

УДК 34**DOI: 10.34670/AR.2020.63.34.037****Специфика правового регулирования киберпреступлений,
совершаемых преступной группой****Алексеев Сергей Владимирович**

Кандидат юридических наук, доцент,
доцент кафедры гражданского и арбитражного процесса,
Самарский государственный экономический университет,
443090, Российская Федерация, Самара, ул. Советской Армии, 141;
e-mail: ecun@sseu.ru

Аннотация

В данной статье рассмотрены новый вид преступности, который ранее не был широко известен - преступность в сфере высоких технологий. Предлагается определение понятия киберпреступность. В статье подробно рассмотрена изученная автором мировая уголовно-правовая практика противодействия киберпреступлениям, совершённым в группе. Рассмотрены основные виды преступных посягательств в области информационных технологий. Приводятся подробные статистические данные по преступлениям, совершённым в России в IT сфере. В статье объясняются причины некоторого снижения киберпреступлений в России. Однако, несмотря на это, правовое регулирование данной сферы не должно стоять на месте. В статье обосновывается необходимость законодательного расширения главы 28 УК РФ «Преступления в сфере компьютерной информации», путём внесения в неё новых норм, предусматривающих ответственность за преступления в сфере высоких технологий.

Для цитирования в научных исследованиях

Алексеев С.В. Специфика правового регулирования киберпреступлений, совершаемых преступной группой // Вопросы российского и международного права. 2020. Том 10. № 11А. С. 97-102. DOI: 10.34670/AR.2020.63.34.037

Ключевые слова

Киберпреступления, кибермошенничество, правовое регулирование, высокие технологии, кибератаки, мессенджер, аккаунт.

Введение

Глобальная информатизация и цифровизация, наряду с несомненными достоинствами, породила новый вид преступности – преступность в сфере высоких технологий. Особенностью этого нового вида преступности в том, что объектом преступных посягательств становится информация. Компьютерные системы в процессе совершения рассматриваемого вида преступления, становятся средством для совершения преступления.

Потерпевшей стороной таких преступлений могут стать не только физические лица, но и организации. Представляется необходимым сформулировать определение киберпреступности как нового, современного вида преступности. Киберпреступность есть совокупность преступных деяний, совершаемые в медиапространстве посредством использования автоматизированных систем и вычислительных сетей, а также других источников допуска к киберпространству, во взаимодействии с компьютерными системами и сетями или же против информационных систем и компьютерных данных [Тропина, 2017].

Основные виды преступных посягательств в области информационных технологий следующие:

- распространение вирусов и вредоносных программ;
- получение доступов незаконным путем к конфиденциальным данным;
- покупка товаров и получение услуг в несуществующих в реальном мире интернет-магазинах;
- распространение компрометирующих сведений, в том числе и ложных, под заказ;
- кража паролей от источников финансовых ресурсов и информации;
- сбор денег на строительство вымышленных объектов;
- сбор денег на заведомо несуществующее лечение животных, детей;
- реклама и продажа запрещённых средств;
- мошеннические схемы со знакомствами в виртуальном пространстве.

Рассматриваемый вид преступлений зачастую совершается групповым способом. Так как, учитывая специфичность данного вида преступлений, возникает необходимость в распределение преступных ролей в зависимости от образования, наличия специфических навыков, умений и опыта киберпреступников. Статья 272 часть 3 УК России «Неправомерный доступ к компьютерной информации» предусматривает уголовную ответственность за киберпреступления, совершенные группой лиц по предварительному сговору или организованной группой. В качестве наказания за такие преступления предусмотрено реальное лишение свободы, либо более мягкие виды наказаний [Гузеева, 2019].

Основное содержание

Действующее уголовное законодательство России содержит и другие нормы, ориентированные на регулирование и контроль за:

- созданием, использованием и распространением вредоносных компьютерных программ, совершенные как одним лицом, так и организованной группой;
- соблюдением правил эксплуатации, средств хранения, обработки или передачи компьютерной информации;
- внешним воздействием на критическую информационную инфраструктуру (КИИ) Российской Федерации.

Мировая уголовно-правовая практика вносит значительный вклад в решение проблемы противодействия киберпреступности.

Уголовный кодекс Федеративной Республики Германии [Шестакова, 2017] выделяет кибермошенничество в качестве самостоятельного преступления. Параграф 263а действующего документа устанавливает ответственность за деятельность, целью которой является имущественная выгода, полученная неправомерными действиями для себя или третьего лица, при которой страдает имущество другого лица. Для достижения преступного результата используются специфические средства: вредоносные программы, несанкционированное применение данных, неправомерное воздействие на что-либо. Компьютерная информация в этом случае выступает способом совершения хищения.

Во второй половине XX века власти США приняли закон «О мошенничестве и злоупотреблениях, связанных с компьютерами». Этот юридический документ представляет собой малую часть федерального законодательства, которая посвящена хищениям с использованием компьютерных сетей. Раздел 18, глава 47, параграф 1030 существующего свода Законов США, устанавливает ответственность за совершение мошенничества путем доступа к электронным системам. В соответствии с описываемой нормой, уголовная ответственность возможна уже только за взлом доступа к компьютеру и иным платформам, нацеленный на хищение или иные виды мошенничества или использование его с намерением получения выкупа или иного ценного эквивалента, с учетом незаконного использования компьютерного времени стоимостью более пяти тысяч долларов в течение года, то есть без оплаты использования компьютерных сетей и сервисов.

Законодательство США отграничивает киберпреступления от обычной, традиционной формы мошенничества. Кроме того, умышленная неоплата полученных услуг, предоставленных посредством сети Интернет, также является имущественным преступлением, организованным в медиаинформационном пространстве [Criminal law of the United States, 2020].

Извлечение имущественной выгоды посредством изготовления недействительных магнитных записей карается уголовным законодательством Японии. В соответствии со 247-II Уголовного кодекса Японии такие преступные действия влекут наказание в виде лишения свободы с принудительным физическим трудом на срок не свыше 10 лет [Коробеева, 2018]. Японский законодатель установил ответственность и за проникновение в личные компьютерные системы и сети с целью кражи, шантажа, порчи информации, а также причинения ущерба владельцам этой информации предусмотрена. Описываемая ответственность регламентирована законом «О несанкционированном проникновении в компьютерные сети» от 2000 года [Grabosky, 2019]. Важно отметить, что применение японским законодателем такого подхода, когда ответственность за противозаконное деяние предусмотрена не только уголовным кодексом, но и дополнительным, самостоятельным законом имеет положительный эффект. Такой комплексный подход стоило бы применить и в российском сегменте киберпреступлений.

Интернет шпионаж, совершённый организованной группой подлежит наказанию в соответствии с уголовным законодательством Швейцарии Согласно статье 143 Уголовного кодекса любое лицо, которое для своей собственной или чужой незаконной выгоды получает для себя или других лиц данные, которые хранятся или передаются в электронном виде или каким-либо аналогичным образом и которые не предназначены для него и были специально защищены для предотвращения доступа к нему, подлежит наказанию в виде лишения свободы на срок не более пяти лет или денежному штрафу.

В соответствии со ст. 147 Уголовного кодекса Швеции, уголовно наказуемыми являются действия с целью получения собственной выгоды путем неправильного, неполного или несанкционированного использования электронных данных, если такие действия повлекли несанкционированную передачу финансовых активов собственника иным лицам.

В Уголовном кодексе Китайской Народной Республики [Корбеева, 2019] в главу, посвященную преступлениям против имущества, включена статья 265, которая наказывает за незаконное подсоединение к телекоммуникациям другого лица, а также при краже адресов, номеров, используемых в личных устройствах.

Таким образом, изученное уголовное законодательство зарубежных государств в области правового регулирования киберпреступлений показывает, что государства заинтересованы в борьбе с киберпреступностью и активно принимают меры по борьбе с ней. Между тем, очевидно, что редуцировать кибератаки возможно не только совместными усилиями государств, но и путём рецепиирования уголовно-правовых норм, нацеленных на недопущение киберпреступлений. Обобщая изученный материал, возможно, заключить, что международные уголовно-правовые нормы, предусматривающие ответственность за киберпреступления достаточно результативно пресекают противоправные посягательства в области IP технологий. Однако им присуща определенная степень фрагментации с точки зрения криминализационных деяний. Отмечается непоследовательность. Часть норм отсылает к проблеме киберпреступности как таковой, то есть информационный терроризм, информационные войны. В оставшейся части норм с трудом прослеживается единый подход к разрешению вопроса преступлений, совершённых групповым способом в киберпространстве. В то же время большинство государств всё же признаёт, что для успешной борьбы с киберпреступностью требуется постоянное совершенствование как уголовно-правовых мер, так и законодательства в целом. Это относится и к России. Согласно статистическим данным МВД РФ если в первый год действия норм гл. 28 УК РФ было зарегистрировано 2698 преступлений, то в 2017 г. таких преступлений стало почти вдвое меньше – 1883. Примечательно, что ст. 274 УК РФ о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации совсем не пользуется популярностью: всего 2 преступления зафиксировано в 2017 г. и ни одного – за первое полугодие 2018-го. Вместе с тем количество преступлений, предусмотренных ст. 273 УК РФ, связанных с созданием, использованием и распространении вредоносных программ, напротив, возросло до 802 в 2017 г. по сравнению с 693 случаями в 2011 г. По всей видимости, снижение киберпреступлений по сравнению с 2011 г. и 2018 г. связано не только с совершенствованием систем безопасности приложений, программных обеспечений и операционных систем, что затрудняет киберпреступникам получить доступ к информации. Немаловажную роль в снижении киберпреступлений играет и отставание законодательства от стремительного развития компьютерных технологий, появления новых программ, нацеленных на неправомерное завладение информацией и имуществом. При этом правовое регулирование данной сферы не должно стоять на месте.

Заключение

Было бы своевременно дополнить главу 28 УК РФ «Преступления в сфере компьютерной информации» нормами, предусматривающими ответственность за кибермошенничество. Вместе с тем предлагается внести на законодательном уровне в УК РФ такие понятия как кибермошенничество и киберпреступление. Помимо этого, в уголовное законодательство

России следует внести норму об ответственности даже за, казалось бы, с первого взгляда, безобидное предложение услуг по взлому различных носителей конфиденциальной информации, в том числе финансовой, аккаунтов соцсетей, взлому переписки в мессенджерах. Предусмотреть ужесточение ответственности за групповое совершение новых составов преступлений. Необходимо обеспечить укрепление информационной структуры, поддерживающей новые возможности сбора, обработки, обмена информацией, обеспечения ее безопасности, внедрение высокоинтеллектуальных методов добывания значимой информации, модернизация приёмов осуществления оперативно-розыскных мероприятий и следственных действий.

Библиография

1. Гузеева О.С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опыт, анализ, практика. 2019. С. 17
2. Свод законов США // URL: <https://www.law.cornell.edu/uscode/text> (дата обращения: 22.11.2020)
3. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08. Владивосток, 2017. С. 33
4. Уголовный кодекс Российской Федерации. Комментарий с путеводителем по судебной практике под редакцией А. И. Чучаева. М., Проспект. 2020 С. 47
5. Уголовный кодекс Федеративной Республики Германии / науч. ред. Д.А. Шестакова; пер. с нем. Н.С. Рачковой. СПб.: Юрид. центр Пресс, 2017. С. 52
6. Уголовный кодекс Швейцарии / пер. с нем. М.: Зерцало, 2017. С. 21
7. Уголовный кодекс Швеции / науч. ред. Н.Ф. Кузнецова и С.С. Беляев; пер. на рус. яз. С.С. Беляева. СПб.: Юрид. центр Пресс, 2018. С. 67
8. Уголовный кодекс Китайской Народной Республики / науч. ред. А.И. Корбеева; пер. с кит. Д.В. Вичикова. СПб.: Юрид. центр Пресс, 2019. С. 94
9. Уголовный кодекс Японии / науч. ред. А.И. Корбеева; пер. с яп. В.Н. Еремина. СПб.: Юрид. центр Пресс, 2018. С. 29
10. <https://мвд.рф/reports/item/21933965/> (дата обращения: 10.12.2020)
11. Criminal law of the United States. The Lawyers co-operative publishing Co. Rochester, New York, 2020. p. 197
12. Grabosky P. Organized cybercrime and national security // Cybercrime risks and responses. New York, 2019. p. 34

Specifics of legal regulation of cybercrimes committed by a criminal group

Sergei V. Alekseev

PhD in Law, Associate professor
Associate Professor of Department of civil and arbitration proceedings
Samara State University of Economics,
443090, 141 Sovetskoi Armii st., Samara, Russian Federation;
e-mail: ecun@sseu.ru

Abstract

This article discusses a new type of crime that was not previously widely known-high-tech crime. The definition of cybercrime is proposed. The article considers in detail the world criminal law practice of countering cybercrimes committed in a group, which was studied by the author. The main types of criminal attacks in the field of information technology are considered. Detailed statistical data on crimes committed in Russia in the IT sphere are provided. The article explains the reasons for a slight decrease in cybercrime in Russia. However, despite this, the legal regulation of

this area should not stand still. The article substantiates the need for legislative expansion of Chapter 28 of the Criminal code of the Russian Federation about cybercrime by introducing new rules providing for liability for crimes in cybercrimes.

For citation

Alekseev S.V. (2020) Spetsifika pravovogo regulirovaniya kiberprestuplenii, sovershaemykh prestupnoi gruppoi [Specifics of legal regulation of cybercrimes committed by a criminal group]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 10 (11A), pp. 97-102. DOI: 10.34670/AR.2020.63.34.037

Keywords

Cybercrime, cyber fraud, legal regulation, high technologies, cyber attacks, messenger, account.

References

1. Guzeeva O. S. Action of the Criminal code of Russia in relation to Internet crimes // *Laws of Russia: experience, analysis, practice*. 2019. P. 17
2. US code of laws // url: <https://www.law.cornell.edu/uscode/text> (accessed: 22.11.2020)
3. Tropina T. L. Cybercrime: concept, state, criminal - legal measures of struggle: dis. ... Cand. the faculty of law.: 12.00.08. Vladivostok, 2017. P. 33
4. Criminal code of the Russian Federation. Commentary with a guide to judicial practice edited by A. I. Chuchaev. M., Pospkt. 2020 P. 47
5. Criminal code of the Federal Republic of Germany / scientific ed. by D. A. Shestakov; TRANS. with N. S. Rachkova. St. Petersburg: Yurid. Center Press, 2017. P. 52
6. Criminal code of Switzerland / TRANS. from German. M.: Zertsalo, 2017. P. 21
7. The Swedish penal code / scientific. N. F. Kuznetsova and Sergei Belyayev; translated in Russian. yaz. S. S. Belyaev. SPb.: The faculty of law. Center Press, 2018. With. 67
8. Criminal code of the People's Republic of China / scientific. Edited by A. I. Korneeva; SPb. The faculty of law. Center Press, 2019. P. 94
9. Criminal code of Japan / scientific ed. by A. I. Korobeev; TRANS. from YAP. V. N. Eremin. SPb.: Yurid. Tsentr press, 2018. 29. 29
10. <https://mvd.rf/reports/item/21933965/>(accessed: 10.12.2020)
11. Criminal law of the United States. The Lawyers co-operative publishing Co. Rochester, New York, 2020.
12. Graboski P. organized cybercrime and national security // *cybercrime risks and responses*. New York, 2019. Page 34