УДК 343.232:004.056
DOI: 10.36979/1694-500X-2024-24-11-167-173

АКТУАЛЬНЫЕ ПРОБЛЕМЫ КЛАССИФИКАЦИИ КИБЕРПРЕСТУПЛЕНИЙ

В.А. Фудашкин

Аннотация. В условиях постоянного развития и совершенствования цифровых технологий и искусственного интеллекта, а также увеличения числа пользователей сети Интернет и социальных сетей становятся все более распространенными и разнообразными киберпреступления. Одной из ключевых проблем, стоящих перед правоохранительными органами и законодательной системой в целом, является построение эффективной системы классификации киберпреступлений. В рамках научной статьи рассматриваются основные проблемы классификации киберпреступлений, а также предлагается классификация данной категории преступлений исходя из таких критериев, как объект киберпреступления, способ его совершения, характер данного противоправного деяния и др. Даются практические рекомендации по совершенствованию законодательства в сфере противодействия совершению преступлений с использованием цифровых технологий.

Ключевые слова: киберпреступления; кибербезопасность; информационная безопасность; искусственный интеллект; информационное пространство; виртуальные активы.

КИБЕР КЫЛМЫШТАРДЫ КЛАССИФИКАЦИЯЛООНУН АКТУАЛДУУ МАСЕЛЕЛЕРИ

В.А. Фудашкин

Аннотация. Санариптик технологиялардын жана жасалма интеллекттин тынымсыз өнүгүшү жана өркүндөтүлүшү, ошондой эле интернет жана социалдык тармактарды колдонуучулардын санынын көбөйүшү менен киберкылмыштар барган сайын кеңири жайылууда жана ар түрдүү болуп баратат. Укук коргоо органдарынын жана бүтүндөй мыйзам чыгаруу системасынын алдында турган негизги көйгөйлөрдүн бири киберкылмыштарды классификациялоонун эффективдүү системасын түзүү болуп саналат. Илимий макаланын алкагында киберкылмыштарды классификациялоонун негизги көйгөйлөрү каралат, ошондой эле киберкылмыштын объектиси, аны жасоо ыкмасы, бул мыйзамсыз аракеттин мүнөзү ж. б. Санариптик технологияларды колдонуу менен кылмыштуулукка каршы күрөшүү чөйрөсүндөгү мыйзамдарды өркүндөтүү боюнча практикалык сунуштар берилген.

Түйүндүү сөздөр: киберкылмыштуулук; киберкоопсуздук; маалыматтык коопсуздук; жасалма интеллект; маалымат мейкиндиги; виртуалдык активдер.

CURRENT PROBLEMS OF CYBER CRIME CLASSIFICATION

V.A. Fudashkin

Abstract. With the development and emergence of digital technologies and artificial intelligence, as well as the increase in the number of users of the Internet and social networks, crimes such as cybercrime are becoming more common and diverse. One of the key problems facing law enforcement agencies and the legislative system as a whole is the construction of an effective system for classifying cybercrimes. This scientific article examines the main problems of the classification of cybercrimes, and also proposes a classification of this category of crimes based on such criteria as the object of the cybercrime, the method of its commission, the nature of this unlawful act, etc. The scientific article provides practical recommendations for improving legislation in the field of combating the commission of crimes using digital technologies.

Keywords: cybercrime; cybersecurity; information security; artificial intelligence; information space; virtual assets.

Современная цифровая эра, известная также как информационная эпоха, начавшись в конце XX века, продолжает свое стремительное развитие, оказывая значительное влияние на все аспекты жизни человечества – от экономики и политики до культуры и социальной сферы.

Эта эра принесла с собой как большое количество возможностей, так и довольно серьезные вызовы в области обеспечения кибербезопасности. В последние десятилетия стремительное развитие информационных технологий и расширение глобальной сети Интернет привело к появлению новых форм противоправных деяний, объединяемых в такую категорию преступлений, как киберпреступления.

Данные преступления, совершаемые с использованием цифровых технологий и искусственного интеллекта, представляют серьезную угрозу для общественной и национальной безопасности, частной жизни граждан, экономической стабильности как в отдельно взятых государствах, так и в региональном и мировом масштабах.

Как определяет ряд авторов, под киберпреступностью понимается совокупность преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, посягающих на информационную безопасность и (или) использующих компьютер, а также иные устройства, обеспечивающие доступ к сети, в качестве орудия (computer-facilitated) либо средства совершения преступления (computer-related). При этом, использование указанных выше технологий повышает эффективность данной преступной деятельности, придавая ей качественно новую форму, делая ее трансграничной, масштабной и трудно раскрываемой [1, с. 129].

Киберпреступления, в силу своей многогранности и постоянно эволюционирующего характера, представляют собой одну из наиболее сложных с правовой точки зрения категорий преступной деятельности. Для эффективного выявления, расследования, пресечения и предупреждения киберпреступлений необходима разработка эффективной и функциональной системы их классификации. Именно установление четких критериев классификации киберпреступлений позволит лучше понять их природу, в том числе с юридической точки зрения, определить специфику и разработать правовые механизмы противодействия.

Анализируя научные изыскания в данной области, мы установили, что авторы, классифицируя киберпреступления, предлагают довольно обширный спектр критериев их разграничения. Так, М.В. Арзамасцев, признавая информационное воздействие отличительной чертой компьютерных преступлений, исходя из характера (направленности) данного способа совершения преступления, классифицирует киберпреступления на:

- информационно-компьютерные (для которых характерно изменение технически компьютерной обрабатываемой информации без воздействия на психику человека или состояние технических устройств);

- информационно-психические (когда при помощи коммуникационных технологий информация адресуется конкретному лицу или неопределенному кругу лиц с интеллектуальным или эмоциональным воздействием);

- информационно-технические (когда информация передается, блокируется, изменяется с целью управляющего или разрушающего воздействия на технические устройства) [2, с. 15].

Б.Э. Шавалеев, анализируя вопрос классификации киберпреступлений, подразделяет их на такие категории, как:

- преступления в сфере компьютерной информации;

- преступления в сфере информационно-телекоммуникационных сетей (технологий);

- преступления в сфере электронных средств платежа;

- иные преступления, сопряженные с использованием информационных технологий [3, с. 95].

Е.В. Христинина, ставя в основу разграничения киберпреступлений предмет, цель и способ совершения, классифицирует данную категорию преступлений на:

- преступления, совершаемые в информационно-телекоммуникационной сфере;

- преступления, совершаемые в киберпространстве с использованием кибертехнологий [4, с. 153].

Нами было установлено, что киберпреступления, объединяющие в себе как самостоятельные составы преступлений, так и «классические» преступления, совершенные с использованием цифровых технологий и искусственного интеллекта, имеют более обширную и разветвленную систему критериев классификации. Их можно классифицировать по таким критериям, как объекты посягательства, на которые они направлены, способы их совершения, характер противоправного деяния и др.

Исходя из объекта посягательства, киберпреступления можно классифицировать на следующие виды.

1. Преступления против информационной безопасности.

Данная категория преступлений направлена на нарушение конфиденциальности, целостности и доступности информации, хранящейся в компьютерных системах. К этим преступлениям мы можем отнести:

- несанкционированный доступ к компьютерной информации, который заключается в незаконном проникновении в компьютерную систему с целью получения, изменения или уничтожения информации (взлом аккаунтов пользователей и др.);
- модификация компьютерных данных, то есть внесение изменений в данные, хранящиеся в компьютерных системах, которые могут привести к серьезным последствиям, таким как искажение финансовой информации или уничтожение важных документов.

2. Преступления против частной жизни граждан.

Эта категория преступлений включает в себя широкий спектр неправомерных действий, направленных на незаконное получение, использование и/или распространение личных персональных данных и другой конфиденциальной информации. Примерами могут служить такие преступления, как:

- кража персональных данных, суть которой заключается в незаконном получении доступа к такой информации личного характера как номера телефонов, паспортные данные, номер социального страхования, адрес проживания лица, данные банковских карт и другие персональные данные, с целью их дальнейшего использования в неправомерных целях и/или последующей реализации другим лицам;
- взлом аккаунтов – взлом аккаунтов социальных сетей, электронной почты и других онлайн-сервисов с целью получения личной информации или шпионажа за частной жизнью граждан, включая чтение личной переписки, просмотр фотографий и другой частной информации;
- доксинг (*«doxing»* или *«doxxing»* – производное от английского слова «docs» – документы). Он представляет собой деятельность, направленную на поиск и/или публикацию персональной или конфиденциальной информации о физическом лице без его согласия. Такие действия не всегда подпадают под уголовную ответственность, однако они нарушают нормы сетевого этикета и часто запрещены внутренними регламентами интернет-сообществ. Мотивами для осуществления доксинга могут быть шантаж, месть или преследование.

3. Преступления в сфере интеллектуальной собственности.

Их сущность заключается в незаконном использовании и/или распространении объектов интеллектуальной собственности, защищенных авторским правом и другими правовыми механизмами. Можно выделить следующие виды преступлений в рамках данной категории:

- пиратство программного обеспечения – незаконное копировании и/или распространении программного обеспечения без лицензии;
- нарушение авторских прав, то есть незаконное использование произведений искусства, литературы, музыки и других объектов интеллектуальной собственности.

4. Преступления против духовно-нравственного здоровья личности (вовлечение в занятие проституцией, распространение предметов порнографического характера, груминг и другие преступления, совершенные с использованием информационных технологий) и др.

В зависимости от способа совершения киберпреступления можно разделить на следующие категории:

1. Мошенничество в сети Интернет.

Интернет-мошенничество включает различные формы обмана, которые осуществляются с целью незаконного завладения имуществом или денежными средствами жертвы преступления. К данной категории можно причислить следующие преступления:

- фишинг (*«phishing»* – производное от английского слова *«fishing»* – рыбная ловля, выуживание) – создание поддельных вебсайтов или рассылка посредством различных сервисов или социальных сетей электронных писем как массового, так и целенаправленного характера, с целью получения личных данных пользователей, таких как пароли, логины и данные банковских карт. Данные письма содержат ссылку на внешне не отличимый от оригинального сайт, либо на сайт с редиректом;
- фарминг (*«pharming»* – производное от английских слов *«phishing»* и *«farming»* – занятие сельским хозяйством, животноводством).

С целью обойти возросшую осведомленность пользователей о фишинговых атаках, злоумышленники разработали механизм скрытого перенаправления пользователей на фишинговые сайты, известный как фарминг. Данный метод заключается в распространении на компьютеры пользователей вредоносных программ, которые после активации перенаправляют запросы к заданным сайтам на поддельные веб страницы. Фарминг обеспечивает высокую скрытность атаки и минимизирует участие пользователя, сводя его к посещению интересующих злоумышленника сайтов. Вредоносные программы, реализующие фарминг-атаку, используют два основных метода для скрытого перенаправления: манипуляция файлом HOSTS или изменение информации DNS. Эти методы позволяют злоумышленникам незаметно перенаправлять трафик пользователей на поддельные сайты, таким образом обеспечивая успешное осуществление преступного замысла;

- спуфинг (производное от английского слова *«spoofing»* – подмена). Маскировка человека либо программы под другую, происходящую посредством фальсификации данных. Выделяют такие разновидности спуфинга как IP/ARP-спуфинг, спуфинг голосовой почты, спуфинг источника отсылки, спуфинг адреса электроной почты, «отравление» файлообменных сетей, спуфинг звонящего, GPS/GNSS-спуфинг и др.);
- мошенничество с использованием нейросетей и дипфейков (производное от английских слов *«deep learning»* – глубинное обучение и *«fake»* – подделка). Дипфейк представляет собой синтез поддельного изображения и/или голоса, созданных с использованием методов машинного обучения и искусственного интеллекта, таких как глубокие нейронные сети. Угроза дипфейков для общественной и национальной безопасности является одним из самых серьезных вызовов современного цифрового общества;
- онлайн-аукционные и торговые мошенничества. В рамках данного вида преступлений происходит обман покупателей через поддельные аукционные сайты или интернет-магазины, предлагающие несуществующие товары или услуги, либо содержащие искаженное описание товара (услуги);
- скама (производное от английского слова *«scam»* – афера, мошенничество) – создание фальшивых проектов Initial Coin Offering (ICO) для обмана инвесторов и кражи их средств.

2. Распространение вредоносного программного обеспечения.

Вредоносное программное обеспечение (черви, вирусы, трояны и т. д.) распространяется с целью повреждения компьютерных систем, кражи данных или получения несанкционированного доступа к информации. К отдельным разновидностям данных программ можно отнести:

- компьютерные вирусы – программы, способные самовоспроизводиться и внедряться в другие программы или файлы, вызывая их повреждение или уничтожение;

- троянские программы – программы, скрывающиеся под видом легитимного программного обеспечения, но выполняющие вредоносные действия, такие как кража данных или удаленное управление компьютером;
- сетевой червь – разновидность вредоносного программного обеспечения, способного самостоятельно распространяться через локальные и глобальные компьютерные сети. Данная категория вредоносных программ может негативно влиять на производительность устройства жертвы, удалять файлы или отключать определенные программы;
- программа – вымогатель (*«ransomware»* – производное от английских слов *«ransom»* – выкуп и *«software»* – программное обеспечение), известная также как программа-шантажист или винлокер (производное от английского слова *«winlocker»* – блокировщик Windows), представляет собой вид вредоносного программного обеспечения, предназначенного для вымогательства. Данное программное обеспечение блокирует доступ к компьютерной системе или предотвращает считывание записанных в ней данных, зачастую используя методы шифрования. После блокировки система требует от пользователя выплату выкупа для восстановления исходного состояния доступа к данным или системе.

3. Атаки на компьютерные системы.

Данные атаки направлены на нарушение нормального функционирования компьютерных систем и могут включать:

- DDS/DDoS-атаки – массовые запросы к серверу с целью его перегрузки и выведения из строя;
- атаки с использованием уязвимостей – использование уязвимостей в программном обеспечении для получения несанкционированного доступа к компьютерным системам.

В зависимости от характера (направленности) противоправного деяния, киберпреступления можно подразделить на такие категории как:

1. Финансово-ориентированные киберпреступления. Эти преступления направлены на получение материальной выгоды и включают такие виды как:

- вымогательство – запрос денежных средств за неразглашение компрометирующей информации или за восстановление доступа к заблокированной системе;
- кража финансовых данных – незаконное получение и/или использование данных банковских карт и счетов для проведения финансовых операций.

2. Киберпреступления, направленные на причинение вреда. Эти преступления преследуют цель нанесения ущерба конкретным лицам, организациям, либо обществу или государству в целом:

- кибертерроризм – умышленные действия, совершенные с использованием информационно-коммуникационных технологий, направленные на подрыв общественной и национальной безопасности, устрашение населения государства и создание у него паники, а также нанесение ущерба государственным и частным учреждениям. Эти действия включают атаки на компьютерные сети, системы управления критической инфраструктуры, распространение дезинформации и другие формы деятельности, преследующие террористические цели;
- кибершпионаж – незаконное проникновение в компьютерные системы с целью получения секретной и конфиденциальной информации, относящейся к государственной или коммерческой тайне. Такие противоправные действия могут включать взлом компьютерных систем, перехват данных, установку шпионского программного обеспечения и другие формы кибератак.

3. Киберпреступления психофизиологической направленности. представляют собой действия, направленные на причинение вреда психическому и физическому здоровью человека с использованием информационно-коммуникационных технологий. Такие преступления могут включать кибербуллинг, кибersталкинг, распространение дезинформации, манипуляцию сознанием и другие формы воздействия. Жертвы данной категории киберпреступлений могут испытывать постоянное психологическое

давление, тревожность, депрессию и другие психические расстройства.

Психическое воздействие может также вызвать физические болезни, такие как головные боли, нарушения сна, сердечно-сосудистые заболевания привести к суицидальной идеации и самоубийству, особенно среди подростков и уязвимых групп населения. К ним мы можем отнести:

- кибербуллинг (киберпреследование, кибермоббинг, троллинг, флейм) – преследование и запугивание граждан посредством таких информационно-коммуникационных каналов и средств как социальные сети, электронная почта, программы для мгновенного обмена сообщениями, форумы, а также размещение на видеопорталах компрометирующих видеоматериалов и сообщений (часто содержащих обсценную лексику) или посредством мобильных телефонов (например, с помощью SMS-сообщений или назойливых звонков);
- кибersталкинг – использование сети Интернет для преследования или домогательств в отношении физического лица, группы лиц или организации. Под данные действия подпадают ложные обвинения, распространение сплетен и клеветы. К кибersталкингу также относятся похищение личности, угрозы, акты вандализма, вымогательство сексуальных услуг или сбор информации, которая может быть использована для запугивания или домогательств;
- распространение интимных материалов – действие по публичному распространению изображений или видеозаписей интимного характера без согласия лиц, изображённых на них. Распространение интимных материалов может осуществляться различными способами, включая: социальные сети, мессенджеры, электронная почта, веб-сайты и т. д.

В зависимости от мотивов совершения киберпреступлений, их можно подразделить на:

- преступления, совершаемые с целью получения финансовой выгоды (скимминг, претекстинг, кража данных, кража криптовалют и др.);
- преступления, совершаемые по политическим мотивам (кибертерроризм, кибершпионаж, атаки на государственные структуры и др.);
- преступления, совершаемые по личным мотивам (кибersталкинг, кибербуллинг и др.);
- преступления, совершаемые по идеологическим мотивам (атаки на системы и данные в целях распространения идеологии или убеждений, хактивизм и др.).

По территории совершения преступления, киберпреступления можно подразделить на:

- внутригосударственные преступления;
- транснациональные преступления.

Исходя из проведенного анализа нами были установлены следующие основные проблемы классификации киберпреступлений:

1. Многообразие киберпреступлений. Киберпреступления охватывают широкий спектр противоправных деяний, от кибермошенничества и кибершпионажа до кибертерроризма и кибербуллинга. Каждое из данных преступлений имеет свои особенности, мотивы, методы и способ совершения, что затрудняет их классификацию по единой системе.

2. Отсутствие единой системы классификации киберпреступлений. На международном уровне отсутствует единый подход к классификации киберпреступлений, так как различные страны используют свои собственные классификационные системы, что, в свою очередь, затрудняет международное сотрудничество в борьбе с киберпреступностью. Это связано с различиями в правовых системах государств, а также уровне их технологического развития.

3. Сложность технической стороны киберпреступлений также является значительным препятствием для их классификации. Современные киберпреступления часто используют сложные методы и инструменты, такие как шифрование, анонимные сети, вредоносное программное обеспечение и искусственный интеллект, что усложняет их идентификацию и классификацию.

4. Быстрый процесс эволюции киберпреступлений. Киберпреступления постоянно эволюционируют и приспосабливаются к новым технологиям и методам защиты от них, что

создает необходимость в постоянном обновлении классификационных систем.

Проанализировав многогранность критериев классификации киберпреступлений, мы пришли к выводу, что данная категория преступлений представляет собой серьезную угрозу не только для частной жизни граждан, но также для информационной, экономической и национальной безопасности государства. Многообразие и сложность квалификации киберпреступлений требуют комплексного подхода к процессу их правового регулирования, включающего совершенствование национального законодательства, международное сотрудничество, развитие институциональных механизмов противодействия, а также разработку превентивных мер. Только такой комплексный подход позволит эффективно противостоять киберпреступлениям и защитить права и интересы всех участников информационного пространства.

Поступила: 12.06.24; рецензирована: 26.06.24;
принята: 28.06.24.

Литература

1. *Витвицкая С.С.* Киберпреступления: понятие, классификация, международное противодействие / С.С. Витвицкая, А.А. Витвицкий, Ю.И. Исакова // Правовой порядок и правовые ценности. 2023. Т. 1. № 1.
2. *Арзамасцев М.В.* К вопросу об уголовно-правовой классификации киберпреступлений / М.В. Арзамасцев // Актуальные вопросы права и отраслевых наук. 2017. № 1(3).
3. *Шавалеев Б.Э.* Классификация киберпреступлений / Б.Э. Шавалеев // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 3(49).
4. *Христинина Е.В.* К вопросу об уголовно-правовом противодействии киберпреступности / Е.В. Христинина // Вестник Сибирского юридического института МВД России. 2021. № 4(45).