нять вред общественным отношениям, охраняемым законодательством об административных правонарушениях.

Существующий правой механизм не позволяет определить лицо, ответственное за нарушение правил дорожного движения, совершенное на транспортном средстве под автономным управлением искусственным интеллектом. В случае если фиксация правонарушения совершена специальными техническими средствами автоматической фиксации, то возможно привлечь к административной ответственности собственника транспортного средства. Тем не менее если правонарушение зафиксировано сотрудниками ГИБДД, то юридическая возможность привлечь к административной ответственности отсутствует, так как отсутствует лицо, осуществляющее управление транспортным средством.

Кроме того, остается непонятным алгоритм действий сотрудника полиции в случае выявления административного правонарушения, совершенного в процессе функционирования высокоавтоматизированного транспортного средства. Например, в 2019 году в СМИ обсуждался случай, когда сотрудники ГИБДД остановили высокоавтоматизированное транспортное средство и проверили документы водителя-испытателя. Однако он пояснил, что транспортным средством в момент движения фактически не управлял. И тут же возникает вопрос: остановится ли высокоавтоматизированное транспортное средство без водителя-испытателя на законные требования сотрудников полиции? И какие действия они должны совершить?

Таким образом, в настоящее время беспилотные автомобили относятся к правовой категории «высокоавтоматизированных транспортных средств» и имеют специальный экспериментальный правовой режим, действующий только в определенных субъектах РФ. При этом подобные транспортные средства не являются субъектами права, а юридическую ответственность за вред жизни и здоровью третьим лицам, причиненный в результате их эксплуатации несут установленные правом субъекты – водитель-испытатель, оператор, субъект экспериментального правового режима.

В то же время существует потребность в правовом регулировании вопросов ответственности за нарушение правил дорожного движения высокоавтоматизированными транспортными средствами, в связи с чем предлагается распространить на такие правоотношения правила, предусмотренные при фиксации административных правонарушений в автоматическом режиме специальными техническими средствами, когда ответственность несет собственник транспортного средства.

Кроме того, отдельно следует обратить внимание на масштабируемость рассмотренной проблемы, так как системы искусственного интеллекта внедряются не только в области беспилотного управления транспортными средствами, но и в иных сферах. При этом вопрос административной ответственности за правонарушения, совершенные с использованием искусственного интеллекта, не имеет широкого научного освещения и требует дальнейшего исследования.

Мельникова Л.Ю.

Сибирский юридический институт МВД России (г. Красноярск)

«Киберпреступления»: проблемы классификации

Развитие цифрового пространства во всех сферах жизнедеятельности общества, начиная с цифровой экономики и заканчивая «Электронным правительством», конечно, существенно расширяет возможности как для общества, так и для государства. Однако цифровой прогресс также предоставляет новые методы и способы совершения преступлений для криминальных элементов. Ведь стремление государства к полной цифровой трансформации всех сфер общественной жизни способствует не только развитию информационных технологий, оптимизации бизнес-процессов и развитию эффективных форм информационной поддержки любых видов деятельности, но и приводит к совершенствованию инструментов для совершения преступлений, внося существенные

изменения как в состав существующих составов правонарушения, так и приводя к появлению новых, совершаемых в виртуальной среде.

Количество правонарушений, которые совершаются с использованием информационных технологий с каждым годом лишь увеличивается (за последние пять лет в несколько раз). По данным МВД России каждое третье преступление совершается с использованием информационно-телекоммуникационных технологий. Например, с января по сентябрь 2023 года рост киберпреступлений составил +29,2 % по сравнению с аналогичным периодом в 2022 году. В связи с чем охрана и защита общественных отношений в цифровой сфере и в сфере кибербезопасности сегодня является одним из приоритетных направлений в деятельности всех государственных органов.

В уголовно-правовой доктрине как зарубежной, так и отечественной нет единого подхода к определению понятия «киберпреступления» и их классификации. Отсутствие единого унифицированного подхода к определению данного понятия и единого перечня киберпреступлений существенно сказывается на результативности и эффективности обеспечения кибербезопасности как на национальном, так и на международном уровнях.

Для обозначения общественно-опасных деяний, совершаемых с использованием информационно-телекоммуникационных технологий, используются различные термины и формулировки. Например, в научной и юридической литературе можно встретить такие термины, как: «компьютерные преступления», «киберпреступления», «интернет-преступления», «преступления, совершаемые с использованием интернет-технологий», «преступления, совершаемые в виртуальной среде», «преступления, совершаемые в Интернете», «преступления, совершаемые с помощью информационно-телекоммуникационных технологий», «компьютерная преступность», «киберпреступность», «интернет-преступность», «кибератаки», «кибервойны», «киберконфликты» и др[1].

Перечисленные термины и понятия имеют разную интерпретацию и коннотацию и по-разному определяют содержание правонарушений, совершаемых в рассматриваемой области общественных отношений. В целом можно выделить несколько основных подходов к определению понятия преступления, совершаемого в сфере информационных технологий, закрепившихся в юридической литературе, на основании которых осуществляется классификация данной категории правонарушений.

Стоит отметить, что проблематика «интернет-преступлений» и «компьютерной преступности» впервые была обозначена в зарубежной литературе, в которой и появился термин «киберпреступность». Данное понятие имеет более широкую коннотацию, чем, например, термин «компьютерная преступность», подразумевая любые правонарушения, сопряженные с информационными технологиями.

Российское уголовное законодательство не содержит правовой дефиниции понятий «киберпреступление» и «киберпреступность». Некоторые отечественные авторы, например, определяют киберпреступления также широко, как и зарубежные, включая в их состав все правонарушения, которые наносят вред разнородным общественным отношениям, но имеющие схожий квалифицирующий признак, такой как совершение правонарушений дистанционно, то есть с использованием ИТ-технологий, средств компьютерной техники и образованного ими киберпространства.

Однако правонарушения рассматриваемой категории могут быть не только разнородными, но и разновидовыми, в связи с чем указанный выше признак не может быть единственным системообразующим признаком структуры киберпреступлений. С точки зрения содержания понятия «киберпреступность» и «преступность в сфере информационных технологий» некоторыми авторами определяются как тождественные, так как под информационными технологиями понимается «совокупность приёмов, способов и методов применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных» (ГОСТ 59853-2021).

Положения Федерального закона «Об информации, информационных технологиях

[1] Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие // Правовой порядок и правовые ценности. 2023. № 1.

и о защите информации» такие понятия, как «компьютерная информация» и «информационно-телекоммуникационная сеть», определяют, как более узкие, что позволяет сделать вывод об их соотношении с понятием «информационные технологии» как общего к специальному. Такой подход позволяет выделить преступления в сфере информационных технологий и киберпреступления не только как вид правонарушения, но и как отдельный самостоятельный структурный признак.

В отечественной доктрине понятие «правонарушений, которые совершаются с использованием информационных технологий» в уголовно-правовом смысле включает в себя в той или иной степени составы преступлений, предусмотренные УК РФ. В соответствии с постановлением Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[1] классификация рассматриваемых деяний сводится к двум категориям преступлений:

1) преступления в сфере компьютерной информации (ст. 272, 273, 274 и 274.1 УК РФ);

2) преступления, совершенные с использованием сети (например, к такой категории можно отнести составы уголовных статей, касающиеся мошенничества и кражи, совершаемые с использованием ИТ-технологий (ст. 158, 159.3, 159.6 УК РФ), незаконный сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации (п. «б» ч. 2 ст. 228.1 УК РФ)). Однако такой подход к квалификации рассматриваемых деяний представляется слишком узким, так как он не дает полное представление об объеме сетевых угроз, существующем на сегодняшний день, и затрагивает практически все сферы жизнедеятельности общества.

С другой стороны, вторая из указанных выше категорий может включать в себя не только специальные виды хищения, но и традиционные составы правонарушений, совершаемые против жизни и здоровья. Например, в зависимости от последствий ненадлежащего оказания медицинской помощи с применением телемедицинских технологий, преступление может быть квалифицировано как по ст. 118 УК РФ (причинение тяжкого вреда здоровью по неосторожности), так и по ст. 109 УК РФ (причинение смерти по неосторожности). Но возможность относить подобные правонарушения к категории IT-преступлений является спорной.

Еще одной существенной проблемой при выработке единой классификации является использование спорных терминов и неопределенных понятий, которые представляют собой ряд признаков, являющихся основополагающими для криминологической характеристики отдельных видов киберпреступлений.

Например, в уголовном законодательстве нет четкого определения понятия «компьютерная информация». По смыслу ст. 272 УК РФ под это понятие попадают любые сведения, которые предоставлены в форме электрических сигналов. Однако использование термина «электрический сигнал» тоже само по себе является спорным, так как компьютерная информация может содержаться не только в стационарных компьютерах, в телефонах, но и в платёжных терминалах, банкоматах и т.д.

Сложности также возникают при определении предмета и объекта рассматриваемых деяний. На основе данного критерия (объект преступного посягательства – компьютерная информация) выделяют преступления, связанные с уничтожением такой информации: неправомерное завладение, а также нарушение исключительного права на её использование; неправомерная модификация; создание компьютерной информации с заданными свойствами (например, разработка и распространение вирусов или вредоносных программ).

Спорной также является формулировка ст. 274 УК РФ, где используется словосочетание «правила эксплуатации», являющееся ключевым в составе преступления. Определение нарушенных правил, норм или стандартов лицом вызывает большую сложность, ведь такая формулировка не исключает возможности содержания таких правил даже в международных договорах и соглашениях[2].

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15.12.2022 № 37.

[2] Влавацкая Е.А. Проблемы квалификации неправомерного доступа к компьютерной информации // Молодой ученый. 2021. № 22(364). С. 283-286.

При выработке классификации киберпреступлений необходимо учитывать множество различных и при этом криминалистически значимых элементов характеристики киберпреступлений. Это и особенности следовой информации, особенности предмета преступного посягательства, способ совершения, объективная сторона, которая может включать действия, связанные с передачей и распространением информации и др. Некоторые авторы выделяют также цель как критерий классификации киберпреступлений, подразделяя их на индивидуальные, имущественные и правительственные.

Подводя итог, стоит отметить, что уголовно-правовая регламентация рассматриваемой категории правонарушений на сегодняшний день всё ещё слабо разработана. Среди основных проблем классификации киберпреступлений можно выделить: отсутствие единого понимания понятийного аппарата, отсутствие единого подхода к используемой терминологии, использование некорректных терминов и некорректное использование специальных терминов, наличие спорных системообразующих признаков при определении состава преступления и, как следствие, недостаточно проработанный набор отличительных криминалистических признаков составов рассматриваемых правонарушений. Тем не менее выработка терминологического аппарата и классификация киберпреступлений необходимы для гарантии всесторонности и полноты расследования.

Фомичева О.Л.

Сибирский юридический институт МВД России (г. Красноярск)

К вопросу о соотношении понятий «правопорядок», «общественный порядок», «конституционный правопорядок»

В Конституции РФ закреплен принципцель, который устанавливает, что Россия является правовым государством. Характеризуя правовое государство, исследователи оценивают такой значимый критерий, как уровень правопорядка. Помимо этого понятия часто затрагиваются такие смежные категории, как общественный порядок и конституционный правопорядок. Иногда эти термины используются в тандеме, в отдельных случаях ошибочно даже подменяют друг друга, при этом все названные понятия имеют различное содержание и признаки. Проведение анализа и сравнение этих фундаментальных понятий позволят понять их взаимосвязь и соотношение между собой, а также уяснить отличия.

Говоря о понятиях «правопорядок» и «общественный порядок», можно отметить, что они встречаются в положениях Конституции РФ (п. «б» ч. 1 ст. 72 и п. «е» ч. 1 ст. 114 соответственно). Детализация указанных понятий проводится в иных законодательных актах и подзаконных нормативных правовых актах, что подчеркивает высокую социальную значимость данных категорий. Однако, несмотря на активное использование этих конструкций в отраслевом законодательстве и значительное число научных исследований по данным вопросам, эти социально-правовые категории характеризуются низкой степенью разработанности.

Связующим звеном для обозначенных фундаментальных понятий является термин «порядок». Обратимся к толкованию слова «порядок» в русском языке. Отметим, что это понятие обозначает «состояние налаженности, организованности, благоустроенности; принятое правило; установленная норма для чего-либо»[1]. Термин «порядок» является достаточно распространенным и применяется в различных сферах жизнедеятельности, образуя такие конструкции, как политический порядок, экономический порядок, социальный (гражданский) порядок, правовой порядок, общественный порядок.

Характеризуя категорию «общественный порядок», часть исследователей рассматривают его как всю совокупность социальных связей и отношений, складываю-

[1] Словарь русского языка: в 4 т. / РАН, Ин-т лингвистич. исследований ; род ред. А.П. Евгеньевой. 4-е изд., стер. М. : Рус. яз.; Полиграфресурсы. Фундаментальная электронная библиотека, 1999.