університету. Серія. «Право». – 2014. – Вип. 7. – С. 27–38.

2. Заблоцький В. Взаємодія держави та місцевого самоврядування України в історичній ретроспективі : [монографія] / В. Заблоцький. – Луганськ : ДЗ «ЛНУ ім. Тараса Шевченка», 2013. – 324 с.

3. Сливка С.С. Проблеми філософії права : [навчальний посібник] / С.С. Сливка. – К. : Ліга-Прес, 2014. – 160 с.

4. Тихонов В.Н. Идеи П.Д. Юркевича о государстве и праве в контексте современности : [монография] / В.Н. Тихонов. – Луганск : РИО ЛАВД, 2003. – 303 с.

5. Філософія права : [підручник] / [О.Г. Данильян, О.П. Дзьобань, С.І. Максимов та ін.] ; за ред. О.Г. Данильяна. – Х. : Право, 2009. – 208 с.

6. Альчук М. Філософсько-правовий дискурс: історія і сучасність / М. Альчук [Електронний ресурс]. – Режим доступу : http://old.filos.lnu.edu.ua/bulletin_philosophy/ ua/docs/visnyk03/articles/01.pdf.

7. Чередніченко Г.О. Взаємообґрунтування моралі та права у філософії П.Д. Юркевича : автореф. дис. … канд. філософ. наук : спец. 09.00.05 «Трудове право; право соціального забезпечення» / Г.О. Чередніченко ; Київ. нац. ун-т ім. Т. Шевченка. – К., 2007. – 16 с.

8. Юркевич П. Історія філософії права. Конспект лекцій ординарного професора П.Д. Юркевича. Москва, 1868 р. Переклад з рос. / П. Юркевич // Юркевич П. Історія філософії права. Філософія права. Філософський щоденник / П. Юркевич. – К. : Редакція журналу «Український світ», 1999. – С. 14–230.

9. Юркевич П. Філософія права. Детальний конспект лекцій ординарного професора П.Д. Юркевича. Москва, 1872 р. Переклад з рос. / П. Юркевич // Юркевич П. Історія філософії права. Філософія права. Філософський щоденник / П. Юркевич. – К. : Редакція журналу «Український світ», 1999. – С. 528–566.

10. Юркевич П. Філософія права. Конспект лекцій ординарного професора П.Д.Юркевича. Москва, 1873 р. Перекл. з рос. / П. Юркевич // Юркевич П. Історія філософії права. Філософія права. Філософський щоденник / П. Юркевич. – К. : Редакція журналу «Український світ», 1999. – С. 568–685.

ВЗАИМОДЕЙСТВИЕ СЕТИ ИНТЕРНЕТ И ПРЕСТУПНОСТИ: КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ

Мария МОКРЯК,
аспирант кафедры криминологии и уголовно-исполнительного права
Национального университета «Одесская юридическая академия»

Summary

The article deals with the possibility of using the Internet and modern communication technologies of the representatives of the criminal world, including organized criminal networks; outlined the concept of the cyber crime. We investigate preventive power of the Internet, as well as the role of the Internet in enhancing the effectiveness of the state and in the fight against corruption.

Key words: mass media, online media, cyber crime, preventive action on the Internet.

Аннотация

В статье рассмотрены возможности по использованию технологий коммуникаций современного образца, а также Интернет-ресурсов представителями организованных преступных сообществ и криминального мира. Помимо этого, освещены следующие тезисы:

– киберпреступность;

– использование Интернет-технологий как средства борьбы с негативными общественными явлениями;

– использование Интернета как средства по борьбе с преступностью;

– Интернет как средство повышения эффективности борьбы с коррупцией со стороны государства.

Ключевые слова: средства массовой информации, Интернет-СМИ, киберпреступность, превентивное действие сети Интернет.

Постановка проблемы. Средства массовой информации, Интернет особенно, достаточно сильно влияют на формирование ценностных ориентиров и модель должного поведения. Важное различие между Интернетом и другими СМИ – то, что Интернет является интерактивным. Люди, которые получают доступ к Интернету, в большинстве своем могут отличаться от тех, кто больше смотрит телевидение или видео. Как уточняют исследователи, большую часть тех, кто получает доступ к Интернету, составляют люди 18–24 лет, и это группа с высоким количеством самоубийств, по крайней мере, в промышленно развитых странах.

Изолированные и отчужденные в социальном отношении люди могут быть в состоянии начать значимые отношения с Интернет-контактами, несмотря на то что не встречали их лицом к лицу. Следовательно, есть потенциальная опасность влияния Интернета на преступное поведение более непосредственно, чем это происходит с печатными СМИ, телевидением и видео.

Актуальность темы исследования подтверждается степенью развития сети Интернет, совершенствования законодательства и необходимостью комплексного теоретического исследования в криминологическом аспекте.

Целью статьи является исследование сети Интернет, преступности и их взаимного влияния.

Вопросы взаимодействия сети Интернет и преступности в работах рассматривали такие ученые, как В.А. Голубев, Ю.И. Гололобова, Н.В. Карчевский, В.А. Номоконов, А.Л. Осипенко, В.О. Чернышева.

В качестве методологической основы исследования использованы диалектический, догматический (формально-логический), системный, социологический, историко-правовой, сравнительно-правовой и другие методы научного познания.

Изложение основного материала исследования. В условиях современного мира, где насильственная преступность поднялась на радикально новый уровень, который по сей день остается высоким, есть все основания полагать, что исследования методов борьбы с преступностью не имеют должного уровня и динамики.

Интернет-ресурс, который является в наши дни обширным, на деле нельзя

называть структурированным. Его образуют различные сети и источники, совершенно разрозненные по методам финансирования, требованиям, условиям. Решением технических вопросов, связанных с управлением Интернетом, занимаются международные общественные организации [4].

Internet Society (ISOC) регулирует слаженную работу Интернета как единого механизма и спонсируется за счет взносов всех добровольных участников. Если же возникает какой-то вопрос, связанный с введением новых систем и стандартов, участие принимают специализированные технические комитеты. Один из таких, под названием Inter NIC, осуществляет контроль над справочными службами, именами доменов и сетевыми адресами.

Другие технические комитеты, число которых достаточно велико, в основном оформляют и разрабатывают стандарты взаимодействия сетевых систем. Они выполняют поддержание базы данных по организациям, которые занимаются сетевой деятельностью, и распределение между ними адресов, а также разрабатывают стандарты. Это является основным критерием того, что каждая Интернет-сеть обладает своим уставом и внутренними правилами. Но стоит отметить, что данные правила обязательны к исполнению лишь для клиентов этой сети. И именно из-за различий в правилах, а также источниках финансирования возникают противоречия, которые в итоге усложняют решение правовых вопросов. Отсутствие официальных списков сетевых адресов и их пользователей также является серьезной проблемой. К усложнению правоохранительной деятельности в сети также приводит географическая разрозненность сетевых информационных центров и методов их распределения.

Сетевые преступления, так или иначе, обладают общими характеристиками. Ниже перечислены признаки, которые присущи преступлениям данного вида:

1. Общая цель (объединение единой целью преступления нанесения вреда общественно опасными средствами).

2. Опасность для общества.

3. Общая открытость (изменения порядка проведения преступления в целях адаптации к окружающим условиям).

4. Самодетерминация (развитие преступности за счет использования преступниками методов пропаганды криминальной психологии или внушения).

5. Устойчивость.

6. Способность организовывать внутреннюю систему самозащиты, а также защиты от общества и активность.

Между тем отдельные свойства сетевых преступлений приобретают особое значение с точки зрения организации борьбы с ними. К таковым стоит отнести латентность, трансграничный характер, наличие элементов преступного профессионализма и организованности [4].

Важным свойством сетевых компьютерных преступлений является их общая латентность. Масштабы таких преступлений очень сложно определить, особенно если сравнивать их с иными преступлениями.

Латентная составляющая преступности объединяет преступления, о которых не было известно правоохранительным органам (скрытая часть), и преступления, известные правоохранительным органам, но которых не было в статистической отчетности (скрываемая часть) [9].

Серьезную проблему для правоохранительных органов также создает и транснациональный характер большинства преступлений, которые совершаются в сети и характер которых связан с рассмотренной спецификой функционирования современных глобальных компьютерных сетей [7].

Под подобными исследованиями специалисты понимают преступления, совершаемые на территории и за пределами определенного государства, которые связаны с нарушением охраняемых международным и государственным законодательством интересов двух или более стран. К подобным признакам таких преступлений относятся «пересечение государственных границ и выход последствий преступной деятельности за пределы одной страны». Часть преступлений, называемых сетевыми, вполне удовлетворяет названному определению [4].

Термин «трансграничные», который используется для обозначений примеров, когда нарушение происходит без пересечения виновным границ государства, обозначает также и «прозрачность» государственных границ для сетей.

Неблагоприятная нравственная и психологическая атмосфера основной части общества в Украине создана во многом средствами массовыми коммуникациями. Эти источники оказывают огромное влияние на осознание последствий стихийных бедствий, обстоятельств взрывов или убийств.

Такие компоненты создают определенный уровень личностной агрессивности. В него входят следующие факторы:

– раздражительность;

– подозрительность;

– агрессия;

– чувство вины;

– обида;

– способность сопереживать чувствам других.

Способность адекватно объединить эти факторы позволяет оценить характер и масштаб влияния телевидения и Интернет-сетей на совершение насильственных действий. Интернет-сети обладают поразительными свойствами: как средства передачи информации на расстояние они стали диктаторами многих социальных норм. Им отводится задача формирования четко определенных мнений, позиций, установок. Часто это используется в политике для формирования необходимого общественного мнения [8, с. 201].

Интернет-сети перед другими средствами массовой информации выделяются тем, что могут поддерживать двустороннюю связь с пользователями, а также в Интернет-сетях доступно общение в режиме реального времени. Иными словами, Интернет можно назвать аспектом, формирующим современную культуру. Он становится популярным во всех сферах общества, так как является наиболее гибким и приспосабливаемым к аудитории, особенно в сравнении с другими средствами коммуникаций. В то же время гораздо более зависим от аудитории и дорожит ее вниманием, поэтому любые попытки обмана могут привести к оттоку посетителей, а значит, к краху конкретного Интернет-проекта [6].

С другой стороны, Интернет наводнен большим количеством информации, которая попадает туда из-за того, что подобные сети гораздо меньше ско-

ванны рамками цензуры, в отличие от других СМИ.

Интернет-общение отличается и тем, что каждый потребитель может примерить на себя любую роль. Даже ту, которая невозможна для него в реальной жизни. Исследования показывают, что большинство форумов, а также крупных чатов имеют свою постоянную аудиторию, объединенную общими интересами. То, что при этом расстояние не играет никакой роли, а само общение на форумах не предполагает личного знакомства, снимает многие психологические барьеры в общении. Иными словами, дает неограниченную возможность практически в любом самовыражении. При всем при этом любой пользователь может остаться анонимным. Но, так как идентификация должна быть в любой сети и в любой системе, пользователю предоставляется право выбора имени и виртуального образа, который соответствует его взглядам, мировоззрению и психологическому типу. Выбранный образ воспринимается как данность, тогда как остальные прекрасно осведомлены о возможном несоответствии сконструированного виртуального образа реальному лицу, создавшему его [8, с. 72].

Такая анонимность порождает безнаказанность в сети Интернет. Не исключены такие варианты поведения, как размещение в сети Интернет информации оскорбительного характера либо информации, порочащей честь и достоинство, а также деловую репутацию различных лиц. Негативный социальный эффект также может дать размещение в Интернет материалов, нежелательных для их просмотра и восприятия определенными категориями пользователей (например, информация эротического или порнографического характера, нежелательная для просмотра детьми).

Основу сетевой компьютерной преступности образует система сетевых преступлений, в которую в основном попадают умышленные, тщательно спланированные деяния, имеющие ряд характерных особенностей, к наиболее значимым из которых нами отнесены следующие:

1. Дистанция (это характер преступных действий, при которых отсутствует прямой контакт преступника и жертвы).

2. Скрытность (анонимность и возможность примерить на себя любую роль в сети обеспечивают определенную специфику сетевого пространства).

3. Территориальность (объект преступлений и жертва могут находиться в разных государствах).

4. Интеллектуальность (высокая подготовленность преступника и его навыки, которые необходимы для совершения преступлений в сети) [8, с. 401].

5. Объект преступления (объектом преступления могут выступать компьютерные системы, сетевые узлы, Интернет-провайдер).

6. Нестандартность (высокая сложность каждого сетевого преступления, которая обеспечивает постоянное обновление способов его совершения, а также применяемых противоправных действий, направленных на устранение общественной опасности).

7. Автоматизированность (возможность совершения преступления путем объединения нескольких слабых компьютерных ресурсов в один мощный сервер, например, с целью хищения денежных средств).

8. Отсутствие фактических свидетелей (отсутствие свидетелей преступления как лиц, наблюдавших событие преступления и способных опознать преступника) [6].

Поскольку криминальная среда в сетевом пространстве способна стать «полигоном» для отработки новых наиболее эффективных в современных условиях форм преступных организаций, стоит более подробно остановиться на особенностях возникающих в ней преступных групп. Можно отметить, что в настоящее время преимущественное распространение получили хакерские группы, участники которых не ведут совместной преступной деятельности, а имеют опосредованные связи: главным образом обмениваются опытом и специальным программным обеспечением, оказывают друг другу моральную поддержку [9].

Для осуществления преступной деятельности наблюдается тенденция объединения преступников, которые всё чаще становятся преступными группировками со сложной структурой, имеющей, ко всему прочему, связи в нескольких разных государствах. Растет не только их общая организованность, но и численность лиц, которые занимаются различной преступной деятельностью в сети.

Выявление подобных группировок имеет очень большое значение. Знание принципов построения таких организаций и особенностей их структур помогает выявить мотивы преступлений. Следует отметить, что среди них практически отсутствуют группы, создающиеся на длительное время, для которых характерны устойчивость, сплоченность, основанная на организационно-иерархических связях.

Анонимность предполагает, что лицо, совершившее преступление, может находиться в любой точке мира, и при всем при этом, задача усложняется еще и тем, что Интернет-пространство предполагает возможность устранения любых следов преступной деятельности и любого шлейфа информации, оставленного преступником. Поэтому всё большее число пользователей могут стать жертвами правонарушений. Остро стоит проблема незаконного копирования и разглашения интеллектуальной информации, которая является личной собственностью.

Вычислить убийцу без каких-либо зацепок довольно сложно. А если это убийство замаскировано еще и под суицид, то раскрыть преступление становится невыполнимой задачей для полиции.

На это и надеялся житель Запорожья, который под разными аккаунтами общался с девушками, пребывающими в депрессии. Киберманьяк добавлялся в друзья в качестве Интернет-подруги к будущей жертве. После завязывалась переписка, которая зачастую заканчивалась похоронами. Самое удивительное то, что убийца даже не встречался со своими жертвами. Находясь за сотни километров от них, он, сидя за компьютером, ждал сообщения о смерти пользователя.

Киберпреступность, что растет с каждым годом, – это незаконное действие, которое осуществляется преступниками, использующими для своих целей различные информационные технологии. Есть несколько основных видов киберпреступности:

– кража кредитных карт;

– кража реквизитов;

– взлом аккаунтов;

– распространение вирусов и вредоносных программ;

– распространение клеветы и других материалов;

– нелегальные Интернет-аукционы, которые организуются с целью вымогательства денег за счет искусственного поднятия ставок на несуществующий товар.

Количество подобных преступлений за 2015 год превысило показатель 2014 года в шесть раз (данные по Украине).

Чаще всего Интернет-мошенники стараются завладеть данными платежных карт клиентов. Это могут быть звонки гражданам якобы от сотрудников банков, где они обслуживаются, с целью получить пароли и данные по карточке. Также нередки случаи, когда данные карточки считывают при помощи специальных устройств. Для этого злоумышленники вступают в сговор с работниками заправок и маленьких магазинов, где можно незаметно для клиента использовать считывающее устройство, а пароль узнать при помощи камер видеонаблюдения [9].

Еще одним распространенным способом мошенничества является создание поддельных сайтов известных Интернет-магазинов в основном бытовой техники, одежды. Для этого создается точная копия известного сайта с заниженными ценами, после чего злоумышленники на протяжении некоторого времени принимают платежи от клиентов, а потом сайт исчезает [8].

Создаются целые группы, участники которых делят обязанности и этапы преступления: некоторые участники отвечают за получение средств на карты, некоторые создают сайты, а кто-то обналичивает украденные деньги. Применение Интернет-технологий может повлиять и на профилактику преступлений, если правильно и перспективно распределять ресурсы.

Сайты правоохранительных органов могут иметь совершенно разный объем информации – от одной до ста страниц. Всё зависит от частоты использования, а также от того, с какой целью сайт используется: как инструмент для связи с общественностью или самостоятельная структура, которая уже, в свою очередь, содержит гиперссылки и ссылки, другие электронные ресурсы.

Так, например, украинский сайт wanted.mvs.gov.ua дает возможность бесплатно получить информацию относительно установления местонахождения безвести пропавших людей, лиц, утративших память; розыска людей, скрывающихся от органов власти; поиска похищенных культурных ценностей; поиска похищенных мобильных телефонов, транспортных средств, находящихся в розыске, оружия в розыске.

Особую роль может сыграть Интернет в борьбе с коррупцией, так как один из ее основных источников – закрытость, непрозрачность процесса принятия решений властными структурами. Так, например, в марте 2016 года Верховная Рада Украины приняла изменения в Закон Украины «О предотвращении коррупции», которым вводится электронное декларирование доходов чиновников. Сайт Национального агентства по предотвращению коррупции открыл доступ к интерфейсу электронного декларирования.

Выводы. В завершение стоит отметить, что связанные с развитием сети Интернет трансформации преступности не только порождают необходимость совершенствования законодательства, изменения организации и тактики борьбы с преступностью, но и требуют новых подходов к комплексному теоретическому осмыслению соответствующих криминологических проблем. Интернет как один из видов средств массовой информации может нести как негативное, так и положительное влияние на уровень преступности.

На общем фоне всего происходящего: социальных преобразований и реформ, изменения методов деятельности органов правоохранения – особенная роль отводится исследованиям по криминологии. Подобные исследования должны будут привести к формированию радикально новых методов по борьбе с киберпреступностью и обеспечению постоянной правоохранительной практики, а также научных и обоснованных рекомендаций.

Список использованной литературы:

1. Конституція України від 28 червня 1996 року № 254к/96ВР / Верховна Рада України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/w/254%D0%BA/96%D0%B2%D1%80.

2. Кримінальний кодекс України від 5 квітня 2001 року № 2341III / Верховна Рада України [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/234114.

3. Кримінальний кодекс України. Науково-практичний коментар : у 2 т. / за ред. В.Я. Тація, В.І. Борисова та ін. – 5-е вид., допов. – Х. : Право, 2013. – Т. 2 : Особлива частина / [Ю.В. Баулін, В.І. Борисов, В.І. Тютюгін та ін.]. – 2013. – 1040 с.

4. Голубев В.А. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью / В.А. Голубев [Электронный ресурс]. – Режим доступа : http://www.crime-research.ru/articles/2004/.

5. Гололобова Ю.И. Средства массовой информации и преступность: Криминологический аспект : автореф. дисс. … канд. юрид. наук : спец. 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» / Ю.И. Гололобов. – М., 2002. – 48 с.

6. Карчевский Н.В. Компьютерные преступления: определение, объект и предмет / Н.В. Карчевский [Электронный ресурс]. – Режим доступа : http://www.ifap.ru/pi/05/karchev.htm.

7. Номоконов В.А. Организованная преступность: транснациональные признаки / В.А. Номоконов [Электронный ресурс]. – Режим доступа : http://www.crime-research.ru/library/Nomokon2.html.

8. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы : [монография] / А.Л. Осипенко. – Омск : Изд-во Омск. акад. МВД России, 2009. – 480 с.

9. Чернышова В.О. СМИ, Интернет и преступность (криминологические аспекты) / В.О. Чернышова [Электронный ресурс]. – Режим доступа : ndki.narod.ru/liblary/articles/komp_prest/Chernyshova_VO-komp_prest1.doc.