

Краснослободцев Максим Алексеевич
студент четвертого курса

юридического факультета

кафедры государственно-правовых
дисциплин,

Российский Государственный

Социальный Университет,

г. Москва, Российская Федерация

Krasnoslobodtsev Maxim Alekseevich

fourth year student

Faculty of Law Department of State and
Legal Disciplines,

Russian State Social University,

Moscow, Russian Federation

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

Crimes in the field of computer information

Аннотация: в статье рассматривается общая криминологическая характеристика преступлений в сфере телекоммуникаций и компьютерной информации. В настоящее время сети Интернет, играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами, как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем, на какой фильм сходить,— все эти действия зависят от информационных технологий. В связи с этим, многие пользователи Интернетом, подвергаются атакам со стороны киберпреступников.

Ключевые слова: высокие технологии, Интернет пользователи., характеристика преступлений, компьютерной информации, сфера телекоммуникаций, состояние преступности, компьютерные преступления, уголовное законодательство, предупреждение, динамика преступности.

Annotation:The article examines the general criminological characteristics of crimes in the field of telecommunications and computer information. Currently, the Internet plays an important role in the field of communications: we carry out various transactions with money, both using a computer, an ATM, and other payment systems, plotting routes, looking for good restaurants, finding out which movie to go to, - all of these activities are information technology dependent. In this regard, many Internet users are exposed to attacks from cybercriminals.

Key words: high technologies, Internet users., Characteristics of crimes, computer information, telecommunications, the state of crime, computer crimes, criminal legislation, prevention, dynamics of crime.

В современных условиях жизнедеятельности общества сети Интернет являются основополагающим фактором сферы коммуникаций: с их помощью осуществляются различные операции с денежными средствами (с использованием компьютеров, банкоматов, иных платежных систем), поиск различных товаров и услуг, информации. Эти действия напрямую зависят от различных информационных технологий, в результате чего ряд пользователей ежедневно подвергаются атакам со стороны киберпреступников. Российская криминалистика длительный период времени развивалась в отрыве от ведущих зарубежных исследовательских школ. Интернет позволяет эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, породить новые, неизвестные мировому сообществу виды общественно опасных преступлений. За последние десять лет в 5 раз увеличилось количество интернет пользователей в России, это охватило около половины населения, а в ближайшем будущем интернет-пространством будет охвачено около 80 миллионов человек. Такая тенденция грозит таким странам, как Китай, США,

Индия, Япония, Бразилия, Россия, Германия, Индонезия, Великобритания и Франция.

Сеть Интернет, превратилась в виртуальную площадку, в пространство, где люди могут выражать идеи и заниматься общественной деятельностью и т.д. В настоящее время сети Интернет, играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами, как с использованием компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем, на какой фильм сходить,— все эти действия зависят от информационных технологий. В российском законодательстве кроме главы 28 Уголовного кодекса Российской Федерации, предусматривающей ответственность за преступления в сфере компьютерной информации, нет иных норм, предусматривающих ответственность за незаконные действия в сфере телекоммуникаций и компьютерной информации, нет соответственно и понятий, определяющих либо регламентирующих незаконные преступные деяния, совершаемые с помощью высоких технологий.

Статистика преступлений демонстрирует печальную динамику: количество зарегистрированных преступлений в сфере компьютерной информации с 1995 по 2018 г. в России выросло более чем в 300 раз, что составило более 10 Тысяч преступлений в год. За прошедший 2018 г. широкое распространение получили мошеннические действия, совершаемые с использованием электронных средств платежа (ст. 159.3 УК РФ), их количество выросло за первое полугодие 2018 г. в семь раз, за второе – в 6 раз. Определены и регионы-лидеры РФ по количеству подобных преступлений: Ставропольский край (66), Мурманская область (52), республика Татарстан (37), Москва (34) и Саратовская область (31).

Наиболее распространенными преступлениями являются:

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)

Жертвы редко обращаются в полицию. 1/4 пользователей сети утверждают, что не предпримут никаких действий, став жертвами кибератаки. К тому же органы правопорядка вряд ли бы справились с постоянным потоком жалоб, так как на раскрытие одного преступления требуется в среднем 28 дней и 334 доллара.

Также следует отметить тот факт, что сумма ущерба от преступлений совершенных в сфере телекоммуникаций и компьютерной информации (если сравнить удельный вес исследуемого состава с иными

преступлениями) значительна по отношению к другим видам составов УК РФ.

В современной криминологии понятие «высокие технологии» ассоциируют, как правило, с совершением преступлений в информационно-телекоммуникационной среде с использованием компьютеров или различных средств связи. Термин «преступления в сфере высоких технологий» ученые рассматривают с разных научных позиций.

Н.Р. Шевко считает, что понятие «преступления, совершаемые с использованием высоких технологий» носит собирательный характер, употребляется в случаях, когда для совершения традиционных в уголовном праве преступлений используются информационные технологии, ответственность за которые предусмотрена статьями различных глав УК РФ: 146, 159.3, 159.6, 187. Понятие «преступления, совершаемые с использованием высоких технологий» и понятие «преступления в сфере компьютерной информации», ответственность за которые предусмотрена в статьях главы 28 УК РФ, имеют существенную разницу. Мнение ряда ученых фактически уравнивает высокие технологии и информационные технологии, в то же время отделяя высокие технологии от сферы компьютерной информации.

Некоторые авторы отождествляют преступления в сфере высоких технологий с преступлениями, совершаемыми при помощи телекоммуникационных сетей, включая сеть Интернет.

Д.К. Чирков и А.Д. Саркисян относят преступления в сфере высоких технологий к новым видам и способам совершения преступлений, возникшим в результате распространения сети Интернет, информационно-телекоммуникационных сетей.

А.А. Комаров не дает четких границ этим понятиям, включает в преступления в сфере высоких технологий и компьютерные преступления, и преступления, совершаемые посредством сети Интернет и информационных технологий.

Число вредоносных программ возросло на 1/3 по сравнению с прошлым годом и составило свыше миллиона. Интернет пользователей становились жертвами кибератак. В прошлом году на каждого жителя планеты пришлось по 5000 спам писем, многие из них содержали вредоносные программы для взлома счетов. [18] Вместе с тем, правоохранительными органами Российской Федерации в 2012 г. по ст.273 УК РФ (Создание, использование и распространение вредоносных программ для ЭВМ) было выявлено 889 преступлений, что на 28,3% выше показателя 2011 г. (693).

На сегодняшний день в Сети Интернет существуют сайты, где предлагаются услуги хакера. Так например, за взлом почты хакеры требуют 50 долл., за внедрения шпионской программы в компьютер 100 долл., за Ddos атаки 300-400 долл. В Америке аналогичные услуги стоят в 5 раз дороже.

Такими услугами в большинстве случаев пользуются преступники. Так например, полицейские-борцы с киберпреступностью рассказывают, что недавно квартирные воры освоили новый способ вычислять отсутствующих дома жильцов. Для этого группировки профессиональных грабителей понемногу начинают сотрудничать с хакерами. Они взламывают наиболее распространенные социальные сети, устанавливают состоятельных посетителей и из переписки узнают, когда те уезжают на отдых. В таких случаях даже "закладки" не требуются. В связи с этим существует угроза того, что компьютерные сети и электронная информация могут также использоваться для совершения уголовных преступлений, а доказательства совершения таких правонарушений могут храниться в этих сетях и передаваться по ним.

Таким образом, нормативно-правовое закрепление понятия «преступления в сфере высоких технологий» подразумевает его понимание в более широком смысле, не ограничивающееся конкретным средством, способом или орудием совершения преступления или сферой преступного посягательства.

Своевременная разработка специально криминологических мер по предупреждению преступлений в сфере высоких технологий при их комплексном использовании будет способствовать существенному повышению уровня информационной безопасности нашей страны и эффективной борьбе с противоправными деяниями. Необходимо учитывать, что предупредительные меры способны обеспечить необходимый эффект на практике лишь в тех случаях, когда осуществляется взаимодействие государственных органов с институтами гражданского общества, включая общественные объединения, органы местного самоуправления, средства массовой коммуникации, образовательные и научные организации на основе осуществления планирования, программирования своей совместной деятельности, учитывая специфику деятельности каждого заинтересованного субъекта профилактики преступной деятельности.

Библиография:

1. <http://www.internetworldstats.com/top20.htm> - 30.06.2012.

2. http://www.gazeta.ru/social/news/2012/07/30/n_2460333.shtml - Газета.ru
30/07/2012
3. . <http://www.internetworldstats.com/top20.htm>
4. Киберпреступник – человек совершающий преступления с использованием информационных технологий.
5. Статистические данные: Форма № 615 ГИАЦ МВД России № 61
6. Мирошников Б.Н. Сетевой фактор. Интернет и общество. Взгляд. – М.: Инфорос, 2012. С.16; http://www.r-trends.ru/trends/social/social_531.html
7. Никодимов И.Ю. ИНФОРМАЦИОННО-КОММУНИКАТИВНАЯ ФУНКЦИЯ ГОСУДАРСТВА И МЕХАНИЗМ ЕЕ РЕАЛИЗАЦИИ В СОВРЕМЕННОЙ РОССИИ (ТЕОРЕТИЧЕСКИЙ И СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ) диссертация на соискание ученой степени доктора юридических наук / Санкт-Петербург, 2001
8. Никодимов И.Ю. МЕСТО И РОЛЬ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ В МЕХАНИЗМЕ РЕАЛИЗАЦИИ ИНФОРМАЦИОННОКОММУНИКАТИВНОЙ ФУНКЦИИ ГОСУДАРСТВА Гуманитарные, социально-экономические и общественные науки. 2014. № 9. С. 216-219.
9. Никодимов И.Ю. ПРИНЦИПЫ И ИСТОЧНИКИ ИНФОРМАЦИОННОГО ПРАВА Юридическая наука: история и современность. 2016. № 3. С. 97-108.
10. Никодимов И.Ю. ТЕОРИЯ ИНФОРМАЦИОННОГО ПРАВА И НЕКОТОРЫЕ АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЕЕ РАЗВИТИЯ Юридическая наука: история и современность. 2015. № 12. С. 91-99.
11. Никодимов И.Ю. СЛОВАРЬ ОПРЕДЕЛЕНИЙ, ПОНЯТИЙ И ТЕРМИНОВ ИСПОЛЬЗУЕМЫХ В ОБЛАСТИ ТЕЛЕКОММУНИКАЦИЙ Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А.Бонч-Бруевича. Рецензенты: Доктор технических наук, профессор А. А. Гоголь; Кандидат юридических наук, доцент В. Ю. Голубовский. Санкт-Петербург, 1999. Сер. Учебники для вузов. Специальная литература