УДК 343.711

Бекишева С.Д.
Главный научный сотрудник Центра исследования проблем уголовной политики и исполнения наказания Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, д.ю.н., доцент

УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ КРАЖ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Основным приоритетом на 2017 год, вытекающим из Послания Президента Республики Казахстан Н.Назарбаева народу Казахстана от 31 января 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность», является «ускоренная технологическая модернизация экономики» [1] с последующим развитием в стране таких перспективных отраслей, как 3D-принтинг, онлайн-торговля, мобильный банкинг, цифровые сервисы. Президентом отдано поручение Правительству – разработать и принять отдельную программу «Цифровой Казахстан», а также дано четкое указание «адаптировать наше законодательство под новые реалии», «принять меры по созданию системы «Киберщит Казахстана» [1].

Предпринимаемые государством меры являются весьма своевременными, так как в Казахстане уже наблюдается тенденция роста хищений с использованием информационных технологий. Так, за два года число кибермошенничеств (ст.190 ч.2 п.4 УК) увеличилось в 23 раза (2015 г.- 45, 2016 г. – 1048) [2].

Хотя в нашем государстве хищения с использованием информационных технологий не получили широкого распространения, однако основные тенденции развития преступности за рубежом показывают динамику роста такого рода уголовных правонарушений. Так, в России «за период с июня 2015-го по май 2016 года у банков в результате целевых атак хакеры похитили 2,5 млрд рублей. Сумма целевых киберхищений у банков, по сведениям Group-IB, к аналогичному периоду 2013-2014 годов выросла на 292%. (По данным ЦБ, с июня 2015-го по май 2016 года у российских банков хакеры украли 1,37 млрд рублей.)» [3].

Данный вид уголовных правонарушений причиняет значительный ущерб экономике государства. По данным, приведенным в июле 2013 г. в совместном анализе американского Центра стратегических и международных исследований и компании McAfee, ежегодные потери мировой экономики от киберпреступлений достигли уже 500 миллиардов долларов. По мнению зарубежных экспертов, доход от киберпреступлений значительно превысит доход от других преступлений, включая торговлю наркотиками [4].

Опасность киберхищений с использованием информационных технологий заключается в том, что они могут носить трансграничный характер, сложны в раскрытии и расследовании и во многих случаях совершаются организованными группами. По мнению зарубежных экспертов, Интернет используется преступными группами не только как вспомогательное средство, но и как место и основное средство совершения традиционных преступлений — мошенничеств, краж, вымогательств. По данным Европола, только в ЕС, действует около 3600 таких групп [5].

Такие неблагоприятные факторы свидетельствуют о необходимости разработки комплекса мероприятий, направленных на опережение преступных проявлений в сфере информационных технологий, подготовки высококвалифицированных сотрудников правоохранительных органов Республики Казахстан, имеющих навыки раскрытия и расследования киберхищений.

Однако на данном этапе не все сотрудники правоохранительных органов способны выявить и правильно квалифицировать киберхищения, что приводит к искажению статистических данных. Так, анализ зарегистрированных за три года в ЕРДР материалов по п.4 ч.2 ст.188 УК РК показал, что на учет ставятся случаи краж, не имеющих никакого отношения к данному составу уголовного правонарушения.

Так, в Жамбылском районе Алматинской области с заявлением обратился гр. К. о том что в период времени с 14.-15.01.2017 г. неизвестные лица путем отжима пластикового окна совершили кражу отопительных батерей.

В Сарыаркинском районе г.Астаны 21.08.17 г. в 04.55 с заявлением обратилась гр.Д. о том, что неизвестный 21.08.17 г. в период времени с 02.00 по 03.00 путем отжатия пластикового окна проник в комнату и тайно похитил личное имущество (сумку, деньги, документы) на общую сумму 35.000 тенге.

В г.Костанае с заявлением обратилась гр.П. и просила принять меры к гр.Б., который путем обмана завладел деньгами в сумме 100000 тенге и т.п. [2].

Вышеуказанное свидетельствует о необходимости исследование понятия и состава хищений с использованием информационных технологий, в частности, киберкраж, что является актуальным по политическим, социальным, экономическим и профессиональным соображениям.

Пунктом 4 ч.2 статьи 188 «Кража» УК РК предусмотрена уголовная ответственность за кражу, совершенную путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций (далее - киберкража).

При рассмотрении киберкражи, являющейся одной из форм хищения, необходимо для ее общей характеристики несколько слов сказать об общих признаках хищения как понятия, объединяющего определенный род преступлений против собственности.

Под хищением согласно п.17 ст.3 УК РК понимаются тайные совершенные с корыстной целью противоправные безвозмездные изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества [6]. Следовательно, объективными признаками хищения являются: 1) противоправность деяния; 2) безвозмездность изъятия и (или) обращения чужого имущества в пользу виновного или других лиц; 3) причинение реального ущерба; 3) причинная связь между ущербом и изъятием имущества. Субъективным признаком выступает виновность.

Указанные признаки характерны и для киберкражи, однако особенностью здесь выступает такой признак как тайность хищения, а также способ ее совершения.

Киберкража представляет собой совершенные с корыстной целью противоправные безвозмездные изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества, совершенные путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

Рассмотрим состав кражи, который состоит из объекта преступления, объективной стороны преступления, субъекта преступления и субъективной стороны преступления.

Профессор Е.И. Каиржанов отмечает, что объект уголовно-правовой охраны имеет серьезную роль не только для криминализации (и декриминализации) определенного человеческого деяния (действия или бездействия), для правовой оценки его при квалификации конкретного преступного деяния, для построения системы особенной части Уголовного кодекса, но и для изучения самой преступности в целом, в особенности для изучения и определения причин преступности [7, с.63].

Что понимается под объектом кражи?

Термин «объект» происходит от латинского objectum — предмет, явление, на которое направлена какая-либо деятельность [8, с.349]. Объект уголовного правонарушения – то, на что направлена преступная деятельность.

Общим объектом киберкражи являются имущественные отношения, т.е. общественные отношения, связанные с правом владения, пользования и распоряжения имуществом. Непосредственный объект – общественные отношения, связанные с правом владения, пользования и распоряжения безналичными денежными средствами, находящимися на банковских и иных счетах.

Рассмотрим предмет кражи. В теории уголовного права имеется два подхода к определению предмета уголовного правонарушения.

В.Н. Кудрявцев, таким образом, определяет предмет уголовного правонарушения: «Вещь или процесс, служащие условием (предпосылкой) существования или формой выражения или закрепления конкретного...общественного отношения и подвергающиеся непосредственному воздействию со стороны преступника при посягательстве на это отношение» [9, с.57].

По мнению Н.И. Коржанского, «предмет преступления – это «материальная вещь, в которой проявляются определенные стороны, свойства общественных отношений, путем психического или физического воздействия на которую причиняется социально опасный вред в сфере этих общественных отношений» [10, с.23]. Отсюда следует, что: 1) предмет выступает в качестве физической вещи; 2) предметом могут выступать только те материальные вещи, в которых проявляются определенные стороны или свойства общественных отношений; 3) вред причиняется в сфере общественных отношений, которые выступают либо стороной, либо свойством, исходящим от материальной вещи; 4) вред наступает посредством воздействия (психического или физического) на материальную вещь, то есть предмет преступления.

Нам больше импонирует вторая точка зрения. Однако, полагаем, что в современный период развития информационных технологий, предметом могут выступать и нематериальные вещи.

Что касается точки зрения В.Н. Кудрявцева, то не вполне понятно, что подразумевается под «процессом», ведь процесс предполагает какую-то последовательность явлений (событий) или действий. Если это последовательность действий людей, то данный процесс охватывается понятием «общественные отношения», т.е. «объект преступления». Если это последовательность явлений, событий, не зависящих от воли человека, то как зафиксировать его физическое существование, если он не очерчен определенными рамками, границами, практически невозможно, а поэтому такой процесс не может выступать предметом преступления.

Предметом посягательства при киберкражах являются денежные средства, лежащие на банковских счетах клиентов кредитных организаций или иных платежных систем, криптовалюта (биткоины).

Рассмотрим объективную сторону киберкражи.

Объективная сторона уголовного правонарушения – это совокупность признаков, определяющих преступление с внешней стороны. В.Н. Кудрявцев верно отмечает, что «объективная сторона преступления есть процесс общественно опасного противоправного посягательства на охраняемые законом интересы, рассматриваемый с его внешней стороны, с точки зрения последовательного развития событий и явлений, которые начинаются с преступного действия (бездействия) субъекта и заканчиваются наступлением преступного результата» [11, с.35].

Конкретно киберкража, как форма хищения имущества с объективной стороны, выражается в действиях, представляющих собой тайное хищение имущества (ст. 188 УК РК). Являясь одной из форм преступного поведения, при краже действие представляет собой противоправный акт, состоящий в скрытом от внешних глаз изъятии и перемещении нематериальных объектов (безналичных денежных средств, находящихся на банковских и иных счетах).

К обязательным признакам объективной стороны киберкражи относятся:

а) деяние, которое осуществляется в форме действия – оно представляет собой акт активного общественно опасного и противоправного поведения, а именно – противоправный акт, состоящий в скрытом от внешних глаз изъятии и перемещении безналичных денежных средств, находящихся на банковских и иных счетах, в чужую собственность. Данный акт состоит из ряда последовательных действий, среди которых можно указать:

- незаконное проникновение в источник компьютерной информации, установление вредоносных программ;
- установка посторонних устройств для считывания информации;
- несанкционированное вмешательство в работу банковской системы.
- вредоносный доступ к дистанционному банковскому обслуживанию;
- перевод денежных средств на другой счет, списание денег со счетов;
- снятие денежных средств с карты потерпевшего.

Киберкражи связаны с уменьшением денежных средств на банковских счетах клиентов кредитных организаций или иных платежных систем, что свидетельствует об очевидности преступного деяния. Исключение составляют киберкражи денежных средств в небольших размерах, которые пострадавшими при больших оборотах на их банковских счетах могут быть незамеченными.

Денежные средства со счета пострадавшего переводятся на счета, оформленные, как правило, на чужие похищенные паспорта; перечисление средств осуществляется по «цепочке»

аналогичных счетов; отдельные счета в электронной платежной системе, использованные при хищении денежных средств, достаточно быстро закрываются преступниками. Сам факт перечисления со счета пострадавшего денежных средств всегда предполагает наличие их получателя, в качестве которого выступает фактический владелец счета, на который переведены денежные средства. Отслеживанием цепочки счетов, участвующих в перечислении похищенных денежных средств, данный фактический владелец счета может быть установлен.

б) общественно опасные последствия – хищение безналичных денежных средств у потерпевшего;

в) причинная связь между действием и последствиями – объективная связь между незаконным проникновением в информационную систему либо изменением информации, передаваемой по сетям телекоммуникаций и снятием денежных средств с карты либо со счета потерпевшего.

Из факультативных признаков киберкражи особое значение имеют место и способ совершения уголовного правонарушения.

Особенностью места совершения киберкражи является то, что оно совершается в так называемом киберпространстве или интернет-пространстве. Интернет – всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов (п.44 ст.1 Закона РК «Об информатизации» от 24 ноября 2015 года [12]). Поэтому место происшествия, как правило, удалено от места, где проживает и работает потерпевший, где он хранит свои деньги.

Особенностью киберкражи является то, что она относится к числу преступлений с материальным составом, считающихся оконченными при условии причинения реального ущерба объекту посягательства. Поэтому в некоторых случаях (например, скимминг, шимминг), место преступления может быть не единым: кибервор крадет PIN-код и персональную информацию гражданс одного банкомата, а получает деньги – с другого.

Можно выделить места подготовки киберкраж. К ним относятся обычные жилые и нежилые помещения. Особенностью этой разновидности преступлений является то, что к таким местам можно отнести помещения, в которых располагаются сервера, в том числе в зарубежных странах (иногда используются PROXY-сервера с IP-адресами других государств).

Способ совершения преступления – это совокупность приемов и методов, используемых для совершения преступления. В случае киберкражи отличается спецификой, так как требует наличия определенного уровня компьютерной грамотности и соответствующего технического устройства (компьютера, ноутбука, ЭВМ, мобильного телефона).

Киберкража совершается путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

Информационная система - организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач (п.12 ст.1 Закона РК «Об информатизации») [12].

Сеть телекоммуникаций - совокупность средств телекоммуникаций и линий связи, обеспечивающих передачу сообщений телекоммуникаций, состоящая из коммутационного оборудования (станций, подстанций, концентраторов), линейно-кабельных сооружений (абонентских, соединительных линий и каналов), систем передачи и абонентских устройств (п.55 ст.2 Закона РК «О связи» от 5 июля 2004 года) [13].

Характерными способами киберкраж являются:

- изготовление, распространение и использование вредоносных программ, позволяющих дистанционно подменять платежные распоряжения с компьютерных устройств жертв или управлять операциями выдачи денежных средств из банкоматов;

- дистанционное проникновение в компьютерные системы коммерческих банков и иных организаций, использование сбоев или недостатков в их работе, позволяющих незаконно списывать денежные средства с банковских счетов и т.п.

Обстановка совершения киберкражи, т.е. совокупность условий, которые создали реальную возможность совершения кражи, играет провоцирующую роль, так как ненадлежащая защита информационных систем граждан и юридических лиц, дистанцированность места совершения преступления, т.е. отсутствие возможных свидетелей,

порождает у потенциальных киберворов чувство безнаказанности и толкает на совершение преступления.

Время совершения преступления в случае киберкражи значения не имеет, так как киберкража может осуществляться в любое время суток, месяца, года. Хотя не исключено, что более сложные действия в киберпространстве могут осуществляться ночью, так как в это время в интернете меньше пользователей, скорость передачи высока и действуют льготные тарифы на доступ к платным информационным сетям.

Субъектом киберкражи может быть вменяемое физическое лицо, достигшее ко времени совершения уголовного правонарушения четырнадцатилетнего возраста (ч.2 ст.15 УК РК). Особенностью данного субъекта является то, что он обладает определенным уровнем компьютерной грамотности: могут написать вредоносные программы и другие средства хищений, являются специалистами в области программирования, системного администрирования, владеют специальными навыками и умениями в сфере управления компьютерами и его составными компонентами.

Рассмотрим субъективную сторону киберкражи.

Субъективная сторона преступления – это совокупность признаков, характеризующих психическое отношение субъекта к совершенному им преступному общественно опасному деянию и к его последствиям.

Понятие субъективной стороны уголовного правонарушения неоднозначно трактовалось многими учеными. В теории уголовного права ряд авторов ограничивают субъективную сторону только виной [14, с.41-42; 15, с.6-7]. Другие, включают в нее (субъективную сторону) не только вину, но и мотив, цель [16, с.183], а некоторые дополняют ее и таким признаком, как эмоциональное состояние [17, с.201; 18, с.29].

Как нам представляется, субъективная сторона состава уголовного правонарушения характеризуется тремя признаками: виной, мотивом и целью. Только при наличии этих трех признаков совершенное деяние будет считаться преступлением. Отсутствие любого из них равнозначно отсутствию уголовно-правового основания для привлечения лиц к уголовной ответственности.

Субъективная сторона по п.4 ч.2 ст.188 УК РК характеризуется умышленной формой вины. Мотивом обычно выступает корысть, хулиганские побуждения и т.д. Цель – корыстная (получение материальной выгоды) либо, в редких случаях – «игра на публику», т.е. демонстрация своих интеллектуальных и профессиональных способностей.

Исходя из вышесказанного, можно сделать следующие выводы:

1. Киберкража – совершенные с корыстной целью тайные противоправные безвозмездные изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества, совершенные путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.

2. Непосредственным объектом рассматриваемого преступления являются общественные отношения, связанные с правом владения, пользования и распоряжения безналичными денежными средствами, находящимися на банковских и иных счетах.

3. Предметом посягательства при киберкражах являются денежные средства, лежащие на банковских счетах клиентов кредитных организаций или иных платежных систем, криптовалюта (биткоины).

4. Состав киберкражи по конструкции материальный, поэтому объективную сторону этого деяния образуют: а) общественно опасные действия, которые заключаются в тайном изъятии имущества; б) общественно опасные последствия, которые состоят в причинении потерпевшему материального ущерба; в) причинная связь между ними.

5. С субъективной стороны киберкража представляет собой умышленное деяние, совершенное, как правило, с корыстной целью и из-за корыстных мотивов.

6. Субъектом выступает физическое вменяемое лицо, достигшее 14-летнего возраста, обладающее определенными навыками работы с информационными технологиями.

Список использованных источников:

1. Послание Президента Республики Казахстан Н.Назарбаева народу Казахстана от 31 января 2017 г. «Третья модернизация Казахстана: глобальная конкурентоспособность» .

2. Информационный сервис Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан /http://pravstat.prokuror.kz/rus.

3. Ограбление по-хакерски: 2,2 млрд рублей украли в 2016 году из российских банков / /www.kommersant.ru/doc/3235006.

4. The Economic impact of cybercrime and cyberspionage. Center for Strategic and International Studies July 2013 Report.

5. Доклад Европола - киберпреступность, серьезная угроза для общества в целом // [Электрон. ресурс]. – Доступно из URL: http://www.crime-research.org.

6. Уголовный кодекс РК от 3 июля 2014 года /Информационная система «ПАРАГРАФ».

7. Каиржанов Е.И. К вопросу о методологии познания объекта преступления /Уголовноеправопонимание на современном этапе: методологические аспекты правоприменения. – Алматы: Глобус, 2009.

8. Словарь иностранных слов. – М.: Русский язык, 1989.

9. Кудрявцев В.Н. К вопросу о соотношении объекта и предмета преступления // Советское государство и право. 1958. № 8. С. 57.

10. Коржанский Н.И. Объект и предмет уголовно-правовой охраны. - М.: Юрид. лит., 1980.;

11. Кудрявцев В.Н. Объективная сторона преступления. – М.: Госюриздат, 1960.

12. Закон РК «Об информатизации» от 24 ноября 2015 года /Информационная система «ПАРАГРАФ».

13. Закон Республики Казахстан «О связи» от 5 июля 2004 года /Информационная система «ПАРАГРАФ».

14. Дагель П.С., Котов Д.П. Субъективная сторона преступления. – Воронеж: ВГУ, 1974.

15. Ворошилин Е.В., Кригер Л.Л. Субъективная сторона преступления. – М.: МГУ, 1987.

16. Уголовное право Российской Федерации. Общая часть. – Саратов: СГУ, 1997.

17. Наумов А.В. Уголовное право. Общая часть: Курс лекций. – М.: БЕК, 1996.

18. Иногамова-Хегай Л., Жовнир С. Субъективная сторона лжепредпринимательства // Уголовное право. 2001. № 4. С.29-32.