DOI 10.25587/2587-5612-2024-3-17-21 УДК 343.9

Понятие киберпреступления и его характеризующие признаки

А. Е. Григорьева
Северо-Восточный федеральный университет им. М.К. Аммосова, г. Якутск, Россия

Аннотация. В статье исследуется понятие киберпреступления и его признаков. Проанализированы содержащиеся в правовых источниках и предлагаемые в научной литературе определения данного понятия. Отмечено, что его содержание подвержено изменениям, вызванным развитием современных технологий и трансформацией способов совершения преступлений с их использованием. Возникает необходимость исследования и выделения характерных признаков киберпреступления, позволяющих отграничить его от иных преступных деяний. Выделены и обозначены характерные признаки киберпреступлений.

Ключевые слова: киберпреступность, киберпреступление, информационные технологии, компьютерные технологии, информационно-телекоммуникационные технологии, компьютерная информация.

The concept of cybercrime and its characteristic features

A. E. Grigorieva
M.K. Ammosov North-Eastern Federal University, Yakutsk, Russia

Abstract. The article examines the concept of cybercrime and its characteristics. The definitions of this concept contained in legal sources and proposed in scientific literature are analyzed. It is noted that its content is subject to changes caused by the development of modern technologies and the transformation of the methods of committing crimes using them. There is a need to study and identify the characteristic features of cybercrime, allowing it to be distinguished from other criminal acts. The characteristic features of cybercrimes are identified and designated.

Keywords: cybercrime, cybercrime, information technology, computer technology, information and telecommunication technology, computer information.

В эпоху глобализации и интенсивного развития информационно-коммуникационных технологий киберпространство становится не только средой новых возможностей для экономического и социального развития, но и ареной совершения различных видов преступлений. Технологический прогресс за последние десятилетия кардинальным образом изменил облик нашего общества, привнеся значительные улучшения практически во все сферы деятельности человека. Это привело к увеличению доступности информации, улучшению качества жизни и расширению возможностей для глобального взаимодействия и сотрудничества на беспрецедентных уровнях.

Современные технологии одновременно открывают новые возможности и для противозаконной деятельности. Развитие технологических возможностей с каждым годом включает все большее разнообразие противоправных деяний, составляющих содержание кибер-

---

ГРИГОРЬЕВА Ачена Егоровна – кандидат юридических наук, доцент, доцент кафедры «Уголовное право и процесс», Юридический факультет, Северо-Восточный федеральный университет имени М.К. Аммосова.

E-mail: achenag@mail.ru

GRIGORIEVA Achena Egorovna – Candidate of Judicial Sciences, Associate Professor, Associate Professor Department of Criminal Law and Process, Faculty of Law, M.K. Ammosov North-Eastern Federal University.

преступности. Способствующими распространению киберпреступности можно назвать следующие факторы. Цифровизированность современной жизни приводит к увеличению количества цифровых данных, доступных в киберпространстве и, как следствие, прорывной рост преступного их использования.

Отслеживание киберпреступности усложняется фактами анонимности и трансграничного характера интернета. К тому же законодательное регулирование во многих странах еще не адаптировано к быстро меняющемуся технологическому миру, создавая некие правовые «серые зоны», которые могут быть использованы злоумышленниками. Увеличение числа пользователей, обладающих компьютерными навыками, также способствует росту количества потенциальных киберпреступников.

Кроме того, значительная экономическая выгода, которую можно получить от киберпреступлений, делает этот вид преступной деятельности особенно привлекательным. Все эти факторы в совокупности обуславливают необходимость более пристального внимания к проблеме киберпреступности со стороны государственных органов и международного сообщества.

Общепризнанное положение, что киберпреступление представляет собой противоправное действие, нарушающее уголовное законодательство, и совершается путем использования информационных технологий. Данный вид преступлений, как правило, направлен на компьютерные системы, сети, конфиденциальные данные с целью совершения преступлений, таких как мошенничество, кража, шантаж или несанкционированный доступ к информации.

Анализируя научные источники и различные нормативно-правовые акты, выделим несколько моментов, которые характерны для киберпреступности и определяют ее понятие.

В международной практике тенденция к широкому толкованию киберпреступлений стала особенно заметной после X Конгресса ООН [1] по предупреждению преступности и обращению с правонарушителями в 2000 г., а также с принятием Конвенции о киберпреступности в 2001 г. в Будапеште [2].

С. С. Витвицкая, А. А. Витвицкий и Ю. И. Исакова критикуют подходы, ограничивающие противодействие киберпреступлениям только рамками компьютерной безопасности, игнорирующих использование информационно-телекоммуникационных технологий в военно-политических конфликтах и в других формах международной подрывной деятельности. Также подчеркивается необходимость учета возможностей мобильного доступа в Интернет для совершения киберпреступлений, что не всегда учитывается в международных документах. Они предлагают следующее понятие киберпреступности, трактуя ее как «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 либо средства совершения преступления» [3, с. 126–136]. Такой подход к определению понятия киберпреступности, считаем, действительно отражает всю полноту этого термина, тем самым, как бы, дополняя ранее выдвинутые другими авторами определения.

К. Ю. Рябинин представил определение киберпреступления как «уголовно-наказуемое деяние, совершенное в среде, образованной взаимодействием совокупности коммуникационных каналов Интернета и других сетей (киберпространство), необходимым и обязательным элементом механизма совершения которого является компьютерная информация, выступающая в качестве предмета или способа реализации преступного посягательства» [4, с. 46–48].

С. Б. Клестов в своей работе обозначил характерные признаки киберпреступлений:

«1) совершение киберпреступления не требует передвижений, активных физических действий и сил (человек все делает, находясь стационарно на одном месте: в офисе, дома, кафе, клубе, т.е. там, где есть доступ в интернет);

2) киберпространство предоставляет идеальные условия для сокрытия преступлений, основными факторами являются: идеальная среда (киберпреступники играют роль законопослушных граждан); самодостаточность киберпространства как социальной системы (в ней есть и культурные, и экономические, и социальные институты, которые позволяют преступникам чувствовать себя как рыба в воде);

3) общие особенности среды совершения киберпреступлений (среда напрямую влияет на психологию киберпреступников);

4) виктимологические особенности совершения преступлений;

5) сеть, виртуальное пространство незаметно влияет на поведение, «растворяет» человека в нем (преступник–потерпевший, преступник–электронное устройство);

6) хакер работает в комфортных условиях (у него отсутствует чувство страха быть задержанным, обнаруженным, привлеченным к уголовной ответственности и пр.);

7) обратная связь ограничивается, мы ее не чувствуем и не ощущаем (пиратские видеофайлы, можем их свободно скачать, не осознавая, что совершаем преступление);

8) вред, который причиняется гражданам визуально, не виден (отсутствует осознание того, что причиняется кому-то вред);

9) анонимность, также позволяет ощущать безнаказанность в совершении действий, проступков (деликтов), преступлений;

10) так как в киберпространстве все происходит в режиме анонимности, то многие граждане создают новый образ собственной личности, а иногда даже несколько образов одновременно, параллельно своему естественному образу;

11) интернет-зависимость, расстройства личности (онлайн-игры несут свою особенность: вымышленный мир и анонимность приводят к этим проблемам);

12) перегрузка социальными контактами приводит к тому, что утрачивается способность и возможность сосредоточения внимания на конкретном отдельном человеке (это приводит к агрессии; обесценивается каждый контакт, особенно на своем личном фоне)» [5, с. 228–231].

Полностью согласны, что все эти признаки характерны для киберпреступлений и они отличают его от других видов преступлений. Отметим, что представленные понятия и признаки киберпреступности обладают рядом общих характеристик, отражающих их сущность и ключевые аспекты: во-первых, они совершаются с использованием информационно-коммуникационных технологий (компьютерных систем, сетей и цифровых устройств); во-вторых, направлены на причинение вреда, посягательство на информационную безопасность или получение незаконной выгоды.

В Уголовном кодексе Российской Федерации (далее – УК РФ) отсутствует понятие «киберпреступления». К ним принято относить преступления в сфере компьютерной информации (глава 28 УК РФ). В содержание данной главы УК РФ включены следующие составы: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ); нарушение правил централизованного управления техническими

средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ).

В разъясняющем Постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 раскрывается содержание указанных преступных действий. Но самыми ключевыми, полагаем, являются разъяснения, раскрывающие понятия «компьютерной информации» и «компьютерных устройств», в привязке к которым изначально с первых международных документов по киберпреступности раскрывалось содержание киберпреступления. Так, к числу компьютерных устройств могут быть отнесены «любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом» [6]. Данное разъяснение отчасти снимает разночтения для правоприменителя при сложившемся терминологическом разнообразии в названиях: киберпреступления, преступления в сфере каких-либо технологий (информационных, информационно-коммуникационных, электронных, цифровых) или с их использованием.

В УК РФ, кроме того, предусмотрены составы, указывающие на использование электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», при совершении иных преступных деяний, не относящихся, по мнению отдельных исследователей, ккиберпреступлениям. Например, в п. «б» ч. 2 ст. 228.1 УК РФ – сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») и многие другие.

В этой связи поддерживаем позицию К. Г. Мамцова и Н. Р. Ачилова, выделявшим две категории преступлений, которые присущи практически ко всем киберпреступлениям: преступная деятельность, целью которой являются сами компьютеры и преступная деятельность, в которой компьютеры используются для совершения других преступлений [7].

Таким образом, понятие киберпреступления следует, по нашему мнению, трактовать шире, включая в него не только преступные деяния, содержащиеся в главе 28 УК РФ, но и более широкий спектр преступных действий, которые совершаются не только в сфере компьютерной информации, но и с ее использованием. Обязательным элементом механизма совершения киберпреступления будет являться компьютерная информация, выступающая в качестве предмета или способа реализации преступного посягательства.

Литература

1. X Конгресс ООН по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 г.).–URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_R.pdf (дата обращения: 04.09.2024).

2. Конвенция о преступности в сфере компьютерной информации ETSN 185 (Будапешт, 23 ноября 2001 г.) // СПС Гарант. – URL: https://base.garant.ru/4089723/ (дата обращения: 21.09.2024).

3. 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. – С. 126–136. – DOI 10.23947/2949-1843-2023-1-1-126-136. – EDNOKGPLW.

4. Рябинин, К. Ю. Понятие и признаки киберпреступлений / К. Ю. Рябинин // Colloquium-Journal. – 2020. – № 5–8(57). – С. 46–48. – EDNMXNGIM;

5. Клестов, С. Б. К вопросу о киберпреступности (психологический аспект) / С. Б. Клестов // Психолого-гуманитарный ресурс технического вуза: сборник научных трудов Всероссийской научно-практической конференции, Хабаровск, 22–23 апреля 2021 года / под ред. Н. Г. Григорьевой и А. А. Лежениной. – Хабаровск: Дальневосточный государственный университет путей сообщения, 2021. – С. 228–231. – EDNPIFAXD.

6. Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «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». – Бюллетень Верховного Суда Российской Федерации. – март 2023 г. – №3.

7. Мамцов, К. Г., Ачилов, Н. Р. Киберпреступность как угроза национальной безопасности / К. Г. Мамцов, Н. Р. Ачилов// Молодой исследователь Дона. –2022. –№ 1 (34). –URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-ugroza-natsionalnoy-bezopasnosti (дата обращения: 24.09.2024).

References

1. H Kongress OON po preduprezhdeniyu prestupnosti i obrashcheniyu s pravonarushitelyami (Vena, 10–17 aprelya 2000 g.).–URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_R.pdf (data obrashcheniya: 04.09.2024).

2. Konvenciya o prestupnosti v sfere komp'yuternoj informacii ETSN 185 (Budapesht, 23 noyabrya 2001 g.) // SPS Garant. – URL: https://base.garant.ru/4089723/ (data obrashcheniya: 21.09.2024).

3. Vitvickaya, S. S. Kiberprestupleniya: ponyatie, klassifikaciya, mezhdunarodnoe protivodejstvie / S. S. Vitvickaya, A. A. Vitvickij, Yu. I. Isakova // Pravovoj poryadok i pravovye cennosti. – 2023. – T. 1, № 1. – S. 126–136. – DOI 10.23947/2949-1843-2023-1-1-126-136. – EDNOKGPLW.

4. Ryabinin, K. Yu. Ponyatie i priznaki kiberprestuplenij / K. Yu. Ryabinin // Colloquium-Journal. – 2020. – № 5–8(57). – S. 46–48. – EDNMXNGIM;

5. Klestov, S. B. K voprosu o kiberprestupnosti (psihologicheskij aspekt) / S. B. Klestov // Psihologo-gumanitarnyj resurs tekhnicheskogo vuza: sbornik nauchnyh trudov Vserossijskoj nauchno-prakticheskoj konferencii, Habarovsk, 22–23 aprelya 2021 goda / pod red. N. G. Grigor'evoj i A. A. Lezheninoj. – Habarovsk: Dal'nevostochnyj gosudarstvennyj universitet putej soobshcheniya, 2021. – S. 228–231. – EDNPIFAXD.

6. Postanovlenie Plenuma Verhovnogo Suda Rossijskoj Federacii ot 15 dekabrya 2022 g. № 37 «O nekotoryh voprosah sudebnoj praktiki po ugolovnym delam o prestupleniyah v sfere komp'yuternoj informacii, a takzhe inyh prestupleniyah, sovershennyh s ispol'zovaniem elektronnyh ili informacionno-telekommunikacionnyh setej, vklyuchaya set' «Internet». – Byulleten' Verhovnogo Suda Rossijskoj Federacii. – mart 2023 g. – №3.

7. Mamcov, K. G., Achilov, N. R. Kiberprestupnost' kak ugroza nacional'noj bezopasnosti / K. G. Mamcov, N. R. Achilov// Molodoj issledovatel' Dona. –2022. –№ 1 (34). –URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-ugroza-natsionalnoy-bezopasnosti (data obrashcheniya: 24.09.2024).