УДК 316.42

КАРПОВА Дарья Николаевна –
научный сотрудник Московского государственного института международных отношений (университет) МИД РФ
119454, г. Москва, пр-кт Вернадского, 76
d.n.karpova@yandex.ru

КИБЕРПРЕСТУПНОСТЬ: ГЛОБАЛЬНАЯ ПРОБЛЕМА И ЕЕ РЕШЕНИЕ

CYBERCRIME: A GLOBAL CHALLENGE AND ITS SOLUTION

Статья посвящена анализу такого глобального социального явления, как киберпреступность. Предложена методология его изучения, в которой выделены и классифицированы цели, объекты воздействия, способы и средства совершения преступлений в виртуальной среде. Проведен вторичный анализ данных социологических исследований по выявлению уровня «цифровой компетентности» и ответственности людей при использовании Интернета. Автор отмечает, что для эффективного противодействия виртуальным угрозам необходима многоуровневая система кибербезопасности, способная защитить как граждан, так и государственные институты. В статье также определена роль социологии как науки, способной предложить конкретные решения проблем борьбы с киберпреступностью.
Ключевые слова: *киберпреступление, фишинг, онтологическая безопасность, кибербезопасность*

The article analyzes the global problem of cybercrime committed through the Internet. The author proposes methodology of studying this phenomenon, for instance, who is the object of cybercriminals, which goals do they pursue while committing their actions. The author represents the secondary data of the scientific sociological research to illustrate the level of the digital competence and Internet responsibility of Russian Internet users. The author also defines the role of sociological knowledge capable of suggesting specific solutions of the problem of cybercrime.
Keywords: *cybercrime, phishing, ontological security, cybersecurity*

Период «поздней современности», о которой в 1991 г. писал Энтони Гидденс, характеризуется наличием перманентных случайностей и рисков – неизменных спутников системы, стремящейся к установлению господства над природой и рефлексивному творению истории [Giddens 1991: 109]. В дигитализированном обществе начала XXI в. сфера проявления риска меняется. Источником угроз и опасностей становится глобальная киберпреступность. По данным международной службы по обеспечению безопасности в области киберугроз *Symantec Security*, каждую секунду в мире подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд долл. США. Глобальная природа киберпреступности проявляется и в ее транснациональном характере: готовится и совершается киберпреступление в одной стране, а урон наносится другой. Так, в списке стран с высоким уровнем совершаемых преступлений в виртуальной среде Россия занимает 1-е место и одновременно относится к группе самых незащищенных от киберугроз государств. Вследствие этого преступления в виртуальном пространстве, или киберпреступления, становятся особой сферой внимания экспертов в области национальной безопасности, а профилактика и предупреждение киберпреступлений артикулируются в средствах массовой информации, государственных документах и научных работах.

Для предупреждения киберпреступлений необходимо осмыслить данное явление. Начнем с определения понятия. Киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба индивиду, организации или государству посредством любого технического средства с доступом в Интернет.

Киберпреступления различаются по своим целям, объектам воздействия, способам и средствам совершения противоправного действия. Охарактеризуем киберпреступления в соответствии с выделенными основаниями.

1. Цели. Киберпреступления чаще совершаются ради экономических целей. Это может быть, например, нанесение экономического ущерба в виде воровства денежных средств и конфиденциальной информации. К другим видам целей относятся политические – нанесение ущерба основным государственным и политическим институтам, подрывающее систему властных отношений и доверия к власти. Третий вид целей – идеологические: распространение идей и идеологий с целью вербовки интернет-пользователей в ряды, например, радикальных террористических и националистических группировок. Наконец, к четвертому виду целей мы относим социально-психологические, такие как нанесение морального, психологического вреда гражданам.

2. Объекты воздействия. Действия киберпреступников могут быть направлены на простых граждан, организации, государственные институты, их личную информацию, свободу и персональную кибербезопасность.

3. Способы и средства воздействия. Пока еще сложно систематизировать и описать все существующие средства, которыми оперируют киберпреступники. Вчерашний метод «выуживания» информации устаревает в течение короткого периода, т.к. кибермошенники используют модифицированные технологичные средства для совершения киберпреступлений. Из общеизвестных способов совершения киберпреступлений можно выделить два типа: социальную инженерию (не путать с социальной инженерией в социологии) и вирусные программы. Отличительной особенностью первого типа является телефонная или компьютерная атака на человека с целью получения личной информации. Прибегая к особенностям психологии личности, мошенники выдают себя за другое лицо, вводя тем самым человека в заблуждение. Социальная инженерия используется узким кругом специалистов в области информационной безопасности для описания способов «выуживания» личной информации, основанных на знании особенностей психологии человека, с применением шантажа, злоупотреблением доверием. Этот психологический способ получения личной информации широко использовался обычными мошенниками в 1990-х гг., однако обезличенный контакт с жертвой посредством Интернета дает большую свободу кибермошенникам. Самым распространенным видом социальной инженерии является мошеннический фишинг (от англ. *fishing* – ловля рыбы и *phone* – телефон), или «выуживание» у неграмотных пользователей Интернета их конфиденциальных данных.

Специфика второго типа киберпреступлений – вирусных программ – заключается в том, что они позволяют киберпреступникам удаленно управлять компьютерами без ведома их пользователей, применяя «продвинутое» современное программное обеспечение. Их называют ботами, а сеть компьютеров, зараженных вредоносным кодом, – ботнетами. Надо отметить, что большая часть обычных пользователей остаются беззащитными перед лицом этих опасностей и не в состоянии противостоять профессиональным действиям киберпреступников. Это объясняется двумя основными факторами. Во-первых, простые люди не обладают достаточным уровнем компьютерной грамотности для своей защиты. Во-вторых, традиционно у нас слабо развиты установки на обеспечение собственной безопасности. Можно предположить, что проблема кроется в

дефиците личной онтологической безопасности, которая имеет социокультурную природу, характерную для россиян в целом. Понятие «онтологическая безопасность» (*ontological security*), введенное Э. Гидденсом, обозначает «субъективное ощущение безопасности, основанное на конфиденциальности или доверии» [Giddens 1991: 35]. Анонимность как главный атрибут виртуальной реальности действительно располагает к кажущимся на первый взгляд доверию и защищенности по отношению к остальным коммуникантам. Этими субъективными представлениями о личной кибербезопасности и пользуются виртуальные преступники в своих целях. Для обеспечения защиты от возможных преступлений в виртуальном пространстве необходимо обладать информацией о сформированных установках граждан по данному вопросу, понять, осознают ли потенциальные жертвы угрозы возможной кибератаки, к каким мерам безопасности они прибегают, чтобы сохранить свои личные данные.

Проведенные в данной области социологические исследования иллюстрируют вышесказанное и выявляют, что далеко не все пользователи российского Интернета (далее – Рунет) готовы защитить себя в киберпространстве и знают, как это осуществить. Одна из попыток изучить «цифровую компетентность» пользователей была предпринята в совместном исследовании факультета психологии МГУ им. М.В. Ломоносова и Фонда развития Интернет в рамках проекта «Дети России онлайн» [Цифровая компетентность... 2013: 59]. В 2013 г. исследователи провели опрос 1 203 подростков (как наиболее уязвимой группы пользователей Интернета) в возрасте от 12 до 17 лет и их родителей, проживающих в 58 городах России. К компонентам цифровой компетентности ученые отнесли: знания, умения, мотивацию и ответственность при пользовании Интернетом. Исследователи пришли к выводам, что важным фактором, увеличивающим вероятность столкновения с онлайн-рисками, является несоблюдение простых правил безопасности: распространение излишней информации о себе при общении с незнакомцами, несоблюдение правил хранения паролей. Подростки зачастую недооценивают негативные последствия, к которым может привести их «фривольное» интернет-поведение: скачивание музыки, фильмов, онлайн-игры, социальные сети. Они отсрочивают во времени возможные негативные последствия свободного пользования Интернетом, которые могут проявиться позже, скажем, при приеме на работу. Исследователи считают, что необходимо учить молодежь правилам безопасного поведения в Интернете и объяснять возможные риски свободного поведения в сети. Хотя родители считают, что в школе детей должны информировать об интернет-угрозах, а также учить их эффективно пользоваться современными инфокоммуникационными технологиями, все же уровень интернет-ответственности самих родителей весьма невысокий. В этой ситуации остро встает вопрос, должен ли сам человек защищать себя и свою личную информацию или же обеспечение сохранности данных как страны, так и своих граждан – это ответственность государства?

Для эффективного противодействия виртуальным преступникам необходима многоуровневая институциональная система кибербезопасности, которая защищала бы и простых граждан, и государственные институты. Система кибербезопасности включает в себя многообразные компоненты, в т.ч. повышение уровня цифровой грамотности населения, содействие в продвижении индивидуальных способов защиты личной информации, механизмы по противодействию и профилактике киберугроз.

Первые попытки создания таких систем кибербезопасности предприняты в США и странах Европейского союза. Так, система американской кибербезопасности основана на Акте о запрете интернет-пиратства (*Stop Online Piracy Act*). Согласно данному законопроекту уголовно наказуемым преступлением считается распространение или вещание запрещенного авторским правом контента с наказанием в виде тюремного заключения и

штрафа. Любой участник деятельности в Интернете, начиная с провайдеров, поисковых систем и рекламодателей, обязан по любому обращению правообладателя прекратить предоставление услуг ресурсу, обвиняемому в пиратстве, и прекратить с ним любое взаимодействие.

Система кибербезопасности ЕС строится на инициативе «Европа 2020». ЕС определил собственную Цифровую повестку дня (*Digital Agenda*) с обязательством выполнения широкого круга задач. Первая группа задач ориентирована на дальнейшую популяризацию Интернета. Так, в ЕС планируется к 2015 г. увеличить число пользователей Интернета с 60% до 75%, а среди инвалидов – с 41% до 60% соответственно; обучить бóльшую часть населения ЕС пользоваться услугами электронного правительства, и производить оплату покупок онлайн и др. Вторая группа задач, обязательства по которым взяла на себя Еврокомиссия, сводится к обеспечению кибербезопасности своих граждан. На базе ЕС было создано Агентство по сетям и информационной безопасности (*ENISA*), которое постоянно проводит мониторинг мнений пользователей сети, в соответствии с этим вносит поправки в уже принятые проекты, которые становятся законом и соблюдаются странами ЕС. Наверное, самое нужное во всей этой инициативе – то, что законодатели проводят ежегодные встречи с политиками, *IT*-специалистами, учеными для обучения и совершенствования навыков безопасного пользования Интернетом, приучаясь тем самым к виртуальной культуре.

Россия наряду с зарубежными странами включилась в международное сотрудничество по борьбе с киберпреступностью. В частности, она выступает за разработку международной стратегии по противодействию киберугрозам и создание единых международно-правовых механизмов регулирования виртуального пространства. Одним из таких механизмов является Конвенция о киберпреступности, которая была открыта для подписания в рамках Совета Европы в 2001 г. Согласно Конвенции, к киберпреступлениям относятся: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с детской порнографией и нарушением авторского права; мошенничество с использованием компьютерных технологий и др. В 2007 г. была открыта для подписания Конвенция СЕ о защите детей от эксплуатации и посягательств сексуального характера.

Стремление государства защитить своих граждан проявляется также в разработке проекта Концепции Стратегии кибербезопасности Российской Федерации, текст которого размещен на официальном сайте Совета Федерации. Авторы проекта определяют кибербезопасность как совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. 29 ноября 2013 г. в Совете Федерации состоялись парламентские слушания, посвященные обсуждению данного проекта. Документ базируется на принципах и законах других государственных документов: Стратегии развития информационного общества[1], а также Доктрине информационного общества Российской Федерации[2]. Целью Стратегии кибербезопасности является обеспечение виртуальной безопасности личности, организации и государства путем определения системы приоритетов, принципов и мер в области внутренней и внешней политики. Стратегия базируется на таких основных принципах, как гарантированность конституционных прав и свобод человека и гражданина в области получения информации; максимальная защищенность личности, организаций, в т.ч. обеспечивающих функционирование государственных органов в киберпространстве; сотрудничество всех субъектов информационного общества – личности, орга-

[1] Стратегия развития информационного общества. Утв. приказом Президента РФ № Пр-212 от 07.02.2008.

[2] Доктрина информационного общества Российской Федерации. Утв. приказом Президента РФ № Пр-1895 от 09.09.2000.

низаций и государства – в области обеспечения кибербезопасности; соблюдение баланса между установлением ответственности за несоблюдение требований кибербезопасности, с одной стороны, и введением избыточных ограничений – с другой; приоритетность рисков кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий от инцидентов кибербезопасности; актуализация средств и методов обеспечения кибербезопасности в целях противостояния изменяющимся киберугрозам.

К сожалению, принятие проекта Концепции Стратегии кибербезопасности приостановлено, хотя на официальном сайте Совета Федерации все еще продолжается обсуждение текста документа. Рост числа совершаемых киберпреступлений не позволяет свести на нет дискурс данной проблемы, о чем свидетельствуют неоднократные правительственные встречи и инициативы. Например, в России в 2014 г. при поддержке Торгово-промышленной палаты РФ состоялся первый международный форум по кибербезопасности «*Cyber Security Forum 2014*», ключевой темой которого стал обмен опытом и выявление лучших практик в сфере информационной безопасности. Следует также отметить, что по инициативе Уполномоченного по правам ребенка П. Астахова начала действовать Всероссийская информационная кампания против насилия и жестокости в СМИ и Интернете, включающая комплекс мер по обеспечению информационной безопасности детей.

Таким образом, отмечаем, что киберпреступность и кибербезопасность – две амбивалентности единого глобального виртуального пространства. Всего десятилетие назад проблема информационной безопасности осознавалась преимущественно узким кругом специалистов в области информационных технологий. Вместе с точными инженерно-техническими и физико-математическими специальностями к поиску эффективных решений подключились социальные науки, например киберсоциология [Кравченко 2013: 498]. Появилась новая парадигма информационной безопасности – парадигма кибербезопасности. Налицо все признаки ее институционализации: формируются правовые нормы в борьбе с кибермошенниками, появляются международные институты по кибербезопасности, развиваются новые сферы деятельности, ориентированные на противодействие киберпреступникам, и.т.д. Тем не менее отмечаем, что для борьбы с киберпреступностью необходим дальнейший системный анализ, в т.ч. с привлечением социальных наук.

Литература

Кравченко С.А. 2013. *Социологический толковый русско-английский словарь*. М.: МГИМО(У), 914 с.

Цифровая компетентность подростков и родителей (под ред. Г.У. Солдатовой, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова). 2013. М.: Фонд развития Интернет, 144 с.

Giddens A. 1991. *Modernity and Self-Identity. Self and Society in the Late Modern Age*. Stanford University Press, 257 p.