УДК 347.77
ББК 67.408.135

А.Н. Косенков
Юридическая академия Украины имени Ярослава Мудрого
Г.А. Черный,
кандидат юридических наук, доцент
Юридическая академия Украины имени Ярослава Мудрого

ОБЩАЯ ХАРАКТЕРИСТИКА ПСИХОЛОГИИ КИБЕРПРЕСТУПНИКА

В статье рассматриваются основные направления психологического изучения киберпреступности, необходимые для борьбы с данным видом преступлений. На основе особенностей киберпространства сформулированы главные криминогенные психологические факторы киберпространства, а также механизмы их влияния на формирование преступного умысла и поведения преступников. Продемонстрирована взаимосвязь между социальными, правовыми, нормативными проблемами киберпространства и психологией киберпреступлений. Даны основные классификации типов личности киберпреступника в зависимости от различных психологических факторов, их характеристика. В общих чертах рассмотрены особенности психологии хакеров (крэкеров). В целом, сделан вывод о киберсоциуме как о достаточно криминогенной среде, а также существенных особенностях психологии киберпреступников. Имеется обзор основных работ зарубежных и российских ученых, подтверждающих мнение авторов. С теоретической точки зрения статья освещает проблему девиантного поведения в киберсоциуме. Результаты работы имеют практическое значение для создания стратегии по борьбе с киберпреступностью, расследования киберпреступлений и построения процессуальных действий.

Ключевые слова: киберпреступность; психология киберпреступности; компьютерные преступления; информационные преступления; борьба с киберпреступностью.

A.N. Kosenkov
National Law Academy of Ukraine named after Yaroslav the Wise
G.A. Cherniy,
Ph.D. in Law, Ass. Professor
National Law Academy of Ukraine named after Yaroslav the Wise

GENERAL CHARACTERISTIC OF A CYBERCRIMINAL'S PERSONALITY

The paper analyzes key areas of psychological research of cybercrimes, which are necessary for fighting these crimes. Specific characteristics of cyberspace allow the authors to define key criminogenic psychological factors of cyberspace as well as the mechanisms of their impact on the criminal intention and the behavior of criminals. The authors show the interconnection between social, legal, normative problems of cyberspace and the psychology of cybercrimes. They present basic classifications of cybercriminals' personality types, which depend on different psychological factors and their characteristics. The authors also give a general overview of hackers' (crackers') psychology. In general, the authors conclude that cyber-socium is a rather criminogenic environment and present essential characteristics of cybercriminals' personalities. The paper contains an overview of basic works of Russian and foreign researchers that support the authors' opinion. From the theoretical viewpoint the paper highlights the issue of deviant behavior in cyber-socium. The results of this research have practical value for designing the strategy of fighting cybercrimes, for their investigation and organization of legal proceedings.

Key words: cybercrimes; psychology of cybercrimes; computer crimes; information crimes; fighting cybercrimes.

В современном мире с каждым годом все более серьезной угрозой для общества становится киберпреступность. Особо актуальной борьба с киберпреступностью остается для стран СНГ, в которых показатели использования информационных технологий еще не достигли уровня западных государств и в дальнейшем компьютерные преступления могут стать серьезным препятствием для создания надежной информационной инфраструктуры. Безусловным приоритетом в борьбе с данным видом преступлений является усовершенствование технической защиты информации, однако данное направление не освещает субъективную сторону правонарушения, изучение ко-

торой является основой для профилактики преступлений.

Целью статьи является изучение основ психологии киберпреступников, на базе которых возможна разработка стратегии противодействия киберпреступности, оценка соответствия уголовного законодательства психологии преступника, разработка тактики ведения процессуальной деятельности.

Применение юридической психологии в расследовании киберпреступлений важно по целому ряду причин: отсутствие достаточного количества материальных следов преступника, широкое разнообразие возможных мотивов некоторых категорий киберпреступлений, порой неограниченный круг лиц, имевших возможность совершить преступление, а также потенциально большой вред, который может нанести киберпреступление. Кроме того, знание основ психологии киберпреступников поможет при разработке средств противодействия им, поскольку злоумышленники достаточно часто используют психологические приемы в своей деятельности.

Необходимость подробного изучения киберпреступлений также вызвана чрезвычайно большим количеством преступлений, охватываемых понятием «киберпреступление». Хотя сегодня до сих пор понятие «киберпреступление» толкуют как в узком смысле – преступления, ответственность за которые предусмотрена соответствующим разделом уголовного кодекса (гл. 28 УК РФ «Преступления в сфере компьютерной информации»), так и в широком – любые преступления, совершенные с помощью электронных устройств.

Для исследования психологии преступников наиболее подходит широкое толкование термина «киберпреступление», что соответствует и рекомендациям экспертов ООН. При использовании данного определения следует, тем не менее, проводить дифференциацию всех киберпреступлений на специальные, ответственность за которые предусмотрена статьями гл. 28 УК РФ, и общие, ответственность за которые предусмотрена другими нормами УК РФ.

С учетом своеобразности киберпреступлений, для общей психологической характеристики лиц, их совершающих, необходимо изучение по трем основным направлениям:

– общие особенности среды совершения киберпреступлений, которые влияют на психологию киберпреступников;

– основы психологии отдельных категорий киберпреступников;

– виктимологические особенности совершения этих преступлений.

Ввиду ограниченности возможности для изложения, в данной статье будут рассмотрены только два первых направления.

Основной особенностью киберпреступлений является среда их совершения – образованное электронным устройством и их сетями киберпространство (или виртуальное пространство). В условиях киберпространства существенно меняется психологическое содержание взаимосвязей *преступник – предмет преступления*, а также *преступник – потерпевший*, которые из прямых превращаются в опосредованные: *преступник – электронное устройство (Сеть) – потерпевший (предмет преступления)*, что ведет к устранению материальной составляющей как действий человека, так и социального взаимодействия. При этом «виртуальные» предметы психологически кажутся более доступными, в том числе для незаконного завладения ими.

Подтверждением менее ответственного отношения к нематериальным, нежели к материальным предметам является широко распространенное нарушение авторских прав. Согласно предварительным результатам опроса «Культура копирования в США и Германии», проведенного по заказу Американской ассамблеи, около 46% взрослых жителей США покупали, копировали или загружали с нарушением авторских прав музыку, ТВ- программы или фильмы, в то время как 70% людей в возрасте 18–29 лет получали пиратские аудио- или видеофайлы [8, с. 2]. Любые же действия в таких условиях воспринимаются изначально как нематериальные по природе, соответственно, не несущие материальных, «серьезных» последствий. По справедливому замечанию директора Центра безопасного и ответственного использования Интернета Нэнси Виллард (Nancy Willard), «информационно-коммуникационные технологии существенно ограничивают обратную связь, любое чувство осязаемой обратной связи наших действий. Поэтому отсутствует влияние осознания того, что мы причинили вред, но также мы считаем, что наше поведение не может причинить никакого вреда, потому что мы не видим вреда» [3, с. 23].

Как показали DDOS-атаки на сайты государственных органов Украины, произошедшие после закрытия файлообменного серви-

са ex.ua (где находился «пиратский» контент) и к совершению которых были причастны обыкновенные пользователи, «пиратство» имеет прямую взаимосвязь с более серьезными видами киберпреступлений и способствует распространению киберпреступности в целом.

Существенным криминогенным фактором психологического характера, присущим киберпространству, является возможность сохранения полной анонимности пользователя устройства или Сети (за исключением технической информации о подключении к Сети, способы сокрытия которой также существуют). Анонимность позволяет не только не быть идентифицированным в определенный момент времени, но также, как следствие, предоставлять о себе ложную информацию, вступать в социальное взаимодействие, представляясь другим лицом. Очевидно, что в условиях анонимности любой человек ощущает возможность безнаказанно совершать поступки отрицательного характера, при этом отсутствие эффективных механизмов порицания только усиливает желание совершать негативные действия, особенно, если первопричина таких действий лежит в реальном мире.

В то же время подобное ощущение безнаказанности влияет не только на отдельных лиц, но и создает атмосферу вседозволенности, которая способствует дальнейшему распространению и развитию общественноопасных идей. Так, после терактов в Норвегии было установлено, что Андреас Брейвик был активным посетителем различных праворадикальных интернет-ресурсов [9]. Адвокат Брейвика заявил, что его подзащитный поддавался влиянию со стороны других интернет-пользователей ультраправых взглядов, в частности, со стороны блогера под ником «Fjordman», личность которого была установлена только после терактов [11]. Для преодоления возможных негативных последствий анонимности в некоторых городах Китая было введено требование по обязательному использованию реальных данных при регистрации в сервисах микроблогов [7]. Чуть ранее власти Шанхая ввели обязательное использование реальных данных на сайтах знакомств, обосновывая это тем, что «...интернет-анонимность открывает дверь для киберпреступлений, в частности мошенничества...» [13]

Именно анонимность делает киберпространство «параллельным» нашей обычной жизни и позволяет создавать новый образ собственной личности или сразу несколько образов, отличающихся от реального и не отягощенных психологической обязанностью следовать реальному образу, как это было бы в случае идентификации пользователя. Особенно ярко это выражено в онлайн-играх, где анонимность сопряжена с вымышленным миром. Поэтому весьма вероятно, что у киберпреступников могут встречаться психические отклонения, которые фиксируют у обыкновенных пользователей Интернета: интернет-зависимость, тревожные расстройства, диссоциативные расстройства личности.

Можно предположить, что на количество преступлений отрицательно может влиять рост потенциальных и действующих факторов социального взаимодействия, скорость протекания связей и возможность установления одновременно нескольких связей. Благодаря перечисленным факторам в киберпространстве, даже в большей степени чем в реальном мире, возможно возникновение перегрузки социальными контактами, бывает «утрата способности и возможности сосредотачивать внимание на конкретном человеке» [4], что ведет не столько к озлоблению и агрессии, как в реальном мире, сколько к «обесцениванию» каждого из контактов на фоне «триумфа» собственного «Я», обеспеченного субъективным (если даже не солиптическим) восприятием киберпространства. При этом, как обоснованно считает С.В. Бондаренко, «в среде с интенсивными обменами и информационными потоками существует проблема информационного переполнения, при котором снижается острота восприятия акторами фактов девиантного поведения» [1].

Также в киберпространстве существуют идеальные условия и для сокрытия преступной деятельности за счет таких факторов как: 1) «самодостаточность» киберпространства как социальной системы — наличие в киберпространстве экономических, культурных и других социальных институтов, которые дают возможность человеку почти полноценно существовать не отходя от компьютера, предоставляя злоумышленникам возможность «маневрировать», сбывать незаконно приобретенную собственность, что, безусловно, играет не последнюю роль в формировании преступного умысла; 2) идеальная среда для «социального раздвоения, как социальной игры, связанной со сменой ролей

и декораций» [2, с. 399], в которой перевоплощение не требует изменения собственного внешнего вида или серьезных психологических затрат как в случае с обыкновенной преступной деятельностью, что позволяет киберпреступникам успешно играть роль законопослушных граждан.

Значительное место занимают психологические процессы, протекающие при непосредственном совершении киберпреступления. В отличие от подавляющего большинства обыкновенных преступлений, совершение киберпреступления не требует, как правило, каких-либо передвижений или принятия каких-либо активных физических действий. Киберпреступник при реализации своего злого умысла находится дома, в компьютерном клубе, месте с бесплатным доступом в Интернет, любом другом выбранном им месте, которое для него является комфортным или, по крайней мере, знакомым и привычным. Поэтому киберпреступники могут не ощущать, или ощущать в значительно меньшей степени, дискомфорт, страх быть случайно обнаруженным и задержанным. Хотя киберпространство и является многогранным социальным пространством, в то же время оно остается искусственно созданной программно-аппаратной средой, деятельность в которой все-таки ограничена техническими рамками, что делает предсказуемыми последствия действий. Это, в свою очередь, позволяет злоумышленнику не ощущать неопределенности ситуации, планировать свои действия даже при неблагоприятных для него обстоятельствах, а значит, чувствовать себя более уверенно и спокойно во время совершения преступления.

Как отмечалось ранее, киберпреступники не имеют возможности адекватно оценивать нанесенный ими вред, а следовательно, и испытывать в полной мере возможное раскаяние. При этом положительные ощущения от «достижения заранее планируемого результата, связанного с совершением преступления, и удовлетворение результатом, которое закрепляет образ акта преступного поведения и облегчает его проведение в дальнейшем» [5, с. 19], наступают в случае успеха, что ведет к последующему совершению преступлений. Если после совершения обычного преступления «на преступника, как правило, в большей степени начинает воздействовать фактор неопределенности своего положения, обусловленный, с одной стороны, сознанием виновности и боязнью наказания, а с другой — недостатком информации о тех действиях, которые предпринимаются правоохранительными органами для расследования преступления и изобличения виновного», то в случае совершения киберпреступления действие данного фактора может уменьшаться либо исключаться по двум причинам. Во-первых, при совершении специальных киберпреступлений преступники, уверенные в высоком уровне своих знаний и возможностей, а порой и своей гениальности, предполагают, что не оставили ни единого следа, который мог бы помочь изобличить их. Во-вторых, в настоящее время, особенно в странах СНГ, органы, ведущие борьбу с киберпреступностью, не всегда обладают достаточным интеллектуальным и кадровым потенциалом, что ведет к недооценке их киберпреступниками.

Не остаются без внимания киберпреступников и проблемы, связанные с глобальным характером киберпространства. Как верно заметил международный эксперт по гармонизации законодательства в сфере киберпреступности Штайн Шьольберг (Stein Schjolberg), киберпространство, как пятое общее пространство, после наземного, морского, воздушного и космического, требует координации, сотрудничества и особых правовых мер на международном уровне [14]. Тем не менее, к сожалению, эффективные меры международного масштаба по борьбе с киберпреступниками сейчас отсутствуют, что создает определенный вакуум в правовом регулировании ответственности и порядке уголовного преследования лиц, совершивших транснациональные преступления, и, соответственно, создает у киберпреступников впечатление возможности уклониться от уголовной ответственности.

Профессор Университета Райдер (США) Джон Шулер (John Suler) для обозначения эффекта, который киберпространство оказывает на человека, делая возможным действовать более свободно, нежели в реальном социуме, ввел понятие «эффект онлайн дезингибиции» [10]. Основу этого эффекта, по мнению Шулера, составляют:

– дисассоциативная анонимность («ты меня не знаешь»), сущность которой состоит в том, что в условиях анонимности люди могут отделить свои действия в киберпространстве от реального мира и реальной личности, в таком случае человек полагает, что

может не брать на себя ответственность за свои действия;

– невидимость («ты меня не видишь») – позволяет избегать установления психологического контакта;

– асинхронность («увидимся позже») – возможность общаться в отдельных случаях без необходимости немедленной реакции на слова или действия собеседника, что является немаловажным дезингибирующим фактором;

– солиптическая интроекция («это все в моей голове») – вероятность того, что при онлайн-общении может возникнуть ощущение, что все происходит исключительно в нашем собственном воображении;

– минимизация власти («мы равны») – возникает из-за опосредованного восприятия атрибутов более высокого социального положения, а также возможности их игнорировать. Тем не менее, необходимо учитывать, что в киберсоциуме можно говорить о существовании качественно другой, но все-таки иерархии.

Безусловно, не только объективные факторы киберпространства превратили его в достаточно криминогенную среду, но также активность различного рода преступников, которые, осознав преимущества Интернета, стали активно его использовать, в том числе для вовлечения в преступную деятельность других лиц. Так, Тина Фрайбургер (Tina Freiburger) и Джефри Крейн (Jefrey S. Crane) в своем исследовании «Интернет как инструмент в руках террористов» («The Internet as a Terrorist's Tool»), применив криминологическую теорию социального обучения к процессу вовлечения в преступную деятельность, доказали, что Интернет является более благоприятной для этого средой [15].

Поскольку ключевым моментом для юридической практики является установление мотивов и целей совершения преступления, не меньшее значение имеют и факторы, детерминирующие их формирование. Основой же формирования субъективной стороны преступления в целом и потребностей человека как исходных мотивов в частности является социальная среда обитания, в особенности ее содержательная часть. Сложность состоит в том, что мотивация киберпреступников формируется сразу в двух пространствах: реальном и киберпространстве. При этом на формирование мотивации большее влияние может оказывать и то и другое пространство.

Киберпространство по-иному влияет на мотивацию преступного поведения в силу следующих причин: 1) это пространство является внетерриториальным и основано на других консолидирующих факторах; 2) в киберпространстве происходит не только взаимодействие, взаимопроникновение и смешивание национальных культур, но и формирование своей собственной культурной среды — киберкультуры. Именно изучение влияния киберкультуры на мотивацию киберпреступников является важной задачей для криминологов, потому как уже сейчас группы хактивистов, подобные Anonymous или LulzSec, совершают тяжкие преступления, явно исходя из мотивов, сформированных в киберсреде.

В киберпространстве, как в фактически параллельной реальному миру социальной системе, вместе со смешением национальных культур и зарождением собственной происходят те же процессы с социальными нормами. Некоторые из социальных норм в киберпространстве отмирают, поскольку являются неприменимыми, но при этом под воздействием ряда негативных факторов, присущих киберпространству, формируются новые нормы. Можно предположить, что поскольку киберпространство играет достаточно большую роль в жизни молодежи, то в сознании молодых активных пользователей Интернета происходит замещение социальных норм нормами киберпространства, точно так же могут нивелироваться социальные нормы реальной жизни, неприменимые во Всемирной сети. Стоит согласиться с британским ученым Алистером Дафом (Alistair Duff), который утверждает, что современное информационное пространство ведет к нормативному кризису во всех сферах человеческой деятельности: экономике, политике, культуре и проч. [6] Подобное пограничное состояние, в свою очередь, отрицательно влияет и на психологию преступников.

Психологическая характеристика отдельных киберпреступников, безусловно, важная составляющая изучения киберпреступности, хотя и чрезвычайно объемная. Поэтому считаем необходимым представить только основные группы киберпреступников. (За основу данной классификации берется вид совершенного преступления и уровень компьютерных навыков преступников.)

1. Преступники специального киберпреступного типа. Данная категория преступ-

ников не только специализируется на совершении специальных киберпреступлений, но также каждый из киберпреступников данного типа совершает их самостоятельно и обладает «профессиональными» техническими знаниями, необходимыми для совершения преступлений данного рода. Критерий наличия специальных знаний является на сегодня крайне важным, вследствие того, что на виртуальном «черном рынке» достаточно программного обеспечения, информации и предложения услуг, которые позволяют совершать специальные киберпреступления без наличия соответствующих знаний. Наличие же специальных знаний фактически означает принадлежность такого преступника к субкультуре хакеров (крэкеров).

2. Преступники общекиберпреступного типа совершают при помощи электронных устройств неспецифические для киберпространства деяния (мошенничество, кражи, отмывание денежных средств, незаконное распространение порнографических материалов и проч.), не используя при этом специальные технические знания либо используя только поверхностные знания и приобретенные программные средства.

Как уже говорилось, условия киберпространства существенно отличаются от реальных, поэтому необходима дифференциация киберпреступников в зависимости от локализации их преступной деятельности. Критерий локализации имеет существенное значение для установления процесса возникновения преступного умысла, его природы, а также степени общественной опасности данного лица. Таким образом, можно выделить три основных группы.

1. Киберпреступники, ведущие основную преступную деятельность только в киберпространстве. Преступные установки у таких лиц сформировались в высококриминогенных условиях киберпространства, следовательно, в случае устранения криминогенных факторов такие лица могут представлять значительно меньшую социальную опасность, нежели реальные преступники.

2. Киберпреступники, занимающиеся в равной степени преступной деятельностью как в киберпространстве, так и реальной жизни. Психология преступников данной категории является типично преступной при незначительном влиянии условий киберпространства.

3. Лица, совершившие ранее преступления, не относящиеся к киберпреступлениям, совершающие киберпреступления в настоящее время. Появление этой категории киберпреступников обусловлено, в первую очередь, пристальным вниманием организованных преступных сообществ к широким возможностям Интернета. Обладая хорошими организаторскими способностями, такие киберпреступники используют лиц, имеющих специальные знания, для совершения преступлений, при этом основные усилия направляют на максимальное получение прибыли и усиление собственного влияния.

В зависимости от мотивации преступного поведения можно выделить следующие типы киберпреступников.

Корыстный тип. Помимо характерных для обыкновенного корыстного типа преступников свойств, киберпреступники могут совершать преступления для получения специфических предметов, имеющих особую ценность в киберпространстве, например игровых предметов, без цели их дальнейшей продажи.

Насильственный тип. Несмотря на отсутствие физического контакта, такие насильственные преступления, как доведение до самоубийства или угроза убийством, могут быть совершены при помощи электронных устройств и сетей. В связи с рядом самоубийств несовершеннолетних, совершенных в том числе под воздействием оскорблений или угроз, сделанных с помощью различных онлайн-сервисов, в США обсуждается возможность введения уголовной ответственности за киберзапугивание (cyberbullying) и киберпреследование (cyberstalking) для предотвращения трагических последствий.

Сексуальный тип. Для данного типа преступников характерно совершение таких преступлений, как незаконное распространение порнографических материалов или предметов, без цели наживы, понуждение к действиям сексуального характера, развратные действия. Вероятно, что в некоторых случаях совершение преступлений в отношении несовершеннолетних будет иметь место насильственно-сексуальный тип преступника.

Социально дезорганизующий тип, основной целью которого является само нарушение обеспеченных законодательно социальных норм и оказание деструктивного влияния на социум и общественные отношения.

Идеологически или *политически мотивированный* тип. В последнее время совершение

специальных киберпреступлений становится распространенной формой протеста и политической или идеологической борьбы. В западных странах для обозначения преступников специально киберпреступного типа, совершающих преступления по политическим или идеологическим убеждениям, используется термин «хактивист».

Статусный тип. Преступники этого типа, совершая преступления, стремятся получить более высокий неформальный социальный статус, зачастую в сообществах киберсоциума. Хотя по своей природе статусность как стимул к совершению преступлений является дополнительным фактором или оказывает кратковременное влияние на преступную деятельность, в среде хакеров (крэкеров) может иметь достаточно серьезное мотивирующее значение.

Исследовательский тип характерен для лиц, совершающих специальные киберпреступления. Основой для их мотивации служит изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения. Данные цели были характерны для первых поколений немногочисленных хакеров, а также отдельных современных преступлений, хотя сейчас в большинстве случаев они выступают только дополнительным мотивом. Преступники данного типа, в первую очередь, направляют свои действия на устранение ошибок и развитие защиты устройств и сетей и поэтому являются социально «полезными». Согласно исследованию Орли Тургеман-Голдшмидт (Orly Turgeman-Goldschmidt), хакеры по-разному истолковывают свою деятельность и цели, но, тем не менее, практически все они характеризуют себя как положительных девиантов: экстраординарных людей, которые умнее других и демонстрируют необычное, лучшее поведение, или даже являются носителями социальных изменений. Одним же из главных выводов исследования было то, что хакеры не ощущают вины за собственные преступные действия [12].

Также в последнее время в некоторых СМИ появилась информация о том, что некоторые из арестованных хакеров страдают таким аутистическим расстройством, как синдром Аспергера, вероятно, в среде хакеров подобного рода расстройства могут быть достаточно распространены. Дальнейшее изучение психологии исследовательского типа киберпреступников требует большого объема эмпирических данных, которые могут быть получены при работе с преступниками в ходе следствия. Большое значение в данных исследованиях имеет обмен полученной информацией между правоохранительными органами разных стран.

В настоящее время достижения, полученные в изучении психологии киберпреступников, уже активно применяются в других странах при расследовании преступлений, в основном, при определении типа преступников. Исследования в данной сфере являются также важным теоретическим материалом и могут способствовать развитию изучения психологии девиантного поведения.

Как показывает сложившаяся ситуация, в борьбе с киберпреступностью и ее профилактике необходим мультидисциплинарный подход, в котором не последнее место занимает психология. Поэтому создание эфективной системы противодействия киберпреступлениям требует активизации исследований психологии киберпреступников и подготовки кадров в данном направлении.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Бондаренко С.В.* Виртуальные сетевые сообщества девиантного поведения. – URL: http://cyberpsy.ru/2011/06/bondarenko-s-v-virtualnye-setevye-soobshhestva-deviantnogo-povedeniya/

2. *Кравченко А.И.* Общая психология : учеб. пособие. – М., 2011. – С. 399.

3. Стенограмма Национальной конференции США по киберэтике. – URL: http://connect.marymount.edu/ethics/cyberethics/sessions/gensession3.PDF

4. *Федоренко Д.* Криминологические аспекты урбанизации // Юридичний вісник. – 2000. – №1. – С. 95 – 99.

5. *Чуфаровский Ю.В.* Психология оперативно-розыскной деятельности. — 2-е изд., доп. — М., 2001. – С. 208.

6. *Alistair Duff.* The Normative Crisis of the Information Society. – URL: http://www.cyberpsychology.eu/ view.php?cisloclanku=2008051201

7. China tightens microblog supervision. – URL: http://www.chinadaily.com.cn/china/2011-12/22/content_14310618.htm

8. Copyright Infringement and Enforcement in the USA: Research Note. – URL: http://piracy.ssrc.org/wp-content/uploads/ 2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf. – P. 2, 11.

9. How far right views created Anders Behring Breivik. — URL: http://mg.co.za/article/2011-07-31-how-far-right-views-created-anders-behring-breivik

10. *John Suler.* The Psychology of Cyberspace. – URL: http://users.rider.edu/~suler/psycyber/psycyber.html

11. Lippestad: Nettdebattanter har ansvar for terroren. – URL: http://www.aftenposten.no/incoming/Lippestad-Nettdebattanter-har-ansvar-for-terroren-6714368.html

12. Orly Turgeman-Goldschmidt. Meanings that Hackers Assign to their Being a Hacker. – URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf

13. Real name registration for matchmaking websites. – URL: http://www.chinadaily.com.cn/china/2011-10/14/ content_13904173.htm

14. *Stein Schjolberg.* A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime. – URL: http://cybercrimelaw.net/documents/UN_12th_Crime_ Congress.pdf

15. *Tina Freiburger, Jeffrey S . Crane.* The Internet as a Terrorist's Tool // Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, 2011. – P. 461.

REFERENCES

1. Bondarenko S.V. *Virtual'nye setevye soobshchestva deviantnogo povedeniya* [Virtual Communities of Deviant Behavior]. URL : http://cyberpsy.ru/2011/06/ bondarenko-s-v-virtualnye-setevye-soobshhestva-deviantnogo-povedeniya/

2. Kravchenko A.I. *Obshchaya psikhologiya* [General Psychology]. Moscow, 2011, pp. 399.

3. http://connect.marymount.edu/ethics/ cyberethics/sessions/gensession3.PDF

4. Phedorenko D. *Yuridicheskij vestnik* [Legal Bulletin]. 2000, no.1, pp. 95 - 99.

5. Chupharovskij Yu.V. *Psikhologiya operativno-rozysknoj deyatel'nosti* [Psychology of Investigation Activities]. Moscow, 2001, pp. 208.

6. Alistair Duff. The Normative Crisis of the Information Society. URL: http://www.cyberpsychology.eu/ view. php?cisloclanku=2008051201

7. China tightens microblog supervision. URL: http://www.chinadaily.com.cn/china/2011-12/22/content_14310618. htm

8. Copyright Infringement and Enforcement in the USA: Research Note. URL: http://piracy.ssrc.org/wp-content/ uploads/ 2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf. P. 2, 11.

9. How far right views created Anders Behring Breivik. URL: http://mg.co.za/article/2011-07-31-how-far-right-views-created-anders-behring-breivik

10. John Suler. The Psychology of Cyberspace. URL: http://users.rider.edu/~suler/psycyber/psycyber.html

11. Lippestad: Nettdebattanter har ansvar for terroren. URL: http://www.aftenposten.no/incoming/Lippestad-Nettdebattanter-har-ansvar-for-terroren-6714368.html

12. Orly Turgeman-Goldschmidt. Meanings that Hackers Assign to their Being a Hacker. URL: http://www.cybercrimejournal.com/Orlyijccdec2008.pdf

13. Real name registration for matchmaking websites. URL: http://www.chinadaily.com.cn/china/2011-10/14/ content_13904173.htm

14. Stein Schjolberg. A cyberspace treaty – A United Nations convention or protocol on cybersecurity and cybercrime. URL: http://cybercrimelaw.net/documents/UN_12th_Crime_ Congress.pdf

15. Tina Freiburger, Jeffrey S . Crane. The Internet as a Terrorist's Tool . Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, 2011. Pp. 461.

Информация об авторах

Косенков Александр Николаевич (Харьков) – студент 5-го курса. Национальный университет «Юридическая академия Украины имени Ярослава Мудрого» (Украина, 61024, г. Харьков, ул. Пушкинская, 77, e-mail: alex_nlau@ inbox.ru)

Черный Геннадий Алексеевич (Харьков) – кандидат юридических наук, доцент. Национальный университет «Юридическая академия Украины имени Ярослава Мудрого» (Украина, 61024, г. Харьков, ул. Пушкинская, 77, e-mail: alex_nlau@inbox.ru)

Information about the authors

Kosenkov, Aleksandr Nikolayevich (Kharkov) – 5th-year student. National Law Academy of Ukraine named after Yaroslav the Wise (Pushkinskaya st., 77, Kharkov, 61024, Ukraine, e-mail: alex_nlau@inbox.ru)

Cherniy, Gennadiy Alekseyevich (Kharkov) – Ph.D. in Law, Ass. Professor. National Law Academy of Ukraine named after Yaroslav the Wise (Pushkinskaya st., 77, Kharkov, 61024, Ukraine, e-mail: alex_nlau@inbox.ru)