Юдинцев Кирилл Олегович
студент
Институт права
ФГБОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область
Калашникова Елена Борисовна
канд. ист. наук, доцент
ФГБОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОЙ ЦИФРОВОЙ ЭКОНОМИКЕ

Аннотация*: в статье рассматриваются понятие и некоторые теоретические аспекты киберпреступности как одной из разновидностей экономической преступной деятельности, говорится о динамике развития компьютерной преступности (киберпреступности), а также о причинах широкого распространения компьютерных преступлений. Определены основные направления борьбы с киберпреступностью.*

Ключевые слова*: цифровая экономика, киберпреступность, компьютерная преступность, информационные технологии.*

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы констатировала вступление России в эпоху цифровой экономики. Это, в свою очередь, затронуло все аспекты правовой безопасности нашей страны [1].

Цифровая экономика, согласно терминологии новой Стратегии, – это хозяйственная деятельность, в которой первоочередным фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых, по сравнению с традиционными формами

хозяйствования, позволяют во много раз повысить эффективность различных видов производства, оборудования, технологий, продажи, хранения, доставки товаров и услуг.

Цифровая экономика пронизывает практически все аспекты современного общества. За несколько последних лет в нашей стране все заметно активней стала использоваться электронная коммерция, значительно увеличился безналичный оборот денежных средств, совсем недавно стала вводиться криптовалюта, появляются технологии blockchain.

Инновационный, цифровой уклад жизни, активное использование новых технологий – все это послужило мотивом для появления нового вида преступности в сфере информационных технологий, которое сейчас называют киберпреступностью.

Проблемы, связанные с компьютерной преступностью и всякого рода мошенническими действиями в сфере высоких технологий, а также возможные пути разрешения этих проблем представляются мне крайне актуальными на сегодняшний день.

Изучение проблем расследования преступлений в сфере компьютерной информации выступает одной из острейших задач современной криминалистической науки. Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных и дискуссионных вопросов.

О важности рассматриваемой проблемы свидетельствует и тот факт, что среди экономических преступлений, по мнению ряда специалистов, киберпреступность растет более стремительными темпами, чем все другие виды преступности. Кроме того, растущую тревогу вызывает то, что ущерб от данного рода преступлений измеряется колоссальными цифрами, опасность от них приобретает все более угрожающий масштаб, причём не только для отдельных финансовых организаций, но и для целых государств.

В августе этого 2018 года на официальном портале Генеральной прокуратуры Российской Федерации была опубликована статистика за 2017 год по преступлениям в сфере информационно-телекоммуникационных технологий. Согласно статистическим данным, в 2017 году число преступлений в области информационно-телекоммуникационных технологий увеличилось с 65949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4% – это почти каждое 20-е преступление.

Наиболее часто встречающимися киберпреступлениями являются неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ). Если в 2017 году зарегистрировано 1883 таких преступления (+7,7%), то за первое полугодие 2018 г. – 1233 (+3,4). Наибольшее количество киберпреступлений совершается с использованием вредоносных программ, а также специфических возможностей операционных систем, позволяющих получить удаленный доступ к информационным ресурсам, в том числе находящимся в госсобственности или отражающим финансово-хозяйственную деятельность компании [2].

Проблема киберпреступности на протяжении ряда лет является предметом внимательного изучения и обсуждения в профессиональных кругах юристов, о чем свидетельствует значительное число публикаций, посвященных данному виду преступности.

Ряд авторов единодушно высказывается о том, что киберпреступность по своей сути гораздо шире компьютерной преступности, и включает в себя целый спектр противоправных деяний.

И.Г. Чекунов считает, что киберпреступность следует рассматривать масштабнее компьютерной преступности, поскольку использование компьютера или компьютерных сетей для составляющих ее преступлений не всегда является необходимостью. Современные реалии таковы, что для совершения киберпреступлений применяются не только компьютеры, но и мобильные (сотовые) коммуникационные технические устройства и системы связи [3].

Современная киберпреступность несет в себе серьёзную угрозу для общества в целом, поскольку она, по мнению ряда экспертов, тесным образом может быть связана с серьезнейшим на сегодняшний день видом преступной деятельности – терроризмом. Давно не является секретом то, что многие террористические организации через своих высокопрофессиональных специалистов имеют доступ к сфере высоких технологий.

По мнению А.С. Линникова, члены террористических групп и преступных организаций путем разрушения жизненно важных систем, совершения терактов с множеством человеческих жертв могут нанести существенный урон экономике с целым рядом социальных последствий [4].

Д.И. Удалов отмечает все нарастающую угрозу от массированных DDoS-атак, направленную не только на банки, но и на ICO новых криптовалют и их инфраструктурных объектов. Причиной этому, как он считает, является малочисленное количество необходимого защитного оборудования, программного обеспечения и мощностей, а также недостаток специальных сервисов. Кроме того, многие гибридные решения защиты не решают полностью проблему безопасности, для этого необходим переход к комбинированным, облачным и операторским технологиям защиты информации [5].

Правовые основы противодействия киберпреступности в настоящее время у нас в стране закреплены в ряде документов. Так 5 декабря 2016 г. вступил в силу Указ Президента РФ N 646, который утвердил новую Доктрину информационной безопасности. Это существенный шаг, направленный на регулирование вопросов информационной безопасности в нашей стране.

12 июля 2017 года был принят Федеральный закон «О безопасности критической информационной инфраструктуры» №187-ФЗ. Закон направлен на создание правовой и организационной основы эффективного функционирования системы безопасности критической информационной инфраструктуры в Российской Федерации, кроме того, данный закон позволит снизить отрицательные последствия от проводимых на неё противоправных хакерских атак.

Несмотря на принимаемые меры, проблема киберпреступности у нас в стране остается весьма актуальной и достаточно болезненной.

Трудность борьбы с данным видом преступной деятельности заключается в ее масштабности. Ни одно государство сегодня не способно противостоять этому злу единолично. Многие эксперты говорят о необходимости скорейшего налаживания международно-правового механизма регуляции проблемы, в частности разработку единых международных стандартов – от понятийного аппарата до унифицированных правовых норм.

Для противодействия киберпреступности необходимы новые, специфические механизмы выявления, пресечения, расследования и предотвращения подобного рода преступлений.

Нельзя не согласиться с мнением ряда специалистов, которые считают, что для улучшения ситуации требуется существенное усовершенствование защитного оборудования и программного обеспечения, а для этого необходима качественная подготовка и увеличение численности IT-персонала. Кроме того, необходимо непрерывное повышение уровня специальной подготовки должностных лиц правоохранительных органов.

Учитывая тот факт, что от действий киберпреступников страдают также и простые рядовые граждане, особенно люди пожилого возраста, представляется немаловажным постоянное повышение компьютерной и правовой грамотности населения страны. Грамотное использование банковских карт при совершении электронных платежей, умение правильно ориентироваться при осуществлении онлайн-покупок – все это позволит населению защитить себя от киберпреступников.

Список литературы

1. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 09.05.2017 №203) [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 23.11.2018).

2. Сайт генпрокуратуры [Электронный ресурс]. – Режим доступа: http://lacerta.su/press-center/overview/14–08–2018.html

3. Чекунов И.Г. Понятие и отличительные особенности киберпреступности / И.Г. Чекунов // Российский следователь. – 2014. – №18. – С. 53–56 [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=17724355

4. Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире / А.С. Линников // Банковское право. – 2017. – №5. – С. 19–29 [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=30452470

5. Удалов Д.И. Угроза и вызов цифровой экономике / Д.И. Удалов // Экономическая безопасность и качество. – 2018. – №1 (30). – С. 12–18 [Электронный ресурс]. – Режим доступа: https://elibrary.ru/item.asp?id=32759170

6. Тропинина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук: 12.00.08 / Т.Л. Тропинина. – Владивосток, 2005. – 235 с. [Электронный ресурс]. – Режим доступа: http://lawlibrary.ru/disser2018106.html

7. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. ... канд. юрид. наук: 12.00.12 / Е.С. Шевченко. – М., 2016. – 29 с. [Электронный ресурс]. – Режим доступа: https://search.rsl.ru/ru/record/01008531943

8. Орлов А.С. Киберпреступность в банковской сфере / А.С. Орлов, Е.Б. Калашникова // Аллея науки. – 2018. – № (27) [Электронный ресурс]. – Режим доступа: https://www.alleyscience.ru/domains_data/files/06December2018/KIBERPRESTUPLENIYa%20V%20BANKOVSKOY%20SFERE.pdf