УДК 004.77,004.85
Doi: 10.17223/16095944/70/8

А.Х. Шелепаева

Пермский военный институт войск национальной гвардии, г. Пермь, Россия

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

Приводятся результаты анализа статистических данных, рассматривающих вопросы расширения разнообразия противоправных действий в сети Интернет с использованием сетевых сущностей, активно наращиваемых для продвижения бренда и / или информационных услуг. На сегодняшний день не хватает методик и средств анализа основных трендов развития киберпреступлений, соответственно мы отстаем в подготовке специалистов, способных противостоять нарастающей глобальной угрозе. На основе анализа данных сделан вывод, что решение данной проблемы необходимо вести не только в правовом поле, возникают и сопутствующие социальные проблемы, требующие исследований специалистами различных сфер для эффективной адаптации в виртуальной среде подрастающего поколения. Также представлен анализ новых трендов в сфере киберпреступности по результатам Центра интернет-технологий и обосновывается необходимость исследования способов защиты от новых схем преступной деятельности в сети для их изучения курсантами высших учебных заведений.

Ключевые слова: информационные технологии, сервисы Интернет, киберпреступность, виртуальная среда, типы сетевых атак, сетевые сущности.

Интернет за свой недолгий период развития стал не только средой, расширяющей возможности взаимодействия в различных сферах деятельности, но и вполне состоявшимся социально-криминогенным пространством. Если раньше киберпреступления связывали с деятельностью хакеров, интересы которых касались в основном финансовых сфер, то на сегодняшний день угрозам подвергаются все – от правительств до обычных граждан. По данным региональной общественной организации «Центр интернет-технологий» (РОЦИТ), осуществляется постоянный рост видов и способов кибератак и у современных типов киберпреступлений; очень высока латентность, т.е. способность скрывать за определенными действиями свои явные намерения, что требует внешнего регулирования процессов взаимодействия различных структур и субъектов для решения возникающих при этом правовых и социальных проблем.

По результатам анализа PandaLabs за 1-й квартал 2017 г., преступления в киберпространстве становятся более изощренными, меняются векторы и количество атак. Усложняется ИТ-окружение, когда автоматизируются разные технологические процессы с различными устройствами, системами и средствами подключений. При этом мы отстаем не только в разработке защитных средств, но и медленно реагируем при разработке учебных программ для обучения курсантов в сфере ИТ, что является колоссальной проблемой, так как мы должны двигаться не вслед, а опережать их развитие, а для этого необходимо понять, с чем мы имеем дело. Для решения социальных проблем необходимо привлечение образовательной сферы, чтобы молодежь была способна адекватно реагировать и на стихийно возникающие тренды воздействия на формируемую психику. Не зря говорят, что современные революции – это итог воздействия социальных сетей, когда любые явные и неявные виды недовольства могут использовать для деструктивных действий, манипулируя дистанционно, с использованием подставных аккаунтов.

Существуют разные подходы к пониманию понятия «киберпреступность», расширенного в современных реалиях до термина «кибертерроризм». Изначально использовалось понятие «компьютерное преступление», которое включало в себя преступную деятельность с использованием информационных коммуникационных технологий. Если рассмотреть современные подходы к пониманию киберпреступности, то они не сильно расширяют содержание понятия. Киберпреступность – это:

– «совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей» (Тропина, 2005);

– «общественно опасные деяния, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете» (Рассолов, 2008).

Многообразие форм проявления киберпреступности не позволяет дать сколь угодно приемлемое определение данного понятия. И можно пока ограничиться лишь описанием различных сторон ее реализации. В «Перспективном анализе тенденций киберпреступлений с 2011 по 2020 г.» авторы выделяют основные аспекты проявления:

– криминальный (связывание преступлений в реальном и виртуальном мире);

– технологический (расширение за счет мобильных устройств, телефонии, средств видеонаблюдения и т.д.);

– антропологический (неадекватное поведение в сети различных социальных групп, связанных с неправильным обучением и отсутствием способов адаптации к новым ресурсам взаимодействия);

– стратегический (разрушение инфраструктуры или обеспечивающих средств сети).

Уже на заре развития сети различали три типа киберпреступлений, когда компьютер выступал как предмет, орудие или интеллектуальное средство преступления (Батурин, Жодзишский, 1991). Речь идет о создании вредоносных программ, взломе паролей, краже номеров кредитных карт и т.д. и действиях, связанных с ущемлением чести и достоинства, с использованием различных сайтов. Каждое из данных направлений требует отдельного рассмотрения, но рост разнообразия предлагаемых сервисных услуг Интернет повышает и множество вариантов киберпреступлений. По словам В.А. Номоконова, киберпреступление может рассматриваться как правовая категория и как социальное явление, которое выполняет «поддерживающую функцию» [1].

Необходимость принятия решений на законодательном уровне важна, и чаще всего речь идет об ужесточении уголовной ответственности за создание вредоносных программ, организацию DDOS-атак, мошенничество с электронными деньгами (Чекунова, 2011) [2]. Д.Н. Карпова предлагает многоуровневую институциональную систему кибербезопасности, начиная с повышения уровня цифровой грамотности до создания механизмов по противодействию угроз. Важный вывод, который делает данный автор: необходимо привлечение социальных наук для исследования данной проблемы [3]. То есть возникает необходимость исследования не только правовой составляющей данной проблематики, но и социальной, чтобы исключить эффект манипулирования сознанием молодежи через различные интернет-ресурсы.

На сегодняшний день объектами правового регулирования в сети Интернет являются ситуации, связанные с потерей и / или порчей данных, приводящих к финансовым потерям или экономическому ущербу заинтересованных сторон. В 2014 г. в России было зафиксировано примерно 11 тыс. преступлений в сфере телекоммуникаций и компьютерной информации, а уже в 2015 г. данная цифра была достигнута уже в сентябре, причем речь идет лишь об официально зарегистрированных цифрах. На конец 2017 г. в сети в течение года появилось порядка 90 млн новых вирусов, а у 40 % российских компаний нет стратегии информационной безопасности. Развитие мобильных платформ становится благодатной сферой для кражи персональных данных и использования их против физических лиц, которые не обеспечены необходимыми средствами защиты, так как основные усилия развития информационной безопасности направлены для защиты банковской сферы.

По данным РОЦИТ, в 2015 г. было зарегистрировано жалоб со стороны граждан:

– 35 % – на проблемы с интернет-магазинами;

– 24 % – на качество услуг связи;

– 17% – на взлом аккаунтов и кражу паролей;

– 12% – на кражу персональных данных в сети.

В 2017 г. проводились исследования по анализу угроз, связанных с социальными сетями и их влиянием на подростков. В опросе участвовало 2 500 человек, три возрастные группы (13–17 лет, 18–30 и их родители). В ходе исследования были выделены такие угрозы:

– Агрессивное онлайн-поведение, которое выражается в формате агрессивных сообщений (44 %), груминга* (48 %), угрозы физической расправы (23 %).

* Тактический подход взрослого человека к несовершеннолетнему, как правило, с сексуальными намерениями.

– Кибербуллинг (травля с помощью мобильных телефонов), флейминг (словесная перепалка), хейтинг (травля с использованием сетевых ресурсов) и т.д.

На основании уже новых исследований появилась новая классификация интернет-рисков [4]:

– контентные – использование вредоносной информации;

– коммуникационные – межличностные отношения;

– потребительские – злоупотребление правами потребителей;

– технические – хищение конфиденциальной информации;

– интернет-зависимость – тяга к чрезмерному использованию Интернета.

Как видим, в качестве явных угроз рассматриваются и исследуются вопросы, связанные с экономическими угрозами и потерей персональных данных не только в юридической, но и иной трактовке. Начинают понимать необходимость исследования социальных эффектов в сетевых сообществах. Исследования не касаются возможных трендов развития мошеннических схем в зависимости от развития сервисных служб сети Интернет и при принятии инновационных решений. Это и обусловливает необходимость исследования одного из направлений, рассматриваемой в данной статье, создания виртуальных сущностей, которые на сегодняшний день не несут явной угрозы, но при этом имеют колоссальные потенциальные возможности для реализации негативных последствий.

На проходившей конференции «Соединяя домены» («CONNECTing the Dots», март 2015 г.) был принят документ, в котором не только подчеркивается важность сети Интернет для развития человечества, но и подтверждается концепция универсальности Интернета, что, свою очередь, предполагает открытость, доступность и демократичность сети, рассматриваемая в контексте равноправия всех участников сетевого взаимодействия. Не подвергая сомнению выводы экспертов, нам бы хотелось заострить внимание на тех аспектах развития сетевого сообщества, которые могут прямо или косвенно повлиять на информационную безопасность страны.

Развитие сети Интернет в первую очередь связывают с концепцией свободы слова, что выражается в следующих документах:

– «Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» (ст. 19 Всеобщей декларации прав человека (ООН, 1948 г.)).

– «Свобода выражения – это свобода высказывать идеи, которые могут быть крайне непопулярны, не опасаясь репрессий, и право на защиту тех, кто выражает такие идеи» (интернет-манифест ИФЛА (Международная федерация библиотечных ассоциаций и учреждений, 2005)).

Между рассмотренными документами практически шестьдесят лет, но авторы интернет-манифеста ссылаются на 19-ю статью, что не является, на наш взгляд, вполне уместным. Возможность выражения своих взглядов в публичных местах ограничивалась территориально и в пределах узких социальных кругов, не влияющих на происходящие социальные процессы вне этих кругов взаимодействия. Сегодня же технологии активно влияют и на политические, и на финансовые, и на социальные процессы, затрагивая интересы всех слоев населения. Существующая практика показывает, что чаще возникают негативные тенденции влияния, нежели позитивные, что и влечет за собой возникновение предложений на ограждение молодого поколения от влияния сети.

Характерными вызовами современного общества являются формальные характеристики развития информационного общества:

– информация становится стратегическим ресурсом (обмен данными);

– происходит трансформация коммуникативных моделей (межличностное взаимодействие);

– инновации рассматриваются как результат взаимодействия формализованного и неформализованного знания (социальное взаимодействие).

Рассматриваемые характеристики информационного общества можно описать как в разрезе протекания информационных процессов, так и в разрезе коммуникационных процессов. В современном мире мы не просто обмениваемся данными, мы обмениваемся смыслами. Информация становится средством манипулирования в опосредованной медиасреде, в которой участвуют не только живые люди. Интернет вслед за теле-

видением теряет свои первоначальные функции как информационно-коммуникационной среды. За этими медиасредствами закрепилась экспрессивная роль, когда оценивается уровень произведенного эффекта, т.е. через эмоциональную сферу навязываются стандарты поведения, вкуса, приоритетов и т.д.

За последние годы в сети сформировалась новая социальная среда, именно социальная, а не просто технологическая или техническая, которая уже имеет собственные не только стихийно сформированные закономерности существования, но и, вполне вероятно, четко регулируемые процессы, направленные на решение конкретных задач определенных социальных кругов. В сети искусственно формируются сущности, которые, на первый взгляд, решают чисто маркетинговые задачи, такие как повышение положительного имиджа, повышение рейтинга, востребованности бренда, товара или услуг, политического веса и т.д. Безобидные на первый взгляд явления могут существенно повлиять на формирование и развитие сетевого сообщества, фактически становясь виртуальными агентами влияния.

«Свобода выражения» или расширенное понятие в связи с развитием сети Интернет «свобода информации», рассматриваемая как «право доступа к данным, находящимся в распоряжении публичных властей, и право получать регулярную информацию об инициативах, предпринимаемых публичными властями», могут интерпретироваться по-разному. Соответственно любые шаги по регулированию процессов распространения и представления данных в медийной сфере и социальных сетях могут рассматриваться как попытка лишения основных свобод граждан. Стихийно формируемая среда предполагает наличие определенных механизмов регулирования, которые первоначально надо обозначить, задать рамки, внутри которых и возможны регулятивные процессы.

Переход от простого обмена данными к социальному взаимодействию приводит к возникновению «сетевого сообщества», по мнению М. Кастельса, – специфической виртуальной структуры, пронизывающей все слои общества и не являющейся материальным объектом [5]. Данное замечание очень важно в рамках данного исследования, ибо описание интернет-сообществ (Жарова, 2011) или «сетевых социальных агрегатов» (Несторов, 1998) включает лишь сетевое представление реальных сущностей (сообществ, субъектов взаимодействия и т.д.) [6]. Ситуация усложнилась ввиду формирования и развития сущностей, которых нет в природе, но существующих в сети и вполне адаптировавшихся в этой среде.

Сетевые сущности, или искусственные личности, могут называться по-разному: боты, зомби, трансляторы и т.д. Но суть их одна – имитация сетевой активности. При анализе сетевой аудитории политические деятели отображают, на первый взгляд, количество сторонников тех или иных взглядов, но на самом деле реальные действия подписчиков не сопоставимы с их численностью. В качестве реальных действий могут рассматриваться лайки, комментарии, репосты и клики. Можно выделить активных пользователей, постоянно участвующих в различных формах взаимодействия, тех, кто участвовал только на начальном этапе, и сущности, не осуществляющие после подписки вообще ничего. Искусственное наращивание «популярности» в сети за счет «цифровых личностей» формирует среду для создания и развития новых видов киберпреступлений, которые направлены против личности и государства. Соответственно необходимо дать правовую оценку данному явлению, формировать правовую базу и начать обучать курсантов отслеживать тенденции развития данного направления.

Проблема идентификации личности сети способствовала созданию виртуальной сети, так называемой ботнет, являющейся компьютерной сетью с совокупностью зараженных хостов, когда пользователь может и не знать, что его компьютер входит в эту сеть. Если первоначально такой ресурс использовали для рассылки спама, продвижения товара или осуществления DDoS-атак, то сейчас уже активно используют боты для участия в голосовании. Пользователь может и не знать, что его аккаунт активно используется для продвижения услуг, рекламы, отражения «его гражданской позиции» и т.д. В социальных сетях уже реализован механизм, который отслеживает пользователей, не посещающих свои страницы, и от их лица рассылаются сообщения с просьбой пополнить счет. Такие действия могут осуществлять сотрудники, обеспечивающие техническую и программную реализацию. Обезопасить себя в такой ситуации каждый пользователь может

только сам, но предварительно его нужно научить отслеживать подобные угрозы.

Другая проблема – это манипулирование сознанием людей. Еще в 2010 г. И.Р. Бегишев писал о новых средствах ведения информационной войны, что Интернет становится «совершенно новым мощным инструментом манипуляции восприятием» [7]. Обладая даже неполной информацией о пользователе, можно с использованием средств интеллектуального анализа спрогнозировать те или иные действия со стороны пользователя и направить потенциал людей в деструктивном направлении. Чтобы не быть голословным, рассмотрим основные разработки хакерского подразделения JTRIG британских спецслужб:

– BOMB BAY – автоматическая раскрутка сайта;

– SLIPSTREAM – увеличение количества просмотров заданных страниц;

– UNDERPASS – утилита для «участия» в онлайн-голосованиях;

– BADGER – массовая рассылка е-мейлов для «поддержки информационных операций»;

– PITBULL – массовая рассылка сообщений пользователям социальных сетей;

– SKYSCRAPER – изготовление и массовое распространение видеоматериалов для «поддержки информационных операций»;

– BUMPERCAR+ – автоматическая система блокирования видео с помощью жалоб видеохостингу (возможность устранения видео с другим содержанием) и т.д.

И это лишь малая часть их разработок. На первый взгляд, данные разработки абсолютно невинные, например, что плохого в автоматической раскрутке сайта? Многие маркетологи этим пользуются. Давайте проанализируем. Современные пользователи ищут необходимые материалы через поисковые системы и всегда просматривают не ниже 10-й позиции результатов поиска. Можно автоматизировать процесс таким образом, чтобы «нужный сайт» нашел своего читателя даже при использовании нерелевантного запроса. В подобных ситуациях возникает иллюзия, что действия человека в сети автономны и выбор всегда за пользователем. На самом деле любое действие фиксируется, сохраняется в базе и выбор уже сделан, но не пользователем, а системой по заданному извне алгоритму.

С 2010 г. в социальных сетях стали появляться люди, активно добавляющиеся в «друзья». На тот момент поражало, что они все были жителями Украины. Самое удивительное, что добавлялись люди соответствующего возраста и пола, молодые – к молодым, а пожилые – к пожилым. Три года они ничего не делали вообще, даже фотографии не выкладывали. Февральские события 2014 г. никак не повлияли на их активность, но с апреля массово стали рассылать сообщения и ссылки на ресурсы антироссийского толка. Вполне вероятно, что делается все уже в автоматическом режиме, за четыре года легализация сетевых личностей уже произошла.

Все сказанное выше не отражено ни в каких учебных планах и программах. В учебные программы по информатике, информационным технологиям необходимо включать вопросы кибербезопасности, а также вопросы социальной адаптации в сети. Данная проблематика затрагивает интересы не только курсантов военных учреждений, необходимо уже в школьном возрасте учить правильно себя вести в сети.

Подведем итог. Созданная виртуальная среда уже живет по своим правилам и начинает активно воздействовать на подрастающее поколение. Для успешной адаптации в среде необходимо постоянное присутствие и взаимодействие с разными социальными группами, чтобы понимать и осознавать, с кем ты взаимодействуешь – с человеком или с «сетевой сущностью». В социальных сетях уже в ленте пользователя появляются не только материалы, которые дублируют «друзья», но и ресурсы, формирующие определенный эмоциональный фон, которые могут привести к негативным последствиям. И при отработанных уже средствах манипулирования сознанием происходит потеря ориентации, когда человек уже не в состоянии понять, чьи смыслы он транслирует, свои или чужие, навязанные извне. Коммуникация в сетевой среде должна быть организована и регламентирована в рамках учебного процесса, чтобы курсанты могли качественно адаптироваться в виртуальной среде и уметь выявлять негативные тенденции развития новой сферы влияния.

ЛИТЕРАТУРА

1. *Номоконов В.А., Тропина Т.Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1. – С. 45–55.

2. *Чекунов И.Г.* Киберпреступность: проблемы и пути их решения // Вестник Академии права и управления. – 2011. – № 25. – С. 97–10.

3. *Карпова Д.Н.* Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 8. – С. 46–50.

4. *Киберугрозы*, кибератрессия, кибербуллинг: различия в восприятии, оценке и поведении у разных групп населения Российской Федерации [Электронный ресурс]. – URL: http://raec.ru/activity/analytics/9880/ (дата обращения: 17.02.2018).

5. *Кастельс М.* Становление общества сетевых структур // Новая постиндустриальная волна на Западе. Антология / под ред. В.Л. Иноземцева. – М., 1999. – С. 494–505.

6. *Нестеров В.* К вопросу о динамике сетевых сообществ [Электронный ресурс]. – URL: http://sbiblio.com/biblio/archive/nesterov_at_question/ (дата обращения: 16.12.2015).

7. *Бегишев И.Р.* Информационное оружие как средство совершения преступлений // Информационное право. – 2010. – № 4. – С. 23–25.

Shelepaeva A.K.
Perm military Institute of national guard troops of the Russian Federation, Perm, Russia

TRENDS IN THE DEVELOPMENT OF CYBER CRIME IN THE INTERNET

Keywords: Information technology, Internet services, cybercrime, virtual environment, network attacks types, network entities.

This article discusses the results of the analysis of the statistical data that contains the issues of expanding the diversity of illegal actions in the Internet with using network entities actively increasing for brand promotion and / or information services. Nowadays, the existing methods and tools for the analysis of main trends of cybercrime development are not enough, and accordingly, we are lagging behind in training specialists who are able to withstand the increasing global threat. On the basis of data analysis, it was concluded that the solution of this problem must be conducted not only in the legal field, but in the social sphere that requires specialists in various fields for effective adaptation of young generation in virtual environment. Moreover, the paper presents an analysis of new trends in the field of cybercrime and the necessity of research of the ways to protect from new schemes of criminal activity in the network in order to study cadets of higher educational institutions.

The paper presents some interesting facts concerning current negative trends of the Internet development and the problems of social adaptation. The main idea is that any changes in the technological sphere are reflected in the social environment. The further developments of the Internet have created new cyber-threats. Cybercrime involves not only the financial sphere but also the legal, social and other aspects of human life. However, more acute problems are the phenomena as aggressive online behavior, cyber bullying, flaming, hater, and etc. The network is the place of manipulation of growing generation consciousness through web-entities.

The author expresses the viewpoint about negative trends in the development of the Network deserving particular attention. There is the need of changing the current curriculum adding computer science subject concerning issues of cyber security and social adaptation in network. It must be studied not only by cadets in military academies, but also by pupils in schools in order to teach them how to behave in the Internet.

In social network the newsfeed displays the material not only given by “friends”, but also the resources of negative content which can form the emotional background that could lead to negative consequences. The author emphasizes the ideas that the communication in the network environment should be organized and regulated in accordance with education, so that the students can adapt to the virtual environment and identify the negative trends in this new sphere.

REFERENCES

1. *Nomokonov V.A., Tropina T.L.* Kiberprestupnost’ kak novaja kriminal’naja ugroza // Kriminologija: vchera, segodnja, zavtra. – 2012. – № 1. – S. 45–55.

2. *Chekunov I.G.* Kiberprestupnost’: problemy i puti ih reshenija // Vestnik Akademii prava i upravlenija. – 2011. – № 25. – S. 97–10.

3. *Karpova D.N.* Kiberprestupnost’: global’naja problema i ee reshenie // Vlast’. – 2014. – № 8. – S. 46–50.

4. *Kiberugrozy*, kiberagressija, kiberbulling: razlichija v vosprijatii, ocenke i povede-nii u raznyh grupp naselenija Rossijskoj Federacii [Jelektronnyj resurs]. – URL: http://raec.ru/activity/analytics/9880/ (data obrashhenija: 17.02.2018).

5. *Kastel’s M.* Stanovlenie obshhestva setevyh struktur // Novaja postindustrial’naja volna na Zapade. Antologija / pod red. V.L. Inozemceva. – M., 1999. – S. 494–505.

6. *Nesterov V.* K voprosu o dinamike setevyh soobshhestv [Jelektronnyj resurs]. – URL: http://sbiblio.com/biblio/archive/nesterov_at_question/ (data obrashhenija: 16.12.2015).

7. *Begishev I.R.* Informacionnoe oruzhie kak sredstvo sovershenija prestuplenij // Informacionnoe pravo. – 2010. – № 4. – S. 23–25.