Научная статья

УДК 343.3
DOI 10.25205/2542-0410-2023-19-3-17-22

Уголовно-правовые аспекты кибербезопасности

Роман Николаевич Боровских

Новосибирский национальный исследовательский государственный университет
Новосибирск, Россия

borovskih80@yandex.ru

Аннотация

В статье рассматриваются вопросы уголовного законодательства РФ об ответственности за преступления в сфере кибербезопасности. Автором анализируется уголовно-правовое содержание данного термина, его юридические границы. На основе исследования формулируются несколько подходов к решению указанной проблемы.

Ключевые слова

уголовное право, преступления в сфере компьютерной информации, кибербезопасность, киберпреступления

Для цитирования

Боровских Р. Н. Уголовно-правовые аспекты кибербезопасности // Юридическая наука и практика. 2023. Т. 19, № 3. С. 17–22. DOI 10.25205/2542-0410-2023-19-3-17-22

Criminal Legal Aspects of Cybersecurity

Roman N. Borovskikh

Novosibirsk State University
Novosibirsk, Russian Federation

borovskih80@yandex.ru

Abstract

The article deals with the issues of the criminal legislation of the Russian Federation on liability for crimes in the field of cybersecurity. The author analyzes the criminal-legal content of this term, its legal boundaries. Based on the study, several approaches are formulated to solve this problem.

Keywords

criminal law, crimes in the field of computer information, cybersecurity, cybercrime

For citation

Borovskikh R. N. Criminal legal aspects of cybersecurity. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 17–22. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-17-22

По данным официальной уголовной статистики [1, с. 31], в 2022 г. в России зарегистрировано 1 966,8 тыс. преступлений, из которых более четверти (522 тыс.) составили преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Важно отметить, что в числе данных преступлений свыше 272 тыс. тяжких и особо тяжких (52 %).

Авторы отчета ГИАЦ МВД России оперируют термином, который включает в себя две группы преступлений: первая – преступления, совершенные с использованием информационно-телекоммуникационных технологий; вторая – преступления в сфере компьютерной информации. При этом обе данные группы, согласно отчету, охватывают широкий спектр уголовно наказуемых деяний, в числе которых:

– кража (ст. 158 УК РФ);

– мошенничество и его разновидности (ст. 159, 159.3, 159.6 УК РФ);

– незаконные организация и проведение азартных игр (ст. 171.2 УК РФ);

– публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ);

– незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ);

– изготовление порнографических материалов (ст. 242, 242.1, 242.2 УК РФ);

– публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ);

– преступления в сфере компьютерной информации (глава 28 УК РФ).

Как видно, к числу «компьютерных» преступлений отнесены преступления различных родов и видов.

Критериями, на основании которых авторы отчета МВД РФ объединили вышеперечисленные преступления в одну группу для статистического измерения, были определены следующие:

– совершение преступления с использованием или применением расчетных (пластиковых) карт (речь идет о средствах совершения преступления);

– использование для преступных целей компьютерной техники, программных средств, фиктивных электронных платежей, сети «Интернет», средств мобильной связи (подразумеваются способы совершения преступлений).

Таким образом, с одной стороны, вышеприведенные сведения определенным образом формируют представление о том, что, по мнению аналитиков МВД РФ, содержательно означают категории «преступление, совершенное с использованием информационно-телекоммуникационных технологий и «преступление в сфере компьютерной информации». Выразим согласие с необходимостью столь широкого подхода в их понимании. Вместе с тем становится понятным, что определенных уголовно-правовых границ первая из рассматриваемых категорий не имеет, равно как и нет четкого понимания ее соотношения со второй категорией, которая формально ограничена главой 28 УК РФ. В связи с этим можно констатировать отсутствие четких дефинитивных границ рассматриваемых групп преступлений (отметим, что понятие «преступление в сфере компьютерной информации», несмотря на указанную одноименную главу, может также иметь более широкую, выходящую за пределы данной главы трактовку; например, когда речь идет о включении в число таких преступлений мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) или ряда иных преступлений).

В научной литературе широко обсуждается вопрос о терминологическом аппарате уголовно-правового противодействия рассматриваемым преступлениям. В числе прочего предлагаются к использованию (в том числе в нормативном аспекте) категории «киберпреступление» или «преступление в сфере кибербезопасности» [2; 3] При этом под киберпреступлениями предлагается понимать любые преступления, которые совершаются в киберпространстве (информационном пространстве) с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных [4, с. 48].

В целом, соглашаясь с возможностью использования в уголовно-правовом лексиконе понятий «киберпреступление» или «преступление в сфере кибербезопасности» (далее будем

рассматривать их равнозначными), попробуем определить критерии, на основании которых конкретное преступление следует относить к числу таковых. Но прежде несколько слов о сочетаемости в уголовно-правовом дискурсе терминов «кибер» и «безопасность».

Во-первых, уголовно-правовой принцип гуманизма предусматривает, что уголовное законодательство России обеспечивает *безопасность* (курсив мой. – *Р. Б.*) человека (ст. 7 УК РФ). Таким образом, категория «безопасность» не только имеет нормативное употребление, но возведена в ранг принципиальных положений Уголовного закона, что определяет ее широкое юридическое значение, в том числе для целей классификации преступлений. В связи с этим отметим, что в Особенной части УК РФ термин «безопасность» употребляется 72 раза, включая 4 раза для терминологического определения отдельных родов и видов преступления (преступления против общественной безопасности, преступления против безопасности движения, преступления против безопасности государства, преступления против безопасности человечества).

Во-вторых, понятие кибернетики не столь эклектично по отношению к правовым категориям, как может показаться при первом приближении. Так, сформулированное в 1948 г. американским математиком Н. Винером определение, на наш взгляд, дает возможность весьма полно определить перечень определенных критериев, на основании которых можно говорить о деяниях в киберпространстве и сфере кибербезопасности.

Согласно определению Н. Винера, кибернетика – это наука об общих закономерностях *процессов управления и передачи информации* (курсив мой. – *Р. Б.*) в машинах, живых организмах и обществе. Заметим, что понимание вышеуказанных процессов может в уголовно-правовом дискурсе осуществляться с позиций объекта и предмета преступления, общественно опасных деяния и последствий, способа, орудий, средств и обстановки совершения преступления, а также в определенной интерпретации служить цели формулирования признаков специального субъекта рассматриваемых преступлений. Такая универсальность позволяет охватить весьма широкие границы понятия «киберпреступление», на что справедливо указывают многие специалисты [5, с. 59–60].

Теперь о видах преступлений в сфере кибербезопасности.

Анализ действующего уголовного законодательства РФ показывает, что с учетом сказанного выше взгляд на преступление в сфере кибербезопасности может быть очень широким. Так, к числу рассматриваемых преступлений, кроме тех, которые непосредственно связаны с компьютерной техникой, компьютерной информацией, информационно-телекоммуникационными сетями (в том числе Интернетом), электронными средствами передачи информации и платежа, средствами хранения, обработки или передачи компьютерной информации и т. д., могут быть отнесены многочисленные преступные деяния, в описании состава которых не содержится упоминания вышеперечисленных признаков.

Например, ч. 1 ст. 138 УК РФ предусматривает ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. При этом в судебной практике под иными сообщениями понимаются сообщения граждан, передаваемые по сетям электрической связи, например СМС- и ММС-сообщения, факсимильные сообщения, передаваемые посредством сети «Интернет» мгновенные сообщения, электронные письма, видеозвонки и пр.

В ст. 276 УК РФ установлена ответственность за шпионаж в форме передачи, собирания, похищения или хранения в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну. Очевидно, что собирание и похищение указанных сведений может осуществляться с использованием компьютерной техники и т. п.

Еще один пример. В соответствии со ст. 290 УК РФ, предметом взятки может выступать незаконное предоставление имущественных прав, под которыми понимаются в том числе доходы от использования *цифровых пра*в (курсив мой. – *Р. Б.*). Кроме этого, Пленум Верховного

суда РФ в Постановлении от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» отдельно разъясняет вопросы применения уголовного закона РФ, когда предмет взятки передается в виде зачисления денежных средств на «электронный кошелек».

Можно привести много других подобных примеров, которые служат свидетельством, что «киберпреступление» в самом широком понимании имеет место и в случаях, когда законодательное описание состава преступления не содержит прямого указания на «кибер»-признаки, в том числе «кибер»-характер.

С другой стороны, столь широкий подход вряд ли может оказаться продуктивным, если речь идет о решении задачи формулирования киберпреступлений как отдельного вида преступлений. В данном случае полезно выделить в тексте УК РФ и перечислить те признаки преступлений, которые позволяют относить данные преступления к категории «кибер».

Анализ показывает, что соответствующими признаками выступают несколько групп признаков (далее приводятся формулировки в точном соответствии с УК РФ).

Первая группа признаков связана с характеристикой объекта и предмета преступного посягательства, а именно:

1) совершение преступления **«в сфере компьютерной информации»** (гл. 28, ст. 272–274.2 УК РФ);

2) совершение преступления в отношении **«электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств»** (гл. 22, ст. 187 УК РФ).

Вторая группа признаков в различных аспектах характеризует обстановку, орудия, средства либо способ совершения преступления. В числе таковых:

1) совершение преступления **«в информационно-телекоммуникационных сетях (включая сеть «Интернет»)»**:

– доведение до самоубийства (гл. 16, ст. 110 УК РФ);

– склонение к совершению самоубийства или содействие совершению самоубийства (гл. 16, ст. 110.1 УК РФ);

– клевета (гл. 17, ст. 129.1 УК РФ);

– нарушение неприкосновенности частной жизни (гл. 19, ст. 137 УК РФ);

2) совершение преступления **«путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей»**: мошенничество в сфере компьютерной информации (гл. 21, ст. 159.6 УК РФ);

3) совершение преступления **«с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)»**:

– жестокое обращение с животными (гл. 25, ст. 245 УК РФ);

– незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (гл. 26, ст. 258.1 УК РФ);

4) совершение преступления **«с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)»**:

– организация деятельности, направленной на побуждение к совершению самоубийства (гл. 16, ст. 110.2 УК РФ);

– понуждение к действиям сексуального характера (гл. 18, ст. 133 УК РФ);

– вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (гл. 20, ст. 151.2 УК РФ);

– незаконные организация и проведение азартных игр (гл. 22, ст. 171.2 УК РФ);

– манипулирование рынком (гл. 22, ст. 185.3 УК РФ);

– публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (гл. 24, ст. 205.2 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия, основных частей огнестрельного оружия, боеприпасов (гл. 24, ст. 222 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств (гл. 24, ст. 222.1 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему (гл. 24, ст. 222.2 УК РФ);

– незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (гл. 25, ст. 228.1 УК РФ);

– склонение к потреблению наркотических средств, психотропных веществ или их аналогов (гл. 25, ст. 230 УК РФ);

– обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок (гл. 25, ст. 238.1 УК РФ);

– незаконные изготовление и оборот порнографических материалов или предметов (гл. 25, ст. 242 УК РФ);

– изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (гл. 25, ст. 242.1 УК РФ);

– использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (гл. 25, ст. 242.2 УК РФ);

– публичные призывы к осуществлению экстремистской деятельности (гл. 29, ст. 280 УК РФ);

– публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (гл. 29, ст. 280.1 УК РФ);

– публичные призывы к осуществлению деятельности, направленной против безопасности государства (гл. 29, ст. 280.4 УК РФ);

– возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (гл. 29, ст. 282 УК РФ);

– реабилитация нацизма (гл. 34, ст. 354.1 УК РФ).

Отметим, что в подавляющем большинстве случаев признаки «киберпреступления» указываются законодателем в рамках квалифицированных составов соответствующих преступлений.

Таким образом, можно выделить несколько возможных подходов к определению уголовно-правового содержания термина «преступление в сфере кибербезопасности».

Первый – максимально широкий: это преступление, объективные элементы состава которого не содержат вышеперечисленных признаков (например, «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», но фактические обстоятельства совершения преступления свидетельствуют о наличии таковых.

При таком понимании, едва ли не каждое преступное деяние, предусмотренное УК РФ, может при определенных обстоятельствах обладать признаками «киберпреступления».

Второй – максимально узкий: это преступление, предусмотренное главой 28 УК РФ, объектом посягательства которого выступают общественные отношения в сфере кибербезопасности.

Выше можно было убедиться, что такой подход является усеченным.

Третий – сбалансированный: это преступление, состав которого содержит прямое указание на вышеперечисленные объективные признаки (например, объектом преступления выступают отношения в сфере критической информационной инфраструктуры РФ; предметом – компьютерная программа; способ совершения преступление – использование сети «Интернет» и т. д.).

Список литературы

1. Состояние преступности в России за январь-декабрь 2022 года / Отчет Главного информационно-аналитический центра МВД России [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 12.05.2023).
2. **Данилов Р. М., Рыбак А. В.** Некоторые вопросы, связанные с преступлениями в сфере кибербезопасности // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2022. № 8. С. 45–51.
3. **Никульченкова Е. В.** О необходимости введения дефиниции «киберпреступление» в Уголовный закон Российской Федерации // Вестник Омского ун-та. Серия: Право. 2022. Т. 19, № 3. С. 98–107.
4. **Номоконов В. А., Тропина Т. Л.** Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55.
5. **Джафарли В. Ф.** Терминологические основы уголовно-правового обеспечения криминологической кибербезопасности (часть 2) // Ученые труды Российской академии адвокатуры и нотариата. 2022. № 2 (65). С. 56–61.

References

1. **The state of crime** in Russia for January-December 2022 / Report of the Main Information and Analytical Center of the Ministry of Internal Affairs of Russia [Electronic resource]. URL: https://mvd.rf/reports/item/35396677 (date of access: 05.12.2023).
2. **Danilov R. M., Rybak A. V.** Some issues related to cybersecurity crimes // Crime in the field of information and telecommunication technologies: problems of prevention, detection and investigation of crimes. 2022. No. 8. Pp. 45–51.
3. **Nikulchenkova E. V.** On the need to introduce the definition of “cybercrime” in the Criminal Law of the Russian Federation // Bulletin of the Omsk University. Series “Law”. 2022. Vol. 19, no. 3. Pp. 98–107.
4. **Nomokonov V. A., Tropina T. L.** Cybercrime as a new criminal threat // Criminology yesterday, today, tomorrow. 2012. No. 1 (24). Pp. 45–55.
5. **Jafarli V. F.** Terminological bases of criminal law support of criminological cybersecurity (part 2) // Scientific works of the Russian Academy of Advocacy and Notaries. 2022. No. 2 (65). Pp. 56–61.

Информация об авторе

Роман Николаевич Боровских, доктор юридических наук

Information about the Author

Roman N. Borovskikh, Doctor of Law

Статья поступила в редакцию 15.05.2023;
одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 15.05.2023;
approved after reviewing 21.06.2023; accepted for publication 31.07.2023