного оборота наркотиков, Беларусь считает, что одним из приоритетных направлений деятельности государств-членов должна стать организация обмена информацией, касающейся средств совершения преступлений и методов обнаружения преступной деятельности в даркнете, на наднациональном уровне; подборка и изъятие электронных доказательств; а также разработка и использование конкретных методов расследования преступлений, совершенных в виртуальном пространстве;

– по мнению Беларуси, разработка и принятие универсального международного документа в рамках ООН будет содействовать развитию сотрудничества между компетентными органами государств-членов в борьбе с использованием информационно-коммуникационных технологий в преступных целях» [9].

*Состояние, динамика и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.* В Республике Беларусь по состоянию на конец 2025 года насчитывалось 8,47 млн интернет-пользователей, что составляет 94,3% от общей численности населения. Число пользователей социальных сетей в Беларуси составило 7,64 млн активных пользователей, увеличившись в период с конца 2024 года по конец 2025 года на 1,8 миллиона (+30,6%) [10].

При этом, по экспертным оценкам, лишь незначительная часть пользователей информационно-коммуникационных технологий обладают навыками принятия мер безопасности. Как отмечается специалистами Национального центра кибербезопасности ОАЦ при Президенте Республики Беларусь, «в области кибербезопасности преобразующая сила ИКТ как катализаторов экономического роста и социального развития находится в критической точке, когда доверие населения и организаций к использованию таких технологий подрывается отсутствием кибербезопасности» [11, с. 3].

Высокие темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место неквалифицированностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего числа противоправных деяний в данной сфере.

На протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений. Так, если в 2006 году было зарегистрировано всего 334 таких преступления, то в 2015 году — 2.473, в 2016 — 2.950, в 2017 — 3.111, в 2018 — 4.769, в 2019 — 10.567, в 2020 — 25.575, в 2021 — 16.446. В 2022 году количество хищения имущества путем модификации компьютерной информации и преступлений против компьютерной безопасности снизилось до 13.541 [12, с. 135].

Данные на 2023 год противоречивы. Национальный статистический комитет Республики Беларусь показывает уменьшение числа рассматриваемых преступлений — до 13.130, в то время как в обзорах статданных о результатах расследования преступлений на территории государств-участников СНГ указывается, напротив, существенный их рост до 18.321 преступлений. При этом если в 2022 году уровень киберпреступности в общей структуре преступности составлял 16,5%, то в 2023-м он вырос до 21,5% [13].

Статистика 2024 года также неоднозначна. Согласно данным статкомитета Республики Беларусь, в 2024 году число регистрируемых преступлений в сфере ИКТ резко сократилось — до 7.086 преступлений, т.е. почти на 50% [12, с. 135]. В то же время, по утверждению аналитиков

F.A.C.C.T. Fraud Protection, количество киберпреступлений в Беларуси продолжало расти и в 2024 году составило более четверти от всех преступлений в стране [14], т.е. по меньшей мере порядка 18 тыс. преступлений. По другим данным, в 2024 году в стране было зарегистрировано 20.137 киберпреступлений, а доля киберпреступлений в общей структуре преступности возросла до 27,5% [15, с. 107].

Подавляющее большинство преступлений, выявленных в сфере высоких технологий (свыше 90%), в последние годы относятся к хищениям путем модификации компьютерной информации (ст. 212 УК). Так, в 2021 году было зарегистрировано 14.291 преступлений (92% от всех киберпреступлений) по ст. 212 УК «Хищение имущества путем модификации компьютерной информации», 1104 — по статье 349 УК «Несанкционированный доступ к компьютерной информации», 45 — по ст. 350 УК «Уничтожение, блокирование или модификация компьютерной информации», 16 — по ст. 352 УК «Неправомерное завладение компьютерной информацией», 33 — по ст. 354 УК «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств» [16]. Атаки происходят в большинстве случаев с территории других стран.

Большая часть преступлений в рассматриваемой сфере на территории Республики Беларусь связана с кибермошенничеством, причем более 60% таких преступлений, по оценке представителей главного управления по противодействию киберпреступности МВД Республики Беларусь, приходится на покупку несуществующих товаров в Интернете и различные виды мошенничества в сфере услуг, таких, например, как аренда жилья. Далее по распространенности занимают преступления, связанные с вишингом, когда гражданам поступают звонки из «банковских учреждений», «правоохранительных органов», а также звонки или сообщения от «руководителей организаций» с вымышленного аккаунта. В каждом из этих случаев проводится психологическая обработка жертвы, основанная на методах социальной инженерии. Главная цель злоумышленника — склонить человека к добровольному переводу средств, оформлению кредита, проведению манипуляций со своими сбережениями, чтобы они попали на контролируемый преступником счет [17].

Киберпреступность отличается высоким уровнем латентности: регистрирующие органы не фиксируют значительную часть совершаемых преступлений в сфере информационно-коммуникационных технологий, а официальная статистика не отражает реальное состояние дел. В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надежных методов сбора таких данных. Значительная часть киберпреступлений остается вне поля зрения правоохранительных органов.

Рассматриваемые преступления, в силу их технологических особенностей и виртуальности, относятся к деяниям, где во многих случаях нет

явно выраженной жертвы (либо она не осознает себя таковой), что предопределяет высокий уровень естественной латентности.

Неотъемлемой и очень важной частью криминологического анализа преступности в сфере ИКТ, является криминологическая характеристика лиц, совершающих киберпреступления.

Совокупность лиц, совершающих преступления в сфере информационных технологий, достаточно разнородна по своему составу. Поэтому стремление построить обобщенный портрет всех личностей, совершающих противоправные действия в данной сфере, обречено на неудачу. Очевидно, что личность хакера будет отличаться от личности преступника, совершающего хищение средств путем взлома банкомата.

В 2024 году, по материалам оконченных производством уголовных дел анализируемой категории, 74,1% обвиняемых — мужчины, 25,9% — женщины, 23,0% — лица, ранее судимые за различные преступления, 17,3% составляют несовершеннолетние [15, с. 108].

Динамика числа лиц, осужденных за совершение хищения имущества путем модификации компьютерной информации (ст. 212 УК), следующая: в 2020 году было осуждено 1.506 человек, в 2022 году — 1.192, в 2023 году — 1.080, в 2024 году — 970, в 2025 году — 892 [18].

Условиями развития киберпреступности в Республике Беларусь можно полагать:

– ускоренную цифровизацию различных сторон жизнедеятельности населения последних лет, включая бытовую и досуговую сферы (безналичные способы оплаты услуг, активное использование соцсетей и др.) и, следовательно, расширение поля деятельности и возможностей киберпреступников;

– сохраняющийся невысокий уровень цифровых компетенций граждан, о чем свидетельствует высокий удельный вес киберпреступлений, подпадающих под состав преступлений мошенничества, и жертв таких преступлений;

– проблемы, связанные с несовершенством деятельности органов правопорядка, среди которых существенную роль играет недостаточный арсенал технических средств и технологий, не позволяющий в ряде случаев эффективно противостоять «новой» преступности;

– отсутствие в международном и национальном уголовных законодательствах унифицированного подхода к описанию признаков состава рассматриваемых преступлений, что не способствует эффективному противодействию им;

– высокий уровень латентности киберпреступности.

При этом, если принимать во внимание общемировые тенденции, прежде всего ожидается дальнейший рост хищений путем использования компьютерной техники и случаев несанкционированного доступа к компьютерной информации, совершаемых, в частности, мошенническими методами, посредством фишинга и взлома учетных записей пользователей в социальных сетях.

В Концепции информационной безопасности Республики Беларусь отмечается, что «в Республике Беларусь создана система предупреждения, выявления, пресечения и всестороннего расследования киберпреступлений… В связи с появлением новых общественно опасных деяний в информационной сфере устанавливается уголовная и иная ответственность за их совершение. Обеспечивается постоянное совершенствование форм и методов предупреждения, выявления, пресечения и расследования киберпреступлений, повышается своевременность и качество оперативно-розыскной деятельности» [6].

В феврале 2023 года был принят Указ Президента Республики Беларусь «О кибербезопасности», в соответствии с которым «в целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз» в Республике Беларусь создана национальная система обеспечения кибербезопасности, задачами которой являются:

– достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

– постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;

– проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

– оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

– прогнозирование ситуации в области обеспечения кибербезопасности [19].

Наряду с созданием и функционированием национальной системы обеспечения кибербезопасности, одним из приоритетных направлений деятельности уполномоченных государственных органов определена профилактика киберпреступности, «основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в СМИ и сети Интернет в целях формирования безопасной национальной информационной экосистемы» [6].

Принимаемые государством меры по предотвращению киберпреступлений способны обеспечить необходимый эффект на практике только в тех случаях, когда осуществляется взаимодействие государственных органов с институтами гражданского общества, включая общественные объединения, органы местного самоуправления, СМИ, образовательными и научными организациями.

**Список использованных источников:**

1. Киотская декларация «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению Повестки дня в области устойчивого развития на период до 2030 года» / 14 Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному

правосудию, Киото, Япония, 7–12 марта 2021 года. — URL: https://www.unodc.org/documents/commissions/Congress/Kyoto_Declaration_booklet/21-02817KyotoDeclaration_ebook_R.pdf (дата обращения: 14.03.2026).

2. Концепция национальной безопасности Республики Беларусь: утверждена Решением Всебелорусского народного собрания 25.04.2024 № 5 // ЭТАЛОН: информ.-поисковая система (дата обращения: 13.03.2026).

3. Овчинский, В.С. Криминология цифрового мира / В.С. Овчинский. — М.: Норма: Инфра-М, 2026. — 348 с.

4. Преступления, связанные с использованием компьютерной сети // 10 Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. — С. 4–5. — URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_R.pdf (дата обращения: 12.03.2026).

5. Convention on Cybercrime Budapest, 23.XI.2001. — URL: https://rm.coe.int/1680081561 (дата обращения: 15.03.2026).

6. Концепция информационной безопасности Республики Беларусь: утверждена постановлением Совета Безопасности Республики Беларусь 18 марта 2019 г. № 1 // ЭТАЛОН: информ.-поисковая система (дата обращения: 13.03.2026).

7. Official 2026 Cybersecurity Market Report: Predictions and Statistics. — URL: https://cybersecurityventures.com/official-2026-cybersecurity-market-report-predictions-and-statistics (дата обращения: 14.03.2026).

8. Киберпреступность / UNODS. — URL: https://www.Unodc.org/e4j/ru/cybercrime/module-1/key-issues/cybercrime-in-brief.html (дата обращения: 10.03.2026).

9. Генеральная Ассамблея ООН. 74 сессия. Противодействие использованию информационно-коммуникационных технологий в преступных целях: доклад Генерального секретаря. — URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 15.03.2026).

10. Интернет и соцсети в Беларуси: отчет Digital 2026 / М-во информации Респ. Беларусь. — URL: http://mininform.gov.by/news/all/internet-i-sotsseti-v-belarusi-otchet-digital-2026/ (дата обращения: 15.03.2026).

11. Рекомендации государственным органам и иным организациям (в том числе владельцам критически важных объектов информатизации) по выполнению обязательных для исполнения требований законодательства в сфере обеспечения кибербезопасности, в том числе технической и криптографической защиты информации / Оперативно-аналитический центр при Президенте Республики Беларусь. Национальный центр кибербезопасности. — URL: https://www.oac.gov.by/public/content/files/files/recom.pdf (дата обращения: 16.03.2026).

12. Статистический ежегодник Республики Беларусь, 2025 год. — URL: https://www.belstat.gov.by/ofitsialnaya statistika/publications/izdania/public_compilation /index_152615/ (дата обращения: 13.03.2026).

13. Подсчитано по: О результатах борьбы с преступностью, в том числе организованной, на территориях государств-участников СНГ в 2023 году: аналитический обзор с предложениями / С.А. Невский, Ю.В. Тарасова, Д.Ю. Гребнев, В.Г. Смирнов, С.Д. Покачалов, О.В. Демковец, М.В. Огнева. — М.: ВНИИ МВД России, 2024. — С. 11.

14. Эксперты рассказали о количестве киберпреступлений в Беларуси. — URL: https://myfin.by/article/biznes/eksperty-rasskazali-o-kolicestve-kiberprestuplenij-v- belarusi-33983 (дата обращения: 10.03.2026).

15. Набатова, А.Э. Органы предварительного следствия Республики Беларусь в противодействии киберпреступности / А.Э. Набатова, А.В. Легчилкин, С.А. Кузьмичёв // Известия Гомельского государственного университета имени Ф. Скорины. — 2025. — № 5(152). — С. 107–111.

16. Сведения о совершенных правонарушениях на территории Республики Беларусь за январь — декабрь 2021 г. / Информационный центр МВД Республики Беларусь. — Мн., 2026.

17. В МВД рассказали об основных видах киберпреступлений, совершаемых в стране. — URL: https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2024/november/79505/ (дата обращения: 15.03.2026).

18. Правосудие в Республике Беларусь: Верховный Суд Республики Беларусь. — URL: https://court.gov.by/ru/justice_rb/statistics/ (дата обращения: 15.03.2026).

19. О кибербезопасности: Указ Президента Республики Беларусь от 14 февр. 2023 г. № 40 // ЭТАЛОН: информ.-поисковая система (дата обращения: 13.03.2026).

## ПРАВОВЫЕ ПРОБЛЕМЫ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ СОЦИАЛЬНОЙ ФИЛОСОФИИ И ЦИФРОВОЙ КРИМИНОЛОГИИ

*М.А. Андреасян*

Проблематика искусственного интеллекта (далее — ИИ) в современном цифровом мире весьма актуальна. Потребовалось всего полвека для того, чтобы искусственные машины успели перерасти из простой антиутопической концепции в реальную систему, способную имитировать мышление, речь и поведение Homo sapiens — единственного вида на Земле, обладающего разумом. В то же время цифровая цивилизация поставила перед человечеством животрепещущий вопрос: не пожалеет ли оно о том, что вознамерилось примерить на себя роль «Творца», детище которого может со временем «вытеснить» своего хозяина и занять главенствующее место на планете? С одной стороны, процесс внедрения ИИ во многом упростил жизнь социума, а с другой — поставил перед государством и обществом задачу решения проблемы необходимости правовой регламентации деятельности «умных машин» и противодействия угрозам, возникающим при их эксплуатации.

Социальная философия затрагивает ряд аспектов, связанных с проникновением ИИ в общественные системы и подсистемы: рост безработицы, предвзятое отношение к человеку, свобода воли и ответственность, угроза информационной и национальной безопасности, социальные последствия использования ИИ в преступной среде. Немаловажную роль в решении данных вопросов играет цифровая криминология как отдельная область знаний, в задачу которой входит принятие конкретных мер по предупреждению потенциальных криминогенных рисков, исходящих от функционирования ИИ, а также поиск путей его использования в правоохранительной системе.

Целью настоящего исследования является философско-правовое осмысление термина «искусственный интеллект» и определение специфики его применения преступным миром, раскрытие положительных и отрицательных криминологических характеристик ИИ, а также классификация