ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ В IT-СФЕРЕ

Е. В. Зыкина,
кандидат юридических наук, доцент, доцент кафедры государственно-правовых дисциплин и теории права, Институт права, экономики и управления, Псковский государственный университет
Д. А. Холтобина, М. В. Васильева,
студентки, Институт права, экономики и управления, Псковский государственный университет

В современном мире Интернет имеет очень важное значение. Нельзя недооценивать его роль, так как на сегодняшний день этой глобальной сетью пользуются миллиарды жителей нашей планеты, а именно, согласно данным статистики, больше половины всего населения Земли.

На данный момент, в сети Интернет хранятся огромные базы данных и информация обо всем на свете, практически все организации и разного рода бизнес хранит и отправляет свои документы при помощи Интернета. Также благодаря сети Интернет обеспечивается максимально быстрое общение с разными странами, можно передать нужный документ куда угодно за пару секунд.

Такая глобализация в IT сфере имеет не только положительные, но и крайне отрицательные последствия, так как постоянно развивающиеся информационные технологии предоставляют необъятные возможности для различного рода махинаций и преступлений. Ведь сейчас Интернет стал для нас настоящей заменой привычной жизнедеятельности, он включил в себя всю социально-экономическую составляющую жизни человека и стал площадкой для развития электронного бизнеса, совершения различного рода сделок на международных рынках. Соответственно в Интернете теперь вращаются огромные суммы денег, и это привлекает мошенников. И они уже другого уровня: образованные, отлично освоившие современные технологии, и очень хитрые и из-за этого, как правило, неуловимые для правоохранительных органов.

Таким образом, современная киберпреступность является закономерным следствием происходящих расширений технологических и информационных процессов. С каждым днем она только все больше развивается и усложняется. [1]

Преступления, которые совершаются в IT сфере, растут также быстро, как и количество пользователей в Интернете. Очередной скачок таких преступлений в России произошел в 2020 году. Их количество выросло

на 83,9% в первом квартале 2020 года, а удельный вес достиг почти 20% от общего числа всех преступлений.

Но такая динамика развития данных преступлений прослеживается не только в России. Киберпреступности подверглись даже африканские страны, такие как Нигерия и Того. А первое место среди всех стран по числу зафиксированных экономических преступлений в IT сфере занимают Соединенные Штаты Америки.

То есть, киберпреступность на данный момент является всемирной и общечеловеческой проблемой. Ее массовое распространение ставит под угрозу миллионы пользователей сети Интернет. Именно поэтому мы решили рассмотреть данную тему.

Количество экономических афер в IT сфере достигло колоссальных размеров. Большинство крупных финансовых махинаций осуществляется преступными группировками и целыми транснациональными сообществами. Например, весной 2018 года путешественники со всего мира пострадали от масштабной атаки одной хакерской группировки. Взломав американский сайт бронирования авиабилетов и систему бронирования британской авиакомпании, мошенники получили доступ к данным примерно 244 тысяч кредитных карт пассажиров, включая номера и трехзначные коды. Хоть вывести деньги злоумышленникам и не удалось, репутация авиакомпании пострадала. Так как это, безусловно, вызывает сомнение относительно плюсов и достоинств «виртуальной» коммерции. Ведь о каком удобстве и эффективности таких операций может идти речь, если вся их безопасность находится под угрозой.

На сегодняшний день, ущерб, наносимый экономическими преступлениями в сети Интернет, достигает огромных размеров. В эту проблему оказались вовлечены совершенно разные организации и структуры. [2, С. 43]

Первая международная конвенция по борьбе с преступлениями в IT сфере была подписана 23 ноября 2001 года, ее участники, осознавая необходимость принятия мер с преступностью в сфере компьютерной информации, обязались принять законы, способствующие борьбе с данными преступлениями.

Преступления в сети Интернет интенсивно изучаются различными учеными из зарубежных стран. Так, в Соединенных Штатах Америки был запущен Независимый центр исследования интернет-мошенничества.

У нас же на данный момент эта деятельность только зарождается, хотя этому следует уделять гораздо больше внимания, так как по опубликованным

данным МВД о состоянии преступности за 2020 год, статистика зарегистрированных в стране преступлений увеличилась именно за счет киберпреступности. Число таких преступлений выросло почти на девяносто пять процентов. При этом платежные карты использовались в мошеннических целях в 6 раз чаще, чем в прошлом году, а средства мобильной связи в 2 раза чаще. А раскрываемость таких преступлений маленькая – не более двадцать трех процентов. То есть, очевидно, что сегодня у наших правоохранительных органов нет четкой методики расследования IT преступлений, и им не хватает квалифицированных сотрудников, которые были бы подготовлены в этой сфере.

В современном мире есть много способов совершения мошенничества в Интернете. Во-первых, это мошенничества, совершенные на интернет-аукционах. Во-вторых, это мошенничества, связанные с электронной торговлей. И в-третьих, это так называемые «письма счастья», получившие наибольшее развитие с появлением массовых рассылок по электронной почте. [3, С. 8]

Еще один популярный вид интернет-мошенничества «кардинг». Это такой вид мошенничества, который связан с пластиковыми карточками. Совершая подобные преступления, мошенники обычно перехватывают данные, а затем проверяют наличие на счету необходимой суммы денег. Мошенники имеют возможность присоединиться к соответствующему проводу и узнать необходимые данные для совершения преступления.

Совершая подобные преступления, аферисты всеми доступными способами стараются заполучить данные кредитных карт с целью дальнейших покупок в интернете. Такая система позволяет тратить деньги с чужого счета, при наличии определенных реквизитов. Именно поэтому данное преступление распространено.

В России наиболее часто используют реквизиты банковских карт для совершения покупок через Интернет. Таким образом, лицо начинает совершать покупки через интернет, оплачивать различные услуги, используя необходимые данные банковской карты. Данный способ слишком привлекателен для мошенников. [4, С. 31]

Еще один распространенный способ мошенничества в интернете - попытка посторонних лиц завладеть информацией о пользователе в целях финансовой выгоды. Данный вид преступления именуется как «фишинг» (финансовое мошенничество).

Финансовое мошенничество – серьезная угроза для организаций, предоставляющих свои услуги в Интернете. Для достижения корыстных целей злоумышленники используют разнообразные приемы, например, вирусы, обман, запугивание и так далее.

Рассматривая статистику подобных преступлений за 2020 год, можно увидеть, что именно жертвой такого преступления стала организация Estee Lauder. Была обнаружена утечка данных организации в феврале 2020 года. У Транснациональной косметической компании было уведено 440 миллионов записей. Из 440 целевых файлов неопределенное количество имели адреса электронной почты клиентов хранящегося виде простого текста. Все похищенные данные были выгружены преступниками на открытых Интернет-ресурсах. В конце января исследователь безопасности Джереми Фаулер обнаружил не защищенную паролем базу данных. Неясно, каким методом мошенники заполучили информацию. Обнаруженная база данных содержала: 440 336 852 записей, «Пользовательские» электронные письма в виде обычного текста, ссылки на отчеты и другие внутренние документы, также мошенники получили IP-адреса, порты, пути и информация о хранилище, которые можно использовать для более глубокого доступа в сеть.

На сегодняшний день такой вид мошенничества наиболее опасен. С каждым годом он получает все большее распространение среди преступников. [5, С.8].

Борьба с подобными преступлениями ведется не только правоохранительными органами, но и крупными организациями. Во многих странах уголовная ответственность за такие преступления уже предусмотрена. К ним относятся ФРГ, США, Эстония и Беларусь. В России компьютерное мошенничество квалифицируется статьями 159 УК РФ, 160 УК РФ, 165 УК РФ, 187 УК РФ.

Компьютерные мошенничества – это преступления против собственности. Непосредственным объектом в таких составах выступают отношения, охраняющие право собственности, дополнительным объектом – общественные отношения в сфере компьютерной информации. Предметом компьютерного мошенничества является чужое имущество. Объективная сторона компьютерного мошенничества выражается в завладении чужим имуществом и правом на него.

Злоупотребляя доверием, преступник выстраивает доверительные отношения с целью причинить вред имущественным правам и законным интересам собственника. В результате лицо завладевает чужим имуществом, то есть злоупотребляет доверием. [6, С. 40]

Важно, что компьютер хранит именно информация, а не сами денежные средства. Если преступник тайно проникает в компьютерную систему с целью похитить денежные средства, то он проникает в систему путем манипуляций с программами. Эти действия считаются обманом.

Подводя итог всему вышесказанному стоит отметить, что преступления против собственности с использованием интернета имеют ряд особенностей, они являются глобальными. С каждым годом компьютерная техника стремительно развивается и появляется все больше возможностей и соблазна для компьютерного мошенничества. Так как данная проблема охватывает не только Россию, но также и другие страны, стоит активнее внедрять изменения в законодательства и применять иные меры по борьбе с данным видом преступности. Многие страны уже начали активную борьбу, но это лишь малое количество. Если упустить развитие данного преступления, то каждое из государств даст возможность миллиону мошенников обманывать людей через интернет, лишая их имущества и денежных средств. Компьютерное мошенничество является транснациональным преступлением. Именно поэтому очень важна не только работа каждого государства отдельно, а именно сплоченность всех государств при решении данной проблемы. Только совместными усилиями можно прекратить развитие IT-преступлений в мире.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конвенция по киберпреступности: одобрена Европейским советом 19.09.1999.
2. Ковалев Н., Куликов А. XXI век против глобализации преступности // Московские новости. - 2000.-№ 43. - С. 43.
3. Крылов В. «Информационные преступления – новый криминалистический объект» // Российская юстиция №4 1997 г.
4. Лунеев В. В. Преступность XX века: Мировые, региональные и российские тенденции. - М., 1997. - С.31.
5. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: народный опыт: монография. - М., 2004.- С. 8.
6. Уголовное право. Особенная часть : Учебник под ред. профессора А. И. Рарога,. – М., 1996.