Омарова А.Б., Маликова Ш.Б.

К понятию личности преступника преступлений в сфере компьютерной информации

За последние десять лет сети Интернет превратились в виртуальную площадку, в пространство, где люди имеют возможность выражать идеи, заниматься общественной деятельностью и пр. На сегодняшний день сети Интернет играют важную роль в сфере коммуникаций: мы проводим различные операции с денежными средствами, с использованием как компьютера, так и банкомата, и других платежных систем, прокладываем маршруты, ищем хорошие рестораны, узнаем любую интересующую нас информацию. Конечно, понятно, что все эти действия зависят от информационных технологий. В статье исследуется проблемы защиты компьютерной информации. Изучена личность преступников в сфере информационных технологий, виктимологические аспекты компьютерных преступлений.

Ключевые слова: компьютерная информация, интернет, информационная сфера, хакер, компьютерная грамотность, преступность.

Omarova A.B., Malikova Sh.B.

To the notion of identity of the perpetrator of crimes in sphere of computer information

Over the past ten years the Internet has become a virtual Playground, a place where people have the opportunity to Express ideas, to engage in social activities, etc. today, the Internet plays an important role in the field of communications: we conduct a variety of transactions with money, like using a computer, ATM, and other payment systems, the device calculates routes, looking for good restaurants, get to know us any interesting information. Of course, all these actions depend on information technology. The article investigates problems of computer information protection. Studied the personality of criminals in the field of information technology, victimological aspects of computer crimes.

Key words: computer information, Internet, media hacker, computer literacy, crime.

Омарова А.Б., Маликова Ш.Б.

Компьютерлік ақпарат аясындағы қылмыстардағы қылмыскер тұлғасына түсінік

Соңғы он жылда Интернет желісі адамдардың өздерінің ойларын, қоғамдық қызметтері мен т.б. айта алатын кеңістігіне, виртуалды алаңға айналды. Қазіргі күні Интернет желісі коммуникация аясында маңызды рөлге ие: біз компьютерді, банкоматтарды, басқа да төлем жүйелерін пайдалана отырып ақша қаражаттарымен әртүрлі операцияларды жүргіземіз, маршруттар жасап, жақсы ресторандар іздейміз, бізді қызықтырған кез келген ақпараттарды біле аламыз. Әрине, бұл әрекеттердің барлығы ақпараттық технологияларға тәуелді. Мақалада компьютерлік ақпаратты қорғау мәселелері қарастырылған. Ақпараттық технологиялар аясындағы қылмыскердің тұлғасы, компьютерлік қылмыстардың виктимологиялық аспектілері зерделенген.

Түйін сөздер: компьютерлік ақпарат, интернет, ақпараттық ая, хакер, компьютерлік сауаттылық, қылмыстылық.

УДК 343.9(4/9)

Омарова А.Б., *Маликова Ш.Б.

Казахский национальный университет имени аль-Фараби,
Республика Казахстан, г. Алматы
*E-mail: msholpan7876@mail.ru

К ПОНЯТИЮ ЛИЧНОСТИ ПРЕСТУПНИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Первостепенное значение в современных условиях приобретают высокие технологии, в особенности в области информатизации. Без собственного информационного потенциала, отвечающего самым строгим меркам научно-технического прогресса, эффективной правовой политики в этой сфере решить задачи вхождения Казахстана в число успешных стран мира невозможно. Вместе с этим без решения вопросов обеспечения информационной безопасности обозначенные задачи будут в целом труднодостижимы.

Главным образом проблема защиты компьютерной информации и информационных систем сейчас является одной из самых актуальных во всем мире. Новые возможности, предоставляемые информационными технологиями, их широкая распространенность и доступность сделали эту область привлекательной для представителей криминальной среды. Стремительное развитие информационно-телекоммуникационных сетей, создание многочисленных информационных систем, разработка более совершенных технических устройств – все это создает условия, облегчающие совершение преступлений в этой сфере, число которых с каждым годом увеличивается как в Республике Казахстан, так и в зарубежных странах.

Преступления в сфере информационных технологий являются одной из важнейших и острейших проблем уголовной политики в XXI веке, особенно в свете глобализации, и как следует из этого – дальнейшей популяризации и доступности технологий любого типа и принципов работы. Данные преступления включают в себя в первую очередь распространение различных вредоносных программ и вирусов, распространение противоправной информации в интернете (например, материалов, возбуждающих межрелигиозную и национальную вражду между людьми, порнографических материалов, способствующих растлению подростков имеющих свободный доступ к персональному компьютеру, а так же клеветы и т.д.). К тому же, одним из самых опасных и распространенных преступлений, совершаемых с использованием интернета, является мошенничество. В этой связи требует изучения важный аспект уголовной политики в сфере информационных технологий – ее непосредственное организационное обеспечение.

Информационная сфера как быстро развивающаяся сфера нуждается и в адекватном правовом регулировании. Задача уголовного законодательства в этой связи – обеспечить пресечение наиболее общественно опасных посягательств на компьютерную информацию, информационные системы и сети. Надо отметить, что именно в указанной сфере уголовное право Республики Казахстан оказалось не вполне готовым к стремительному развитию компьютерной техники и ее внедрению в повседневную жизнь людей. Не только уголовное право Казахстана, но и право в целом и уголовное право зарубежных стран в том числе, нередко отстают от развития общественных отношений, связанных с использованием информации, и поэтому процесс нахождения адекватных форм и способов их правового регулирования, в том числе противодействия компьютерным преступлениям, идет уже не один десяток лет во многих развитых странах мира.

В Республике Казахстан и во многих странах СНГ первые нормы об уголовной ответственности за преступления в информационной сфере были включены во второй половине 90-х годов прошлого века и уже не отвечали современному состоянию общественных отношений и техническому прогрессу. В этой связи была очевидна необходимость их совершенствования. Этим отчасти и было обусловлено принятие нового Уголовного кодекса Республики Казахстан.

Однако это обстоятельство не снимает проблему окончательно, поскольку со временем появляются новые технологии, соответственно, новые формы преступности, к примеру, взлом сотовых телефонов с использованием Bluetooth или беспроводной сети связи Wi-Fi, нарушение работы информационных систем (Dos-атаки), на которые в рамках действующих редакций статей УК РК от 3 июля 2014 года не всегда можно эффективно реагировать. С принятием нового Уголовного кодекса возникла проблема отсутствия необходимых механизмов реализации его норм. Личность преступника рассматривается в криминологии как совокупность свойств, присущих совершающему или совершившему преступление человеку, составляющих его индивидуальность. В криминологии эта совокупность свойств изучается, чтобы на их основе определить факторы, влияющие на совершение конкретного преступления. Эти факторы могут быть использованы в ходе расследования и рассмотрения уголовного дела, а также при создании основ и методик индивидуальной профилактики.

С учетом общественной опасности, высокой латентности, сложности расследования компьютерных преступлений, особое внимание правоохранительных органов должно быть сосредоточено на их выявлении и качественном расследовании. Этому процессу способствует криминалистическая характеристика преступлений как часть методики расследования преступления, где большое значение имеет элемент или система свойств, характеризующих личность преступника, совершившего такое преступление с учетом виктимологических аспектов данных деяний. Здесь важно отметить связь криминалистической и криминологической характеристик личности преступника.

Исследование системы свойств, характеризующих личность преступника, предполагает исследование криминологической структуры личности преступника, которая включает: сведения о поле, возрасте, гражданстве, образовании, социальном и должностном положении, а также прежних судимостях, характере, мотивах и целях преступной деятельности, действий, роли в преступлении и других признаках личности преступников.

Круг лиц, совершающих преступления в сфере компьютерной информации, довольно широк. По данным специальных исследований, это могут быть как и высококвалифицированные специалисты, так и дилетанты, которые имеют разный социальный статус и уровень образования. Учитывая специфику преступлений в сфере компьютерной информации, для решения задач расследования важно получить представление о «портрете» преступника.

Достаточная информационная база для этого в полной мере еще не сложилась, так как статистика таких преступления относительно молода, да и сами преступлений в сфере компьютерной информации обладают определенной спецификой, требующей от преступников наличия навыков, умения, знаний о функционировании компьютерных систем, свойств компьютерной информации, определенного программного обеспечения.

Если в 2001году, по данным Комитета по правовой статистике и специальному учету Генеральной Прокуратуры РК в 2011году, было выявлено 312 лиц совершивших преступления, то в 2015 году это число уже составило 744. Очевидная положительная динамика свидетельствует о том, что, несмотря на рост количества зарегистрированных преступлений в сфере компьютерной информации, качественно-количественное

соотношение отдельных свойств, характеризующих личность преступника, не стабильно.

Достаточно стабильными остаются лишь сведения о возрасте преступников. Так, в 2011-2015 гг. «компьютерные» преступления совершали граждане в возрасте от 16 до 17 лет – 2-17,5%; 18-24 года от 30% – 41%; от 25 до 34 лет от 8,5-15,6%. Различие в возрастных категориях может свидетельствовать лишь об общем подъеме компьютерной грамотности в Казахстане.

Образовательный уровень лиц, совершивших данную категорию преступлений, является важным показателем интеллектуального уровня преступников и находится в определенной взаимосвязи с характером их преступных действий. Исследование преступлений рассматриваемой категории свидетельствует о том, что среди совершивших их лиц преобладают лица со средним образованием – от 50% до 69%, со средним специальным образования – от 7% до 21%, с высшим образованием – от 17% до 20,1%.

Повышение уровня «компьютерной грамотности» преступников увеличивает латентность преступлений данного вида.

Проведенный анализ указанных выше статистических данных личности лиц, совершивших преступления в сфере компьютерной информации, позволяет выделить некоторые достаточно общие характеристики личности преступника – это молодой человек, имеющий среднее (среднее – специальное) образование, в возрасте 18-24-лет, противоправные действия он совершает преимущественно без соучастников, ранее в противозаконных действиях незамечен, с достаточно высоким уровнем технического и специального образования. По роду своей профессиональной деятельности они связаны либо с определенным режимом работы, либо с затруднениями осуществления контроля при исполнении последними своих профессиональных обязанностей, имеют свободный доступ к компьютерным системам. Важно отметить психологические аспекты личности: замкнутость, скрытность. Специфические интересы личности, связаны с увлечением литературой по компьютерной технике, информационным технологиям, программным обеспечением.

Выделение типовых характеризующих черт разных категорий «компьютерных» преступников, знание их основных черт способствует оптимизации процесса выявления лиц, облегчает процесс расследования.

Что касается виктимологических аспектов компьютерных преступлений, то в криминологии уже давно известны зависимости между личностью, состоянием, поведением жертвы и вероятностью стать жертвой и признано, что изучение преступности без анализа виктимологического аспекта является неполным и неточным.

Выявлено, что в существующих исследованиях киберпреступности мало уделяется внимание проблеме виктимологии жертв компьютерных преступлений, либо в них характеризуются лишь отдельные подвиды таких преступлений, не раскрывающие подробно другие виды и все явления компьютерной преступности в целом. Большинство таких исследований интернет-преступности носят фрагментарный характер в отношении виктимологической характеристики компьютерной преступности в целом.

Компьютерная (Интернет) преступность не имеет однородный характер, и поэтому причины виктимности в зависимости от конкретного вида деяний могут существенно различаться: неправомерный доступ к информации, в информационную систему (ст. 205 УК РК); неправомерное уничтожение или модификация информации (ст. 206 УК РК) и др. Преступления стали часто совершаться путем использования краденых паролей доступа к различным Интернет-ресурсам.

Самым распространенным видом Интернет-преступлений является неправомерный доступ. Исходя из изученных уголовных дел, возбужденных по ст. 205 УК РК в 2014-2015 гг., где неправомерный доступ был осуществлен с помощью Интернет-сети, получилась следующая картина: мужчины становились жертвами преступлений в 50,8% случаев, а женщины – в 47,5%.

Один из самых важных и главных принципов работы в сети Интернет – анонимность, поэтому жертвы, как правило, не знакомы со злоумышленником практически во всех случаях и видах противоправных деяний в Интернете.

Путем социального опроса было установлено, что в 82,6% случаев пострадавшие от незаконного доступа посредством Интернет не защищали свои данные, и преступники беспрепятственно с помощью общераспространенных программ получили доступ к вычислительным машинам жертв.

Выяснилось, что основная причина таких преступлений – небрежность в вопросах защиты своей информации, в том числе использования технических средств защиты, является обстоятельством, способствующим росту количества преступлений, совершенных посредством Интернет. Иными словами, основным виктимологическим фактором является несоблюдение по-

терпевшим мер информационной безопасности, а не знакомство с преступником, антропологические характеристики или какие-либо другие факторы виктимизации.

Как выяснилось, основной причиной высокой латентности компьютерных преступлений является также несообщение в правоохранительные органы о факте преступления. Кроме того, многие из Интернет-преступления не оставляют следов: например, неправомерный доступ без причинения материального ущерба, что чаще всего и встречается. Все эти причины способствуют высокой латентности компьютерной преступности.

В этой связи необходимы активные меры в борьбе с компьютерными преступлениями и в частности разработка и внедрение системы виктимологической профилактики Интернет-преступлений: важно создать систему мер правовой пропаганды; выстроить криминологическую профилактику, направленную на повышение технического уровня пользователей с учетом определенной категории Интернет-пользователей: в первую очередь, тех, которые не используют средства защиты или не знают о существовании таковых, а затем профессиональных пользователей, которых необходимо информировать о новых внедрениях в сфере компьютерной безопасности. При этом все рекомендуемые средства защиты необходимо ранжировать в зависимости от ценности защищаемых компьютерных данных и навыков пользователя.

В новом Уголовном Кодексе РК киберпреступности посвящена отдельная глава 7, в которой предусмотрено 9 статей за уголовные правонарушения в части киберпреступности. Она введена с целью надлежащего обеспечения уголовно-правовой защиты информационной безопасности. Тем не менее анализ норм уголовного законодательства в сфере обеспечения информационной безопасности показал, что не всегда корректно формируются базовые правовые понятия в этой области. С 2009 года в казахстанских законах понятие «веб-сайт» заменило более широкое понятие «интернет-ресурс».

Анализ последних законодательных новелл показывает, что вопросам терминологии, используемой законодателем для формулирования норм о преступлениях в сфере информационной безопасности, не уделяется должного внимания. Соответственно, предлагается в дальнейшем изучить зарубежный опыт борьбы с такими преступлениями.

Новая редакция УК РК поставила ряд серьезных проблем: определение объекта соответствующих преступлений, четкое определение их понятия и систему; установление критериев выделения близких по содержанию видов преступных посягательств, отграничение их от других составов преступлений; решение вопросов квалификации.

Бланкетный характер диспозиций уголовно-правовых норм требует обращения к различным нормативным правовым актам, регулирующим возникающие правоотношения, и знания их терминологии.

Здесь следует считать верной позицию, по которой именовать всю совокупность данных преступлений термином «компьютерные преступления» не верно, поскольку термин «компьютер» является лишь разновидностью коммуникационной техники или информационного оборудования и не исчерпывает всего разнообразия техники и отношений, связанных с обращением информации, например, использование телефонов, коммуникаторов, микроволновой, спутниковой или другой системы передачи данных.

Исследование проблем в рассматриваемой сфере позволило прийти к выводу, что с развитием технологий, несомненно, появятся новые специфические формы правонарушений, к которым, возможно, будут не применимы составы преступлений, предусмотренные вышеуказанными статьями нового УК РК.

Поэтому в настоящее время главным шагом в борьбе с преступностью, посягающей на информационную безопасность, должно стать создание универсального развитого и детального понятийного аппарата. Эти термины и понятия потребуют определенных пояснений, основанных на осмыслении технических характеристик новых средств обработки информации и сущности самой информации, хранящейся на машинном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, как новой уголовно-правовой категории. Терминологическая неточность изложения уголовного законодательства может повлечь неправильное его применение, и, следовательно, негативные последствия.

Статья выполнена в рамках исследования № 2576/ГФ4 «Уголовная политика Республики Казахстан в сфере обеспечения информационной безопасности и противодействия компьютерной преступности».

Литература

1 Фатьянов, А.А. Правовое обеспечение безопасности информации в Российской Федерации. – М., 2001. – 234 с.

2 Лопашенко Н.А. Уголовно-правовая и криминологическая политика государства в области высоких технологий // Информационные технологии и безопасность: Сб. науч. тр. Междунар. конф. Вып. 3. – Киев, 2003. – С. 89-97.

3 Войниканис Е.А., Якушев М.В. Информация. Собственность. Интернет: Традиция и новеллы в современном праве. – М., 2004. – 368 с.

4 Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества: дисс. ... доктор. юрид. наук. – М., 2008. – 438 с.

References

1 Fat'janov, A.A. Pravovoe obespechenie bezopasnosti informacii v Rossijskoj Federacii. – M., 2001. – 234 c.

2 Lopashenko N.A. Ugolovno-pravovaja i kriminologicheskaja politika gosudarstva v oblasti vysokih tehnologij //Informacionnye tehnologii i bezopasnost': Sb. nauch. tr. Mezhdunar. konf. Vyp. 3. – Kiev, 2003. – S. 89-97.

3 Vojnikanis E.A., Jakushev M.V. Informacija. Sobstvennost'. Internet: Tradicija i novelly v sovremennom prave. – M., 2004. – 368 s.

4 Poljakova T.A. Pravovoe obespechenie informacionnoj bezopasnosti pri postroenii informacionnogo obshhestva: diss. ... doktor. jurid. nauk. – M., 2008. – 438 s.