УДК 347

Гокунь Юлия Сергеевна
Донецкий национальный университет
Юридический факультет
Донецкая Народная Республика, г. Донецк
yulya.gokun@mail.ru
Gokun Julia
Donetsk National University
Faculty of Law
Donetsk People's Republic, Donetsk

КВАЛИФИКАЦИЯ ХАКЕРСКИХ АТАК ПО ГРАЖДАНСКОМУ ЗАКОНОДАТЕЛЬСТВУ

Аннотация: статья посвящена изучению квалификации хакерских атак по гражданскому законодательству. Установлено, что гражданское и энергетическое право обладают общим предметом регулирования в части правоотношений, возникающих при добыче, переработке, передаче, продаже, использовании, распределении, торговле, потреблении и сохранении разнообразных видов энергетических ресурсов, в отечественном законодательстве отсутствует указание на то, как должны квалифицироваться хакерские атаки на предприятия нефтяной промышленности. Сделан вывод о необходимости квалификации компьютерного вируса как источника повышенной опасности, а хакерской атаки – как деятельности, создающей повышенную опасность для окружающих.

Ключевые слова: энергетическое право, гражданское право, хакерская атака, компьютерный вирус, квалификация, нефтяная промышленность.

QUALIFICATION OF HACKER ATTACKS UNDER CIVIL LAW

Annotation: the article is devoted to the study of the qualification of hacker attacks according to civil law. It has been established that civil and energy law have a

common subject of regulation in terms of legal relations arising from the extraction, processing, transfer, sale, use, distribution, trade, consumption and conservation of various types of energy resources, it is determined that there is no indication in domestic legislation on how hacker attacks on oil industry enterprises should be qualified from the standpoint of civil law. Concluded that it is necessary to classify a computer virus as a source of increased danger, and a hacker attack as an activity that creates an increased danger to others.

Key words: energy law, civil law, hacker attack, computer virus, qualification, oil industry.

Нефть является жизненно важным ресурсом для любого государства по всему миру. С середины 1950-х годов нефть стала самым важным источником энергии в мире. Обеспечивая электроэнергией, обогревая дома и являясь топливом для транспортных средств и самолетов, которые перевозят товары и людей, она лежит в основе современного общества.

Некоторые лица, понимая потенциально важное значение нефти, решают нарушить закон и воспрепятствовать нормальному функционированию нефтедобывающих, нефтеперерабатывающих и занимающимся транспортировкой нефти предприятий. На протяжении нескольких последних лет их противоправные посягательства направлены на кибербезопасность указанных юридических лиц. Так, в 2017 году жертвами кибератаки, совершенной с использованием программы-вымогателя Petya, стали юридические лица по всему миру, включая в Российской Федерации, где от хакерской атаки пострадали Роснефть, Башнефть и Евраз. Общая сумма ущерба, причинённого вирусом Petya, по всему миру составила более $10 млрд. С конца марта до середины июня 2020 года в Китае и на Ближнем Востоке было обнаружено большое количество компьютерных программ-червей, умеющих собирать логины и пароли из памяти системных процессов с помощью разных версий утилиты Mimikatz. В мае 2021 года крупнейшая

трубопроводная система в США Colonial Pipeline подверглась кибератаке с использованием программ-вымогателей. Через несколько часов после атаки Colonial Pipeline перевела хакерам $4,4 млн. По словам главы компании Джозефа Блаунта, решение заплатить вымогателям было вызвано необходимостью получения инструмента дешифровки для разблокировки своих систем и скорейшего восстановления работы трубопровода.

Обратим внимание на то, что в законодательстве Российской Федерации отсутствует указание на то, как с позиции гражданского права должны квалифицироваться хакерские атаки на нефтедобывающие, нефтеперерабатывающие и на занимающиеся транспортировкой нефти предприятия. Решение данного вопроса в гражданско-правовой сфере усовершенствует и энергетическое право, т.к. последнее принято считать молодой и комплексной отраслью права, сочетающей в себе правоотношения, урегулированные нормами гражданского, уголовного и административного права. Применительно к гражданскому и энергетическому праву отметим, что они обладают общим предметом регулирования, т.к. гражданское право регулирует по большей мере имущественные отношения, энергетическое право делает предметом своего регулирования отношения, возникающие при добыче, переработке, передаче, продаже, использовании, распределении, торговле, потреблении и сохранении разнообразных видов энергетических ресурсов [1, с.102-106], а также связанные с обеспечением энергетической безопасности. Следовательно, общим предметом регулирования вышеуказанных отраслей права необходимо признать комплекс договорных и внедоговорных отношений, которые возникают при добыче, переработке, передаче, продаже, использовании, распределении, торговле, потреблении и сохранении разнообразных видов энергетических ресурсов.

Решая проблему квалификации хакерских атак с позиции гражданского права отметим, что за рубежом они детерминируются как деликты, о чем в своих научных трудах говорят такие исследователи, как: Michael L. Rustad,

Thomas H. Koenig, Vincent R. Johnson, Dane Mcleod, Beatrice Walton, Tjong Tjin Tai, Jovan Kurbalij. Полагаем, что и в отечественной правовой системе хакерские атаки необходимо рассматривать не иначе как деликты, поскольку:

1) хакерская атака представляет собой действие лица, которое нарушает нормы права [2, с.17];

2) хакерская атака осуществляется виновно, налично виновное поведение лица;

3) хакерская атака причиняет вред государству, обществу, физическим и юридическим лицам, который существует в виде шифровки данных с целью получения денежных средств за их дешифровку, утечки и удаления данных, удаленного управления серверами и передачи файлов, слежки за всеми действиями пользователей и, к примеру, сотрудников нефтедобывающего предприятия, и т.д.;

4) за хакерскую атаку, как и за любой гражданско-правовой деликт, предусмотрена санкция [3, с.1-59], а именно обязанность возместить причиненный вред в полном объеме (ст. 1064 ГК РФ) [4].

Отметим, что вредоносную программу, компьютерный вирус, который хакеры используют для причинения вреда предприятиям, осуществляющим деятельность в нефтяной промышленности, возможно рассматривать как источник повышенной опасности [5]. Способность компьютерного вируса быстро распространяться, удалять часть хранящейся на компьютере информации, изменять способ ее хранения [6, с.385-401], самораспространяться через различные каналы передачи данных [7, с.4], мешать работе пользователей, содействовать появлению сбоев в системе, а значит быть неподконтрольным третьему лицу, т.е. пользователю, и создавать угрозу для него, для конкретного юридического лица, а в некоторых случаях и для всей нефтяной промышленности и даже государства. Сама же хакерская атака должна квалифицироваться как деятельность, создающая повышенную опасность для окружающих. Следовательно, в данном случае лицо,

использующее компьютерный вирус, будет нести ответственность по ст.1079 ГК РФ как за вред, который был причинен деятельностью, создающей повышенную опасность для окружающих.

Подытожив все вышеизложенное отметим, что определение гражданско-правовой природы хакерских атак позволит привлечь к гражданско-правовой ответственности всех нарушителей, предотвратить дальнейшие противоправные посягательства на информационную безопасность нефтяной промышленности, а значит и на энергетическую безопасность Российской Федерации в целом.

Список литературы:

1. Прудникова Л.Б. Принципы энергетического права как идеологическая и организационно-системная основа его функционирования и развития (виды и краткий анализ содержания) // Глобальная ядерная безопасность. 2015. № 3(16). С.102-106

2. Егоров А.А. Категория «правонарушение» в отечественной теоретико-правовой мысли: авторефер. дис. на соиск. учён. степ. канд. юрид. наук. Москва. 2018. С.1-19.

3. Nolan A. Cybersecurity and Information Sharing: Legal Challenges and Solutions // Congressional Research Service. 2015. Pp.1-59.

4. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 N 14-ФЗ (ред. от 09.03.2021, с изм. от 08.07.2021) // СПС КонсультантПлюс

5. Табунщиков, А.Т. Виды источников повышенной опасности в российской цивилистической науке // Электронный архив открытого доступа Белгородского государственного университета. 2018.

6. Цветкова Е.С. Виды источников повышенной опасности в аспекте развития новых технологий // Вопросы российской юстиции. 2019. №1. С.385-401.

7. Harper A., Regalado D., Linn R., Sims S., Spasojevic B. Gray Hat Hacking: The Ethical Hacker's Handbook. – New York City: Graw-Hill Education. 2018. Pp.4.