документов / сост.: Г. А. Метелкина, И. Н. Ширяев ; отв. ред.: К. С. Павлищев, С. А. Шишков. – М : Юрид. лит., 1981. – 288 с.

3. О введении в действие Положения о судоустройстве Р.С.Ф.С.Р. : Постановление ВЦИК от 11 ноября 1922 года // СУ РСФСР. – 1922. – № 69. – Ст. 902.

4. Полное собрание законов Российской империи. Собр. 2-е. – СПб., 1862. – Ст. 35, отд. 1. – С. 710–711.

5. Учреждение судебных установлений // Российское законодательство X–XX веков: Судебная реформа. Т. 8 / отв. ред. В. Б. Виленский. – М., 1991. – С. 52.

6. Устав уголовного судопроизводства // Российское законодательство X–XX веков: Судебная реформа. Т. 8 / Отв. ред. В.Б. Виленский. – М., 1991. – С. 147.

7. Уголовно-процессуальный кодекс Республики Молдова от 14 марта 2003 г. № 122-XV // ИПС «Консультант Плюс».

8. Уголовно-процессуальный кодекс РСФСР от 15 февраля 1923 года. – М., 1923.

9. Фойницкий, И. Я. Курс уголовного судопроизводства / И. Я. Фойницкий. – СПб., 1996. – Т. 2. – 606 с.

Султанбекова Г. Б., Збинская Е. Ю.

ПРОБЛЕМНЫЕ ВОПРОСЫ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЯМИ В РЕСПУБЛИКЕ КАЗАХСТАН

Карагандинский государственный университет имени Е. А. Букетова,
ул. Университетская, 28, 100028 Караганда, Казахстан, *kafprosses@mail.ru*

Стремительное развитие и постоянное расширение Всемирной сети интернет открыло возможности для пользователей информационных ресурсов, а также породило новый вид преступлений – киберпреступления.

Распространение вредоносных программ, кражи номеров кредитных карт и других банковских реквизитов, распространение противоправной информации, пропаганда религиозного экстремизма, финансирование терроризма, отмывание доходов, полученных преступным путем, приводит к разрушению 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. Так, по итогам первой половины 2018 г. 92,9 % от общего количества нарушений составили DDos-атаки.

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 [5, с. 65]. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в информационной сфере.

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. В конце 2017 г. кибератакам подверглись 81 % организаций и физических лиц в Казахстане. Участившиеся кибератаки привлекли пристальное внимание, что привело к небезопасности при проведении операций в интернете.

«Киберпреступность – это не только спам, вирусы, ботенты и DOS-атаки, также 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» [6, с. 8].

Первым международным документом, в котором приводится классификация киберпреступлений, является Конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г. 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, с. 21].

Во многих странах, в том числе постсоветских республиках (Россия, Молдова, Грузия, Украина, Азербайджан) имеется национальное законодательство о борьбе с киберпреступностью. В нашей стране более пяти лет действовал Указ Президента РК «О Концепции информационной

безопасности Республики Казахстан» от 10 октября 2006 г. № 199, который в апреле 2011 г. 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»[3, с. 26].

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 г. 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 г. специалистами отдела «К» было раскрыто 47 уголовных правонарушений в сфере авторских и смежных прав, проведено досудебное производство по двум фактам реализации порнографической продукции, по двум 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.

В настоящее время человечество столкнулось с ростом терроризма. Ключевыми здесь являются вопросы борьбы с финансированием

деструктивных сил и связями с зарубежными террористическими организациями. Необходимо проводить работу по предупреждению пропаганды религиозного экстремизма в Интернете и социальных сетях. 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.

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 этих действий был нанесен существенный вред системообразующим банкам, что повлекло рост социальной напряженности в обществе, а также подорвало доверие населения к финансовым институтам страны [1, с. 17].

Анализ современного состояния информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государств. Необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации [2, с. 15].

Одной из значимых проблем, связанных с эффективностью расследования киберпреступности, является недоверие 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.

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 использования Интернета в преступных целях. В конце 2018 г. в Казахстане заработает система информационной безопасности «Киберщит».

Одним из важных факторов является низкая грамотность населения по вопросам компьютерной безопасности, поэтому нужны курсы повышения грамотности по вопросам кибербезопасности. Недостаточна квалификация сотрудников, расследующих данные преступления. Иными словами, таким сотрудникам необходимы также знания по IT-технологиям. Соответственно, большой процент данных дел прерывается за неустановлением лица. Таким образом, проблематика видится в том, что не могут найти соответствующих лиц. Лица скрываются за границей. Путем удаленного доступа совершают преступления. За последнее время на государственные серверы совершается до 100 тысяч кибератак в день. Необходимо работать на опережение и уже сегодня разработать законопроекты, касающиеся противодействия киберпреступности.

Библиографический список

1. Айвазова, О. В. Междисциплинарный характер категории «способ преступления»: проблема соотношения уголовно-правовых, уголовно-процессуальных и криминалистических аспектов / О. В. Айвазова, С. И. Коновалов // Юристъ-Правоведъ. – 2007. – № 4. – С. 17–22.

2. Багаева, С. А. Участие Казахстана в международной борьбе с терроризмом / С. А. Багаева // Молодой ученый. – 2014. – № 3. – С. 621-624.

3. Балановская, А. В. Современное состояние и перспективы развития информационной безопасности Республики Казахстан / А. В. Балановская, В. А. Сейткереев // Вестник Самарского муниципального института управления. – 2014. – № 29. – С. 17–26.

4. Волеводз, А. Г. Конвенция о киберпреступности: новации правового регулирования / А. Г. Волеводз // Правовые вопросы связи. – М. : Юрист, 2007. – № 2. – С. 17–25.

5. Голик, Ю. В. Преступность – планетарная проблема. К итогам XI Конгресса ООН по предупреждению преступности и уголовному правосудию / Ю. В. Голик, А. И. Коробеев. – М. : Юрид. центр Пресс, 2006. – 280 с.

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