Жуковский Максим Юрьевич

Магистрант

Направление: Юриспруденция

Магистерская программа: Уголовный процесс, криминалистика и судебная экспертиза, теория оперативно-розыскной деятельности

Понятие и этапы развития компьютерной преступности

Аннотация. В статье проведен анализ понятия и этапов развития компьютерной преступности. Установлено, что по оценкам некоторых исследователей существует более 30 видов мошеннической деятельности в глобальной сети, среди них яркими представителями являются фишинг, лотереи, подарочные акции, благотворительность, спам с заманчивыми предложениями, «волшебные аккаунты» платежных систем и все возможные их комбинации. Также мошенники эксплуатируют легальные способы заработка в интернете – фрилансинг (удаленная работа), онлайновые инвестиционные схемы, схемы проведения аукционов и розничной торговли в режиме он-лайн.

Ключевые слова: компьютерная преступность, фишинг, фрилансинг, личность преступника, киберпреступник, ник-неймы.

Современные процессы по унификации и интеграции культурных, экономических, политических сфер общества как на мировом, так и на внутригосударственном уровне позволяют говорить о создании единого информационного пространства, не имеющего каких-либо рамок и условных границ [1, с. 90]. На этом фоне, в юридической литературе все чаще высказываются мнения о зарождении нового комплексного межотраслевого института – интернет-права, под которым профессор И.М. Рассолов предлагает понимать объективно обособившуюся внутри различных отраслей права совокупность взаимосвязанных правовых норм, объединенных общностью регулирования отношений в виртуальном пространстве Интернета [3, с. 104]. В

подобных условиях актуализируются вопросы обеспечения охраны основных прав и свобод граждан с учетом цифровых реалий общественной жизни. Поэтому, в рамках настоящей статьи, авторами проведена попытка комплексного исследования криминологических и виктимологических особенностей компьютерных преступлений на основе анализа судебно-следственной практики и статистических показателей.

Проведенное исследование последних позволяет выделить несколько тенденций:

1. На протяжении последних 15 лет в России отмечается стремительный рост числа регистрируемых компьютерных преступлений. Так, если в 1997 г. было зарегистрировано лишь 33 таких преступления, то уже в 2005 г. их количество составило 10214, в 2016 г. – 11636. Согласно статистическим данным МВД РФ, если в 2012 г. их число снизилось до 7398, то по данным только за второе полугодие 2017 г. было зафиксировано 5696 киберпреступлений [4]. Однако приведенные показатели свидетельствует не столько об уменьшении числа компьютерный преступлений, сколько о росте уровня их латентности и снижении эффективности деятельности правоохранительных органов в этом направлении. Причиной этому служат сразу несколько обстоятельств, а именно низкий профессиональный уровень сотрудников правоохранительных органов; отсутствие специальных центров по подготовке квалифицированных кадров в данной сфере уголовно-правовых знаний; определенная специфика методики расследования компьютерных преступлений и т.д.

2. Значительными являются также показатели причиненного киберпреступлениями ущерба. Так, согласно результатам «Norton Cybercrime Report 2012» ущерб, причиненный пользователем от киберпреступлений, составил 110 млрд. долларов США. Жертвами преступлений стали 556 млн. человек по всему миру (431 млн. – в 2011 г.) и 31,4 млн. человек – в России, а сумма причиненного ущерба, по оценкам специалистов «Botnet-мониторинг» компании Group-IB, составила 1,93 млрд. долларов [6].

3. Аналитиками рынка киберугроз отмечается рост количества атак на интернет-пользователей. К примеру, в 2013 г. компания Symantec отразила около 5,5 млрд. атак, что на 81% больше показателя 2012 года. По данным системы KasperskySecurityNetwork в 2014 г. показатель опасности сети Интернет составил 34,7% (32,3% в 2013 г.) [7]. Отмечается тенденция к изменению вектора компьютерной преступности, в частности, прогнозируется, что в 2017 году основным объектом посягательств киберпреступников станут социальные сети и мобильные устройства.

4. Как показал анализ судебной практики, количественное распределение компьютерных преступлений выглядит следующим образом [5]:

–наибольшей удельный вес в числе компьютерных преступлений составляет неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 85%;

–создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 15%;

–нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) – около 1%.

Компьютерные преступления имеют свою специфику. При изучении и разработке мер по их предупреждению необходимо учитывать целый комплекс особенностей, среди которых можно выделить:

1) условия информационного пространства, как особого «места совершения» компьютерных преступлений;

2) предметом таких посягательств является информация, лишенная физического воплощения;

3) исследуемые преступления являются многообъектными. По словам О.А. Герасимовой, объектом становится «не только информация, но и личность, сфера экономики, общественная безопасность и общественный порядок, сфера функционирования государства, безопасность человечества» [2, с. 22];

4) особенности субкультуры киберпреступников;

5) трансграничный характер киберпреступности, в соответствии с которым участниками хакерских атак становятся граждане нескольких государств, вступающие в преступный сговор через глобальные информационные сети, благодаря которым осуществляется координация их деятельности.

Характеризуя личность преступника, совершающего преступления в сфере компьютерной информации, стоит указать на следующие особенности:

1. Общий возрастной предел составляет 15–45 лет. Причем, наибольшее количество преступлений совершают лица в возрасте 18-24 лет (40-51%).

2. Среди лиц в возрасте 20–25 лет около 95% компьютерных преступлений совершается лицами мужского пола и около 5% женского; в возрасте 25–45 лет доля мужчин составляет 92%, женщин – 8%.

Среди особенностей личности киберпреступника (хакера) можно выделить «стремление к паразитическому образу жизни, отсутствие постоянного места работы, определенного места проживания», наличие высшего либо неоконченного высшего профессионального образования, обладание определенными навыками и познаниями в области компьютерной техники и информационных технологий, а также высокий уровень интеллектуального развития. Основными мотивами совершения киберпреступлений являются: хулиганский, основанный на стремлении злоумышленника противопоставить себя интересам общественной безопасности; стремление к «самореализации» посредством совершения хакерских атак; желание получения определенной прибыли от преступной деятельности. Как правило, компьютерные преступники принадлежат к так называемой «субкультуре хакеров», основными идеями которой являются свобода доступа к информации, неприятие культуры потребления, противопоставление себя обществу и миропорядку [1, с. 91].

3. Наблюдается тенденция к росту группового характера компьютерных преступлений (3–8,7% в 2013 году и 13–17% в 2014 г.). Как правило,

значительная часть киберпреступлений совершается высокоорганизованными преступными группами, в структуре которых можно выделить следующие элементы: центральное ядро, представленное фигурой организатора, осуществляющего функции планирования и координации хакерских атак; непосредственные исполнители. Злоумышленники, как правило, поддерживают контакт посредством сети «Интернет», не знают друг друга лично, при общении используют хакерский жаргон, сленг, а также вымышленные имена («ник-неймы» и др.).

Совсем недавно считалось, что данное криминальное явление существует только в зарубежных капиталистических странах, а в России, по причине слабой компьютеризации, отсутствует. Именно это обстоятельство обусловило, так называемое «отставание» в изучении злоупотреблений в сфере использования компьютерной информации и сетей Интернет у нас. Первое преступление с использованием компьютера в бывшем СССР было зарегистрировано в 1979 г. в Вильнюсе. Именно данный факт, поскольку он был занесен в международный реестр правонарушений подобного рода, научное сообщество признает «отправной точкой» в развитии компьютерной преступности в нашей стране. Но признание самостоятельного значения уголовно-правовой охраны общественных отношений, связанных с формированием и использованием автоматизированных информационных ресурсов и средств их обеспечения состоялось только в 1996 году, когда в УК РФ была включена глава 28 «Преступления в сфере компьютерной информации». Местом «дислокации» данной главы стал раздел IX УК РФ, озаглавленный «Преступления против общественной безопасности и общественного порядка».

Следует отметить, что общепринятого определения «компьютерной преступности», как и «компьютерного мошенничества» в науке уголовного права еще не предложено. В разных странах по-разному определяют структуру «компьютерной преступности» и виды преступлений с использованием компьютерных технологий. Данное положение дел является не только

теоретической проблемой, оно также значительно усложняет деятельность правоохранительных органов по противодействию преступлениям в рассматриваемой сфере, негативно влияет на правоприменительную практику. Поскольку отсутствовали соответствующие нормы в уголовном законодательстве, не было полной ясности относительно критериев фиксации совершенных мошенничеств в сфере высоких технологий.

Литература

1. Алавердов О.С. Криминологическая характеристика преступлений, совершаемых с использованием компьютерных технофлогий // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2009. №2.

2. Герасимова О.А., Анохин С.А. Правовые качества сотрудников органов внутренних дел (полиции) // Полицейская деятельность. 2011. – № 1.

3. Рассолов И.М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи // Вестник Московского университета МВД России. 2013. № 12.

4. Статистика и аналитика – МВД России [Электронный ресурс] // Режим доступа: https://mvd.ru/Deljatelnost/statistics.

5. Судебная статистика по делам, рассматриваемым федеральными судами общей юрисдикции и мировыми судьями [Электронный ресурс] // Режим доступа: http://www.cdep.ru/index.php?id=5.

6. 2012 NORTON CYBERCRIME REPORT [Электронный ресурс] // Режим доступа: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

7. Symantec [Электронный ресурс] // Режим доступа: www.symantec.com/ru/ru/.