ЮРИДИЧЕСКИЕ НАУКИ

УДК 343:004

М. М. Гедгафов
Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, г. Нальчик, e-mail: shmv1978@yandex.ru

ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ВЫСОКИХ ТЕХНОЛОГИЙ КАК ОБЪЕКТА ПРЕСТУПЛЕНИЙ

Ключевые слова: компьютерная информация, высокие достижения, преступление, угроза, правовое регулирование.

Целью данного исследования было изучение проблем и механизмов правовой характеристики преступлений в сфере компьютерной информации и высоких технологий. Задачи исследования: проведен анализ современного уголовного законодательства и научной литературы, который позволил нам выделить ряд особенностей, отличающих данные преступления от других: во-первых, данный вид преступления не требует физического сближения между жертвой и субъектом преступления в момент совершения преступления; во-вторых, они являются «автоматизированными»; в-третьих, субъект данного преступления не подвластен ограничениям, которые существуют в реальном физическом мире; в-четвертых, наука не способна еще устанавливать модели распространение различных видов данных преступлений географически демографически; в-пятых, сложность установления места преступления. Выводы: компьютерная информация ввиду ее реальной или потенциальной экономической ценности, сегодня является объектом преступных посягательств. Причем происходит это чаще всего умышленно и большей частью «теряются» персональные данные, коммерческая, государственная и военная тайны. В сложившейся ситуации задача государства и правоохранительных структур заключается в обеспечении информационной безопасности. Данный вид преступлений сегодня выступает отдельным видом бизнеса. Кража данных осуществляется путем несанкционированного извлечения информации из мест ее хранения при помощи взлома сетевых ресурсов государственных структур, больших и малых компаний, частных лиц и т.д. При этом данные преступления продолжают динамично развиваться и набирать обороты, превращаясь в источник серьезной угрозы государственной безопасности и правам человека.

M. M. Gedgafov
North Caucasus Institute of advanced training (branch) Krasnodar University of the Ministry of internal Affairs of Russia, Nalchik, e-mail: shmv1978@yandex.ru

CHARACTERIZATION OF COMPUTER INFORMATION AND HIGH TECHNOLOGY AS AN OBJECT OF CRIME

Keywords: computer information, high achievements, crime, threat, legal regulation.

The purpose of this study was to study the problems and mechanisms of the legal characteristics of crimes in the field of computer information and high technologies. Research objectives: the analysis of modern criminal legislation and scientific literature was carried out, which allowed us to highlight a number of features that distinguish these crimes from others: first, this type of crime does not require physical rapprochement between the victim and the subject of the crime at the time of the crime; secondly, they are «automated»; thirdly, the subject of this crime is not subject to the restrictions that exist in the real physical world; fourthly, science is not yet capable of establishing models for the dissemination of various types of these crimes geographically and demographically; fifth, the complexity of establishing the crime scene. Conclusions: computer information, due to its real or potential economic value, is today the object of criminal encroachments. Moreover, this happens most often on purpose and for the most part personal data, commercial, state and military secrets are «lost». In this situation, the task of the state and law enforcement agencies is to ensure information security. This type of crime is now a separate type of business. Data theft is carried out by unauthorized extraction of information from its storage sites by hacking network resources of government agencies, large and small companies, individuals, etc. At the same time, these crimes continue to develop dynamically and gain momentum, turning into a source of serious threat to state security and human rights.

Введение

Современная жизнедеятельность общества обусловилась повсеместным распространением глобальной сети Интернет, которая сегодня выступает основополагающим фактором сферы коммуникации. Так, посредством сети Интернет происходит неограниченный обмен товарами, услугами, работами, информационными и финансовыми ресурсами между пользователями. Как известно, эти действия напрямую зависят от достижений и возможностей различных информационных технологий и подвергаются постоянным кибератакам.

Таким образом, достижения современных информационных технологий предопределили оперативный и практически неограниченный обмен цифровой информацией и дали возможность зарождению специфического, сложного вида преступлений, связанных с посягательством на электронную информацию [1].

Постановка проблемы

Компьютеризация – явление социально значимое, которое можно рассматривать совершенно с разных позиций сообразно тем последствиям, которые сопутствуют данному феномену. И здесь следует принимать во внимание, что наряду с позитивными достижениями компьютеризация имеет и оборотную сторону, обусловившую возникновение преступлений в сфере компьютерной информации и высоких достижений.

Сегодня компьютерное преступление в качестве уголовно-правового понятия можно представить как предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства [1].

Преступления в сфере компьютерной информации и высоких достижений можно подразделить на три категории:

– злоупотребление компьютером, которое выражается в осуществлении мероприятий с использованием компьютера для извлечения выгоды с нанесением ущерба третьим лицам;

– прямое незаконное использование компьютерных сетей в совершении преступления;

– любое незаконное действие, для успешного осуществления которого необходимы хорошие познания в информационных технологиях.

Наряду с этим в практический оборот учеными и практиками введены термины «киберпреступность», «кибератака» под которыми стали понимать любые преступления, совершаемые посредством компьютерных сетей и систем, т.е. в электронной среде. На практике различают два вида указанных преступлений:

– в узком смысле под киберпреступлением понимается любое противоправное деяние, которое осуществляется с помощью компьютерных технологий с целью преодоления защиты компьютерных систем и обрабатываемых ими данных;

– в широком смысле под киберпреступлением следует понимать любое противоправное деяние, которое совершено при помощи компьютерных систем или сетей, в том числе незаконное хранение или распространение информации с их помощью [2].

Вместе с тем, сегодня мы становимся свидетелями произошедшего перехода от простой одиночной компьютерной преступности к организованной и данный вид криминалитета выйдя за пределы национальных границ, трансформировался в международную преступность. Все это конечно усложнило возможности раскрытия и расследования таких преступлений сотрудниками правоохранительных органов [3, 4].

Обоснование

Компьютерная информация ввиду ее реальной или потенциальной экономической ценности, сегодня является объектом преступных посягательств. И никого уже не удивляет происходящая утечка конфиденциальной информации, как коммерческих, так государственных и некоммерческих организаций. Причем происходит это чаще всего умышленно и большей частью «теряются» персональные данные, коммерческая, государственная и военная тайны [4, 5].

В сложившейся ситуации задача государства и правоохранительных струк-

тур заключается в обеспечении информационной безопасности общества.

Как мы выше указали, высокие технологии, являясь средством обмена больших объемов цифровой информации, в значительной степени облегчили жизнедеятельность людей, и вместе с тем, создали реальную угрозу для правопорядка, обусловив возникновение ранее неизвестных правонарушений.

Компьютерную информацию начали похищать с целью ее сбыта заказчикам. Так данный вид преступления стал отдельным видом бизнеса. Кража данных осуществляется путем несанкционированного извлечения информации из мест ее хранения при помощи взлома сетевых ресурсов государственных структур, больших и малых компаний, частных лиц и т.д. При этом данный вид преступления продолжает динамично развиваться и набирать обороты, превращаясь в источник серьезной угрозы государственной безопасности и правам человека. Следует также обратить внимание, что возросло и количество субъектов, совершающих данные преступления. Это обусловило и их различие по уровню их профессионализма и социальному положению. Так, среди них можно выделить:

– хакеров – это лица, взламывающие компьютерные системы и сети для получения полного доступа к их содержимому. По большей части это делается для удовлетворения собственных амбиции (хакеры, они своеобразные «позеры», которые просто хотят продемонстрировать миру свои умения);

– шпионов – это лица, взламывающие компьютерные системы и сети для установления слежки и получения информации для использования в политических, экономических и иных целях;

– террористы – это лица, взламывающие компьютерные системы и сети в целях достижения эффекта опасности, который впоследствии используется для политического воздействия на государственные органы и структуры;

– корыстные преступники – это лица, вторгающиеся в компьютерные системы и сети для приобретения личных выгод;

– вандалы – это лица, вторгающиеся в компьютерные системы и сети для их разрушения, собственно не преследуя больше никаких выгод [6].

Законодательство, регулирующее сферу компьютерных технологий и высоких достижений содержит 11 информационных процессов, защищаемых от преступных посягательств. Это:

– создание и обработка информации;

– сбор и поиск информации, в т.ч. доступ к ней;

– накопление и хранение информации;

– защита информации;

– распространение и предоставление информации;

– непредставление информации;

– копирование информации;

– уничтожение информации;

– изменение информации (модификация);

– хищение, изъятие и утрата информации;

– блокирование информации [7].

Произошедший в последнее десятилетие скачок в научно-техническом развитии обозначил ряд проблем, связанных с информатизацией государства, общества и правопорядка. Так, обусловилась необходимость информационного обеспечения оперативно-розыскной деятельности, которое являясь элементом структуры информатизации правоохранительных органов, выступает неотъемлемой частью информационной системы [3, 6].

Следует обратить внимание, что выявление и раскрытие компьютерных преступлений, в особенности тех, которые совершаются организованными преступными группировками, требует не только специального профессионального образования (квалификации) и высокого интеллектуального уровня сотрудников правоохранительных органов, но и хороших знаний, как в области права, так и вычислительной техники.

В последние годы, произошедшие в обществе глобализационные процессы, привели к сращиванию компьютерной преступности с организованной преступностью, а также к интернационализации этого вида преступлений. Больше всего кибератакам подвергаются банковские структуры, когда со счетов физических и юридических лиц «исчезают» большие денежные суммы. Также к наиболее распространенным видам незаконного использования глобальной компьютерной сети является несанкци-

онированное вмешательство в работу автоматизированных систем мобильных операторов связи в целях шпионажа, политических целей, терроризма [6, 7, 8].

Вместе с тем, такая специфическая особенность глобальной сети как отсутствие границ, стала благоприятной почвой для организации виртуальных банд хакеров, которым стали доступны информационные системы различных государств с возможностью проникновения в специально защищенные информационные ресурсы.

Анализ современного уголовного законодательства и научной литературы позволил нам выделить ряд особенностей, отличающих данные преступления от других:

– во-первых, данный вид преступления не требует физического сближения между жертвой и субъектом преступления в момент совершения преступления;

– во-вторых, они являются «автоматизированными»;

– в-третьих, субъект данного преступления не подвластен ограничениям, которые существуют в реальном физическом мире;

– в-четвертых, наука не способна еще устанавливать модели распространение различных видов данных преступлений географически демографически;

– в-пятых, сложность установления места преступления [5, 6, 8].

Главная проблема для правоохранительных органов при раскрытии и расследований таких преступлений состоит в установлении места их совершения и право, какого государства следует применять, если объект и субъект находятся в разных странах. Следует также принимать во внимание тот факт, что суды разных стран устанавливают свою территориальную юрисдикцию в отношении преступлений в сфере компьютерной информации и высоких достижений, в зависимости от следующих оснований:

– место совершения преступного деяния;

– место нахождения компьютера;

– место нахождения субъекта преступления – принцип субъективной территориальности;

– место наступления общественно опасного последствия – принцип объективной территориальности;

– место нахождения любой из перечисленных оснований, в том числе и транзит через территорию страны [9].

Еще одной особенностью данной группы преступлений является разграничение их в зависимости от объекта – на что посягает субъект преступления. В данном случае преступления подразделяются на те, которые наносят ущерб конкретным объектам (например, хищение персональных данных из компьютерной базы) и те, которые посягают на неопределенный круг объектов (например, создание и распространение вредоносных программ).

Таким образом, преступления в сфере компьютерной информации, несмотря на свою распространенность, до сегодняшнего дня остаются феноменами, так как наукой еще четко не установлено правовое регулирование ответственности за данные преступления, поскольку они обладают особенностью стремительно развиваться, появляются новые виды преступлений с использованием компьютерных технологий, что правоприменительная практика просто не поспевает охватить указанные достижения [6, 8, 9].

Важнейшим элементом криминалистической характеристики преступления выступает способ его совершения, состоящего из комплекса специфических действий правонарушителя по подготовке, совершению и маскировки преступления. Указанные действия являя собой определенную систему, отображаются во внешней среде представляя собой в информационном плане своеобразную модель преступления. Наибольший интерес для криминалистов в отношении данных преступлений представляют следы, указывающие на то, как преступник попал и скрылся с места происшествия, преодолел преграды, использовал свое служебное положение, выполнил намеченную преступную цель, какие знания и навыки использовал, попытался скрыть следы своих действий. Важны также следы, свидетельствующие о характере связи преступника с предметом преступного посягательства [10].

Основные следственные задачи при расследовании компьютерных преступлений состоят в установлении:

– факта неправомерного доступа к локальной сети;

– места, времени и способа несанкционированного проникновения в сеть;

– надежности средств защиты компьютерной информации;

– лиц, совершивших неправомерный доступ, их виновности и мотивов преступления;

– вредных последствий преступления;

– обстоятельств, способствовавших преступлению [10, 11].

Способ совершения преступления в ряде составов является необходимым элементом объективной стороны преступления и входит в его уголовно-правовые характеристики, а в некоторых случаях служит даже квалифицирующим обстоятельством.

Однако следует помнить, что в уголовно-правовом аспекте способ совершения преступления представлен в общем виде и для него безразличны конкретные способы проникновения, средства, которые используют при этом, источники их получения и т.д. Если же эти обстоятельства носят существенный характер, то применяют криминалистическую характеристику способа совершения преступления. Вместе с тем, преступления в сфере компьютерной информации, как мы уже указывали, довольно специфичны и отличаются от известных криминалистической науке преступных посягательств. Наука и практика выделяет три группы неправомерного доступа к компьютерной информации:

– способы непосредственного доступа;

– способы удаленного доступа;

– комплексные способы [10, 11].

Вместе с тем, выделяют также три группы потерпевших от таких преступлений: собственники компьютерной системы; клиенты, пользующиеся их услугами; иные лица.

Следует отметить, что первая группа потерпевших, чаще всего, предпочитает не обращаться в правоохранительные структуры, что делает такие преступления латентными.

Заключение

В заключении отметим, что расследование преступлений, связанных с компьютерной информацией должно производиться с обязательным участием специалиста этой области, поскольку даже малейшие неквалифицированные действия с компьютерной системой могут привести к необратимой утрате ценной розыскной и доказательственной информации [12].

Выводы

На основе изложенного мы приходим к выводу, что сегодня возможности компьютерных технологий, высоких достижений и глобальной сети Интернет предоставили практически неограниченные возможности злоумышленникам для осуществления противоправных деяний, связанных с неправомерным получением, распространением и использованием компьютерной информации. Обобщая уголовно-правовой аспект преступлений в сфере компьютерной информации и высоких достижений, следует отметить, что борьба с данным явлением сегодня особенно актуальна, особенно когда, в последние годы при постоянном количественном и качественном росте кибепреступности, раскрываемость почти не изменилась. Такая ситуация коррелируется с перечисленными выше проблемами и свидетельствует о том, что необходимо постоянно совершенствовать способы защиты информации.

Библиографический список

1. Ефремова М.А. К вопросу об уголовно-правовом обеспечении информационной безопасности // Вестник Тверского государственного университета. Серия: Право. 2013. № 35. С. 86-91.

2. Аносов А.В., Кашапова Е.С. Понятие преступлений в сфере высоких технологий // Академическая мысль. 2018. № 4 (5). С. 15-19.

3. Лапунин М.М. Общая характеристика преступлений в сфере компьютерной информации // Право. Законодательство. Личность. 2013. № 1. С. 36-44.

4. Нечаева Е.В., Латыпова Э.Ю., Гильманов Э.М. Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27 (1-4). № 1. С. 80-86.

5. Козаев Н.Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: монография. М.: Издательство Юрлитинформ, 2019. 480 с.

6. Бегишев И.Р., Бикеев И.И. Преступления в сфере обращения цифровой информации: монография // Издательство «Познание». Казань. 2020. Сер. Цифровая безопасность. 300 с.

7. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ. [Электронный ресурс] // Режим доступа http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.10.2020).

8. Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации / Диссертация на соискание ученой степени // Казанский (Приволжский) федеральный университет. Казань. 2017.

9. Никеров Д.М., Хохлова О.М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2019. № 2 (89). С. 82-93.

10. Шифельман С.А. Специальные знания в области компьютерных технологий // Академия педагогических идей Новация. Серия: Студенческий научный вестник. 2019. № 1. С. 538-540.

11. Ткаченко Н.Н. Некоторые аспекты определения понятий киберпреступлений и кибертерроризма // Общественная безопасность, законность и правопорядок в III тысячелетии. 2019. № 5-1. С. 161-164.

12. Сексенбаев К.К., Султанова Б.К., Кисина М.К. Информационные технологии в развитии современного информационного общества // Молодой ученый. 2015. № 24 (104). С. 191-194.