преступлений против собственности (грабеж, разбой, неправомерное завладение автомобилем или иным транспортным средством без цели хищения, умышленное уничтожение или повреждение имущества).

Понуждение путем использования материальной или иной зависимости жертвы будет только в том случае, когда виновный угрожает совершить те или иные действия в отношении материально, по службе или иным образом зависимого от него лица, которые приведут к ущемлению законных прав и интересов.

Материальная зависимость жертвы от виновного или виновной может быть обусловлена полным или частично иждивением, проживанием на жилплощади виновного или когда от него зависит улучшение или ухудшение материального положения потерпевшего и т.п [4; 165].

В понуждении к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера сексуальная эксплуатация выражается в удовлетворении половой потребности путём полового сношения, мужеложства, лесбиянства или иных действий сексуального характера с применением понуждения.

Исходи из вышеизложенного половые преступления совершаемые с применением насилия следует относит к сексуальной эксплуатации.

Список литературы:

1. Уголовный кодекс Республики Казахстан: Практическое пособие. – Алматы, «Издательство «Норма-К», 2014. – 240 с.

2. Ерохина Л.Д., Буряк М.Ю. Торговля женщинами и детьми в целях сексуальной эксплуатации в социальной и криминологической перспективе. - М., 2003. - С. 201.

3. Рахметов С. М., Мукажанов А.К. Изнасилование (уголовно-правовые и криминологические проблемы)**.** Научно-практическое пособие. - Алматы: ТОО Издательство «Норма-К», 2003.-128 с.

4. Уголовное право Республики Казахстан. Особенная часть: Курс лекций. Кн. 2 /Под общ. ред. И.Ш. Борчашвили. — Алматы, Жет1 жаргы, 2006. — 704 с.

НЕКОТОРЫЕ ПРОБЛЕМНЫЕ ВОПРОСЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РЕСПУБЛИКЕ КАЗАХСТАН

Султанбекова Г.Б., докторант Международного университета Кыргызстана
м.ю.н., старший преподаватель кафедры уголовного процесса и криминалистики
Збинская Е.Ю., магистрант юридического факультета КарГУ им. академика Е.А. Букетова

В связи с модернизацией и развитием информационных технологий преступления, совершаемые в сети интернет – киберпреступления - привлекают особое внимание. Распространение вредоносных программ, кражи номеров кредитных карт и других банковских реквизитов, распространение противоправной информации, пропаганда религиозного экстремизма, финансирование терроризма, отмывание преступных доходов, используя виртуальную валюту, становятся новым мощнейшим инструментом разрушения государственной инфраструктуры.

По причине отсутствия современного технического оснащения правоохранительной системы и экспертных учреждений киберпреступность оказывается вне досягаемости правоохранительных и иных компетентных органов, и напрямую представляет большую угрозу не только отдельным лицам или организациям, но потенциально - национальной безопасности любой страны, достигшей значительного уровня компьютеризации жизненно важных отраслей экономики.

«Согласно рекомендациям экспертов ООН термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети» [1]. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в информационной сфере.

Виртуальная валюта в киберпреступности - это средство выражения стоимости, которым можно торговать, использовать в качестве средства обмена, расчётной денежной единицы, средства хранения стоимости, но не обладающей статусом законного платёжного средства, ни в одной юрисдикции [2; 8]. Виртуальные валюты обладают свойством обмена на реальные деньги,

осуществления трансграничных переводов денежных средств, находящихся вне государственного контроля и учёта. Однако виртуальные валюты значительно снижает потенциал экономического роста государства.

Следует подчеркнуть, что профессиональные компьютерные преступники объектом преступления выбирают локальные сети и серверы крупных компаний, которые являются особо уязвимыми с точки зрения риска анонимности. Из-за отсутствия центрального сервера счета, как правило, не содержат имен или иной информации о клиентах, с помощью которой правоохранительные органы могли бы отслеживать и выявлять схемы подозрительных операций для проведения соответствующих расследований. Жертвами компьютерных мошенников, орудующих в виртуальном мире, могут стать не только граждане, но и целые государства. При этом безопасность тысяч пользователей интернет ресурсами может оказаться в руках нескольких преступников.

«Киберпреступность - это не только спам, вирусы, ботенты и DOS-атаки, это еще и очень много утечек. Существуют криминальные группы, имеющие в своем составе банковских инсайдеров, ворующих информацию о банковских счетах, которую впоследствии их подельники продают в интернете. Для этих групп не существует географических границ. Для борьбы с такими явлениями необходима соответствующая нормативная база» [3].

Первым международным документом, в котором приводится классификация киберпреступлений, является Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 года. К концу 2005 г. Конвенцию о киберпреступности подписали 38 стран-членов Совета Европы, а также США, Канада, Япония и ЮАР. Свое намерение присоединиться к этому международному соглашению выразила и Россия, но впоследствии отказалась присоединяться к Конвенции, так как России не удалось договориться о приемлемых условиях трансграничного доступа к компьютерным системам.

В этом международном документе освещены проблемные вопросы взаимодействия правоохранительных органов при ситуации, когда киберпреступник и его жертва проживают в разных государствах и подчиняются разным законам. В международном соглашении прописаны вопросы хранения личной информации клиентов интернет-провайдеров на случай, если она потребуется при расследовании киберпреступлений. Поскольку Конвенция направлена на усиление борьбы с киберпреступностью, что предполагает тесную кооперацию между правоохранительными структурами различных государств, она наделяет правоохранительные органы государств-участников широкими полномочиями [4; 21].

Во многих странах, в том числе постсоветских республиках (Россия, Молдова, Грузия, Украина, Азербайджан) имеется национальное законодательство о борьбе с киберпреступностью. Так, в России для борьбы с киберпреступностью руководствуются Указом Президента РФ о защите государственной тайны от утечек через Сеть. В Китае в ноябре 2016 года принят новый закон о кибербезопасности, который позволяет замораживать финансовые счета граждан из-за границы. В нашей стране более пяти лет действовал Указ Президента РК «О Концепции информационной безопасности Республики Казахстан» от 10 октября 2006 года №199, который в апреле 2011 года утратил свою силу.

Солидаризируемся с авторами, которые считают, что «настоятельным требованием для Казахстана является выработка национальной доктрины информационной безопасности, которая должна стать базовым концептуальным документом, рассматривающим границы и условия обеспечения информационной свободы и безопасности, служащим задаче преодоления негативных тенденций в информационной сфере современного казахстанского общества»[5; 28].

В последнее время правонарушения, совершаемые в киберпространстве, приобретают большую популярность среди населения, так как покупку товара, оплату каких-либо услуг можно произвести даже с мобильного телефона. В связи с анонимным характером и большим кругом субъектов вовлеченных в совершении операций, обычные граждане, юридические лица непреднамеренно могут быть вовлечены в противоправную деятельность, связанную с легализацией доходов, полученных преступным путем, и финансирование терроризма.

Киберпреступность является сложной, актуальной темой современности, затрагивающей не только область ПОД/ФТ, но также и вопросы защиты потребителей, граждан, общества, налоговое регулирование, а также безопасность сетевых информационных технологий в целом.

Казахстан нельзя отнести к наиболее кибер-криминогенным странам, так как доля преступлений, совершаемых в сфере информационных технологий от количества общеуголовных правонарушений составляет только 5%. Этим преступлениям подвержены такие крупные города

как Астана, Алматы, Караганда, в связи с тем, что здесь сконцентрировано большое количество финансовых и банковских учреждений, учебных заведений, промышленных предприятий и учреждений, с различными формами собственности.

В новом Уголовном кодексе РК от 3 июля 2014 года появилась новая глава «Уголовные правонарушения в сфере информатизации и связи». Обращает на себя внимание то, что наказание за совершение уголовных правонарушений в сфере информатизации и связи незначительное - от 200 до 3000 МРП, так и в части сроков лишения свободы - от 2 до 5 лет.

Для борьбы с киберпреступностью в г.Алматы двенадцать лет тому назад создано оперативное подразделение, получившие название отдел «К». В этом подразделении несут службу высококвалифицированные оперативные работники, использующие IT- технологии. Такие специалисты без особого труда могут выйти на след хакеров. Кроме того, на базе этого подразделения проходят подготовку работники правоохранительных служб.

Полицейские отдела «К» не работают с зарубежными сайтами, их работа ограничивается отечественными сайтами, поэтому результаты их деятельности могут показаться не столь значительными. В 2015 году специалистами отдела «К» было раскрыто 47 уголовных правонарушений в сфере авторских и смежных прав, проведено досудебное производство по 2 фактам реализации порнографической продукции, по 2 фактам распространения средств технической связи, по факту пропаганды культа жестокости и пяти фактам интернет-мошенничества и хищения денежных средств. Незначительное количество раскрытых уголовных правонарушений в сфере компьютерной информации не говорит о том, что такие уголовные правонарушения совершаются редко, в отличие от стран, в которых компании обязаны сообщать об атаках на их IT-инфраструктуру, в нашей республике компании зачастую замалчивают о таких атаках, чтобы не потерять репутацию.

Информационные технологии, оказывающие услуги распространения запрещенной информации, сервис массовых интернет рассылок, отслеживания и хищения денежных средств банков, счетов физических лиц развиваются ускоренными темпами. К тому же, различные системы в цифровом пространстве находятся в юрисдикциях, в которых отсутствуют меры контроля в сфере противодействия отмывания преступных доходов, хищения денежных средств, навязывания им ложной и недостоверной информации. Назрела необходимость государствам принимать превентивные меры в борьбе с надвигающейся угрозой в сфере информационной безопасности. Борьба с такими преступлениями носит трансграничный характер. Поэтому, организация эффективной борьбы с киберпреступностью требует выработки четкого механизма международного сотрудничества

Работники органов прокуратуры нашей республики отмечают, что киберпреступность подрывает устои государства. Приводятся примеры провокационных SMS-атак, касающихся финансового положения ряда банков, которые были направлены на дестабилизацию банковской системы страны. В результате, эти действий был нанесен существенный вред системообразующим банкам, что повлекло рост социальной напряженности в обществе, а также подорвало доверие населения к финансовым институтам страны[6].

Анализ современного состояния информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства… Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [7; 28].

Одной из значимых проблем, связанной с эффективностью расследования киберпреступности является причина недоверия граждан к правоохранительной системе. Так, по результатам опроса, проведенного по государственному заказу Агентства Республики Казахстан по статистике, из 356 тысяч респондентов 12 тысяч (3,5%) заявили, что становились жертвами преступлений, из них только 46% или 1,6% от общего числа опрошенных обращались в правоохранительные органы. Отсюда правовой нигилизм преступников, которые чувствуют себя безнаказанно и потерпевших, которые не хотят обращаться в правоохранительные органы с заявлениями о несанкционированном доступе, потому что понимают, что должного наказания для преступников они все равно не добьются.

Для предупреждения такого рода правонарушений следует отметить важность развития и создания законодательства в рамках сетевой информационной технологии, что в перспективе

позволит, повысить эффективность компетентных органов, укомплектованных надежными специалистами в вопросах борьбы с соответствующими правонарушениями.

В соответствии с ФАТФ (Группа разработки финансовых мер борьбы с отмыванием денег) должны быть определены компетентные ведомства, отвечающие за обеспечение должного расследования в рамках компьютерной сети.

Сегодня в нашей республике осуществляется поэтапный переход к современным методам превентивного воздействия на преступность и расследования уголовных дел, основанным на инновационных технологиях. Вместе с тем, назрела необходимость активного сотрудничества специализированных подразделений по борьбе с киберпреступлениями с различными государственными органами, отвечающими за финансовые расследования, криминалистическую экспертизу, конфискацию доходов, мер по борьбе с отмыванием денег с целью расследования дел, связанных с преступлениями в сети Интернет. Межведомственное сотрудничество правоохранительных органов с зарубежными коллегами в этой сфере будет залогом успеха по противодействию преступлениям, совершаемым с использованием высоких информационных технологий.

В этих целях на первых порах нужно создать спецподразделения подобные отделу «К» во всех областных центрах. Есть необходимость в разработке специального оборудования для проникновения в компьютерную сеть с целью отслеживания правонарушений и предотвращения злоупотребления Интернета в преступных целях.

К организационным мероприятиям можно отнести совместные профилактические мероприятия, направленные на выявление продукции и информации, запрещенной в свободном обороте, пропагандирующей религиозный экстремизм, терроризм, культ жестокости и насилия.

Нужно работать на опережение и уже сегодня разработать законопроекты, касающиеся противодействия киберпреступности, в том числе преступлений, совершенных с использованием виртуальных денег. Нельзя упускать из виду то обстоятельство, что законодательное регулирование киберпространства в одной отдельно взятой стране вряд ли возможно. Однако без государственного контроля компьютерных сетей обойтись нельзя. Подготовка специалистов для спецподразделений становится насущной проблемой. Нужны юристы, специализирующиеся на IT-технологиях.

Список литературы

1. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями.

2. Отчет ФАТФ Виртуальные валюты, ключевые определения и потенциальные риски в сфере ПОД/ФТ. – 2014. – С. 8.

3. http://www.cnews.ru/news/top/putin_otkazalsya_podpisat_konventsiyu

1. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 21.

4. Балановская А.В., Сейткереев В.А. Современное состояние и перспективы развития информационной безопасности Республики Казахстан // Вестник Самарского муниципального института управления. – 2014. - №29. – С.28.

5. Омарханулы Б. О борьбе с киберпреступностью // http://prokuror.gov.kz/rus/novosti/stati/o-borbe-s-kiberprestupnostyu

6. Ахметов Е. Киберпреступность в Казахстане //Законность и правовая статистика. – 2009. - № 11. – С.15.