LAW

DOI https://doi.org/10.51647/kelm.2020.7.1.19

ZAPOBIEGANIE PRZESTĘPCZOŚCI NIELETNICH W ZAKRESIE TECHNIKI INFORMATYCZNEJ

Vadym Babakin
kandydat nauk prawnych, docent, pracownik naukowy Wydziału Organizacji Działalności Naukowo-Badawczej i Patentowej Centrum Badawczego Narodowego Uniwersytetu Obrony Cywilnej Ukrainy (Charków, Ukraina)
ORCID ID: 0000-0002-7157-0241
Email: vadon7373@gmail.com

Adnotacja. Artykuł poświęcono aktualnym zagadnieniom przeciwdziałania cyberprzestępstwom popełnianym przez osoby młode. Badana jest istota tego negatywnego zjawiska, a także proponowane są działania mające na celu poprawę zapobiegania badanej grupie. W artykule przeanalizowano treść i cechy środków zapobiegawczych, rozważono ich znaczenie w praktycznej działalności jednostek operacyjnych. Wyróżnia się i analizuje najbardziej problematyczne kwestie teoretyczne i prawne, które pojawiają się w jednostkach operacyjnych policji Ukrainy w kwalifikacjach przestępstw popełnionych przy użyciu sprzętu komputerowego i innych systemów telekomunikacyjnych, i przedstawia propozycje poprawy zapobiegania takiej grupie osób, w celu zapewnienia skuteczności zwalczania tego negatywnego zjawiska. Uzasadnia się pogląd, że szczególnie istotne są informacje o specyfice wykorzystania wiedzy specjalistycznej w rozwiązywaniu i dochodzeniu przedmiotowych przestępstw popełnionych przez młodzież.

Słowa kluczowe: jednostki operacyjne, informacja operacyjna, przestępstwo, młodzież, technika informatyczna, cyberprzestępczość, cyberbezpieczeństwo.

COUNTERACTION TO JUVENILE DELINQUENCY IN THE SPHERE OF INFORMATION TECHNOLOGIES

Vadym Babakin
Candidate of Law Sciences, Associate Professor,
Researcher at the Department for the Organization of Research and Patent Activity of the Research Center National University of Civil Defense of Ukraine (Kharkiv, Ukraine)
ORCID ID: 0000-0002-7157-0241
e-mail: vadon7373@gmail.com

Abstract. The article is focused on topical issues of counteracting cybercrimes committed by young people. The essence of this negative phenomenon is considered; and actions to improve the counteraction to the studied group are suggested. The author of the article analyzes the content and specific features of preventive measures, considers their importance in the practical activities of operative units. The author of the article highlights and analyzes the most problematic theoretical and legal issues faced by operative units of the Ukrainian police while qualifying crimes committed with the use of computer equipment and other telecommunication systems. The author provides suggestions for improving the counteraction to such group of persons in order to ensure the effectiveness of the fight against this negative phenomenon. The author of the article substantiates the opinion that information about the specifics of the use of special knowledge while detecting and investigating studied crimes committed by young people is especially significant.

Key words: operative units, operative information, criminal offense, youth, information technologies, cybercrime, cyber security.

ПРОТИВОДЕЙСТВИЕ МОЛОДЕЖНОЙ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Вадим Бабакин
кандидат юридических наук, доцент,
научный сотрудник отдела организации научно-исследовательской и патентной деятельности научно-исследовательского центра
Национального университета гражданской защиты Украины (Харьков, Украина)
ORCID ID: 0000-0002-7157-0241
e-mail: vadon7373@gmail.com

Аннотация. Статья посвящена актуальным вопросам противодействия киберпреступлениям, совершаемым лицами молодого возраста. Рассматривается сущность этого негативного явления, а также предложены действия по усовершенствованию противодействия исследуемой группы. В статье проанализированы содержание и особенности мер предупреждения, рассмотрено их значение в практической деятельности оперативных подразделений. Выделяются и анализируются наиболее проблемные теоретико-правовые вопросы, которые возникают у оперативных подразделений полиции Украины при квалификации преступлений, совершенных с использованием компьютерной техники и других телекоммуникационных систем, и приводятся предложения по усовершенствованию противодействия такой группой лиц с целью обеспечения эффективности борьбы с данным негативным явлением. Обосновывается мнение о том, что особо значимой является информация о специфике использования специальных знаний при раскрытии и расследовании рассматриваемых преступлений, совершенных молодежью.

Ключевые слова: оперативные подразделения, оперативная информация, уголовное правонарушение, молодежь, информационные технологии, киберпреступление, кибербезопасность.

Вступление. Современное общество характеризуется постоянным совершенствованием информационных технологий и повседневным использованием компьютерной техники, сетей связи, мобильных средств коммуникации и других технических средств. Ежедневная работа правительственных структур, банковской, энергетической, транспортной и других систем жизнеобеспечения человека не возможна без надежного функционирования компьютерной техники и средств коммуникации. Информационные технологии стали постоянным спутником человека не только на рабочем месте: они вошли практически во все сферы человеческой жизни и быта. Быстрое распространение новых информационных технологий, в основе которых лежит широкое использование компьютерной техники и средств коммуникации, оптимизация и автоматизация процессов всех без исключения сфер жизнедеятельности привели к тому, что информационное пространство стало использоваться маргинальными лицами как непосредственный инструмент совершения преступления. Главным инструментом преступника становится компьютер, с помощью которого он получает доступ к информационно-коммуникационным системам, а также к системам получения денежных и иных средств, применяет компьютерные вирусы, использует другие противозаконные технические средства, обеспечивая себе доступ к базам данных, банковским счетам, автоматизированным системам управления (Гуржій, 2014: 3–4). В совершении таких преступлений принимает непосредственное участие наиболее развитая в техническом отношении молодежь. В связи с изложенным необходимо исследовать использование новых достижений науки и техники в целях предупреждения этих видов преступлений.

Основная часть. Проблемы противодействия преступности в сфере информационных технологий исследовали такие ученые, как А.М. Бандурка, В.Н. Бутузов, М.Г. Вербенский, А.Н. Джужа, Г.А. Зорин, Б.И. Калачов, Л.Л. Каневский, М.В. Корниенко, Н.Н. Перепелица, Е.Д. Скулиш, В.В. Шендрик, А.А. Юхно. Однако проблемные вопросы противодействия преступлениям в сфере киберпреступности остаются в науке открытыми и приобретают все большую актуальность.

Цель статьи заключается в определении путей противодействия молодежной преступности в сфере информационных технологий.

Результаты. Согласно исследованию, современные тенденции развития теории и практики оперативно-розыскной деятельности, а также досудебного расследования в сфере использования информационных технологий опираются на применение технических средств в раскрытии, документировании и расследовании киберпреступлений. Многолетний анализ практической деятельности следственных и оперативных подразделений свидетельствует о том, что на современном этапе оперативные подразделения остаются недостаточно оснащенными научно-техническим арсеналом, в связи с чем возникают проблемы в организации и эффективности проведения мероприятий по выявлению, предупреждению и пресечению уголовных правонарушений в сфере киберпреступности.

Анализ статистики правоохранительных органов свидетельствует о том, что около 35–40% преступлений ежегодно совершаются с использованием современных телекоммуникационных, компьютерных и других современных технологий, а в будущем данные показатели могут резко увеличиться. По нашему мнению, одним из стратегических направлений в противодействии киберпреступности является совершенствование поиска, сбора, фиксации и мониторинга оперативной информации с использованием современных информационных технологий, имеющихся технических средств ОРД, которые ежегодно совершенствуются.

Дети, несовершеннолетние и молодежь все активнее осваивают компьютерные технологии. Мотивацией отдельных представителей этой группы является стремление завладеть денежными средствами. Одни из них специализируются на уголовном посягательстве на денежные средства путем несанкционированного проникновения в компьютерные сети банковских учреждений, другие – на использовании пластиковых платежных документов (Лук'яненко, 2003: 214–216).

Исследования, которые осуществила Г.М. Шорохова путем анкетирования, показали, что возраста компьютерных правонарушителей колеблется в пределах от 14 до 35 лет. Возраст 33% злоумышленников на момент совершения правонарушения не превышал 20 лет, возраст 54% преступников составлял от 20 до 40 лет, 13% злоумышленников старше 40 лет. Правонарушения в сфере использования компьютерных технологий в 5 раз чаще совершаются мужчинами. Большинство злоумышленников имеют высшее или незаконченное высшее образование (53,7%), а также другое профессиональное образование (19,2%). Интересно, что в последнее время постоянно увеличивается доля женщин (Шорохова, 2010: 125).

Как указывает В.Б. Вехов, лицо молодого возраста, совершившее киберпреступление, рассматривается в криминалистике как личность с присущими ей социальными, психологическими, психофизическими,

нравственными качествами. Именно личные качества молодого человека и окружающая среда взаимоотношений во взаимодействии последовательно определяют мотивацию принятия решения об объединении с другими лицами для совместной преступной деятельности в сфере информационных технологий и выполнения принятого решения. Мотивация включает процесс возникновения, формирования мотива преступного поведения и его цель. Мотив преступного поведения, как считают криминологи, нужно рассматривать как внутреннее побуждение к действию; желание, которое определено потребностями, интересами, чувствами, которые возникают и обостряются под влиянием внешней среды и конкретной ситуации. В то же время, как считают большинство исследователей, при совершении корыстных преступлений личность «преобладает» над ситуацией, а мотив формирует цель. Это в полной мере относится и к молодежи, поскольку количество совершенных нею корыстных преступлений составляет более 70%, а по нашим исследованиям – 87,3%. Мотив преступного поведения формируется под влиянием социального окружения, жизненного опыта личности, побуждением внутреннего состояния, которое направлено на преступную деятельность (Вехов, 1996: 66).

Указанное дает основания говорить о том, что при организации и проведении комплексных и целевых оперативно-профилактических мероприятий в противодействии уголовным правонарушениям в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи эти психологические, психофизические свойства, которые присущи молодежи, должны учитываться оперативными работниками, в частности желание уголовно настроенных молодых людей каждый день совершенствовать свои знания в этих вопросах (в основном бесплатно) при общении со сверстниками.

Рассматривая лицо, которое готовит и совершает киберпреступления, В.Б. Вехов выделяет три группы, а именно лиц, особенностью которых является устойчивое сочетание профессионализма в сфере компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности; лиц, страдающих психическими заболеваниями (компьютерные фобии); профессиональных компьютерных преступников с ярко выраженной корыстной целью (Вехов, 1996: 38–39), что мы поддерживаем.

Некоторые авторы, в частности А.В. Соколов и А.Н. Степанюк, классифицируют правонарушителей как искателей приключений, идейных хакеров и компьютерных специалистов. По результатам изучения уголовных производств, чаще всего к уголовной ответственности за совершение правонарушений в сфере информационных технологий привлекалась молодежь в возрасте от 18 до 35 лет. По результатам исследования, количество киберпреступников в возрасте 16–35 лет выросло почти в 4 раза (Соколов, Степанюк, 2002: 43), что мы поддерживаем.

Согласно научной позиции С.С. Малыгина, решение проблем информационного обеспечения деятельности подразделений криминальной полиции Украины, занимающихся предупреждением, пресечением и расследованием преступлений и розыском преступников, в современных условиях зависит от их технической оснащенности, компьютеризации, реализации новых информационных технологий, что связано с ростом профессионального мастерства всех подразделений, участвующих как в сборе необходимой информации, так и в наполнении информационных систем и использовании этих сведений в решении задач ОРД (Малыгин, Чечетин, 2001: 164). По нашему мнению, это касается получения оперативной информации оперативными подразделениями касательно молодых людей, которые готовятся совершить, совершают или совершили уголовные преступления в сфере высоких информационных технологий.

Согласно научной позиции А.А. Юхно, для осуществления предупреждения преступлений, как и любой другой процедурной деятельности, необходимо несколько блоков информационных ресурсов, в частности блок основной (структурной) информации, которая отражает системные параметры; блок дополнительной (функциональной) информации, которая отражает налаженные системные связи между различными компонентами; блок прогнозной информации, которая отражает количественно-качественные параметры равновесия системы предупреждения преступлений (Юхно, 2005: 13), что мы поддерживаем.

В связи с ростом в банковской сфере объемов безналичных расчетов лица молодого возраста готовят и совершают уголовные преступления, особенно через систему интернет-банкинга. По данным Национального банка Украины, в 2018 году количество противоправных операций по платежным картам украинских банков выросло до 7,6 тыс. по сравнению с 2017 годом, когда было осуществлено только 2,9 тыс. операций. Объем неправомерно списанных средств увеличился почти в полтора раза, а именно с 6 300 000 до 9 100 000 грн. (Малыгин, Чечетин, 2001: 5).

Так, кражи данных платежных карт (банковских счетов) или данных доступа к системе интернет-банкинга с целью завладения средствами клиентов банка, похищения персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное повреждение работы информационных систем или средств коммуникаций с целью создания убытков компаниям – это далеко не полный перечень подобных угроз, которые несет с собой бурное развитие современных информационных технологий, при этом киберпреступность приобретает все больший мировой масштаб, новейшие технологии превращают реальных преступников в анонимных, а легкость быстрого обогащения обольщает все больше людей присоединиться к этой преступной деятельности.

Популярность сети Интернет вполне закономерна, поскольку пользователь, особенно молодые люди в возрасте 14–35 лет, имеет возможность круглосуточного доступа к значительному объему информации, быстрого обмена информацией с другими пользователями. Банковская система Украины является одной из сфер, где наиболее широко и активно используются современные возможности информационных технологий

и сети Интернет при расчетах физических и юридических лиц. С учетом того, что указанные технологии используются для денежных переводов, эта сфера привлекает все больше внимания преступников.

Согласно оценкам экспертов, преступность в сети Интернет способна нанести ущерб, который можно сравнить с объемом кражи изделий искусств во всем мире. По данным ООН, убытки, которые наносит такая преступность, можно сравнить с доходами от противозаконного оборота наркотиков и оружия. Кроме того, такая преступность выступает сдерживающим фактором для развития конкурентоспособности экономики стран мира, в том числе Украины, поскольку покупатели, предприятия и банки с опаской используют новые технологии и интернет-услуги (Юхно, 2005: 1–2).

По данным Департамента киберполиции Национальной полиции Украины, только за второе полугодие 2019 года в Киеве зафиксировано до двадцати случаев кражи денег через клиент-банк. Суммы составляют от 100 тыс. до 75 млн. грн. Однако подобные факты замалчиваются, сообщений в СМИ о них практически нет. Ни потерпевшим, ни банкам, ни полиции не выгодны разговоры вокруг таких факторов. В ряде случаев бывают ситуации, когда такие мошеннические схемы реализуются организованными группами, в которые входят представители банков и силовых структур (Киберпреступность в Украине набирает обороты: 2012), поэтому совершенные уголовные преступления в системе Интернет имеют латентный характер. Согласно исследованию В.Б. Вехова, компьютерная преступность характеризуется огромной латентностью. Это означает, что большинство незаконных действий в сфере высоких технологий остается не только не раскрытой, но и даже не учтенной. У этого есть две причины. Прежде всего, многие люди могут даже не заметить, что кто-то имел доступ к их конфиденциальной материальной информации. Вторая причина латентности компьютерной преступности заключается в нежелании компаний или частных лиц признаться в том, что они стали жертвами злоумышленников. Во втором случае большую роль играют страх перед потерей имиджа фирмы и боязнь, что правоохранительные органы могут найти информацию, которая для них не предназначена. Частные же лица считают, что действия хакеров не наносят им большой ущерб, поэтому обращение в правоохранительные органы и связанная с этим потеря времени представляются им большей потерей. Наверное, даже не нужно объяснять, почему эта точка зрения ошибочна. Пока мы не будем помогать правоохранительным органам, а именно оперативным подразделениям полиции, которые должны заблаговременно получать информацию и адекватно реагировать на правонарушения, которые готовятся или совершаются молодежью в сфере высоких информационных технологий, компьютерная преступность в нашей стране будет расти (Вехов, 1996: 103–105).

Одним из наиболее эффективных способов противодействия киберпреступности, особенно тем преступлениям, которые совершаются молодежью, является использование оперативными подразделениями различных форм, методов и средств предупредительного характера. Одной из форм является информирование населения, в том числе молодых людей, которые в случае совершения правонарушений в сфере высоких информационных технологий должны привлекаться к уголовной ответственности. Анализ практической деятельности оперативных подразделений свидетельствует о том, что большинство лиц молодого возраста во время совершения киберпреступлений сохраняет иллюзию собственной безнаказанности. Особенно это важно учитывать оперативным подразделениям при организации проведения мероприятий по предупреждению указанных правонарушений. Учитывая стремительные процессы развития информационных технологий, считаем особенно важным то, что меры, принимаемые правоохранительными органами в целях противодействия киберпреступности, должны быть своевременными и эффективными, а это зависит от таких условий:

1) организация обеспечения надежного сохранения информационно-аналитической базы данных и конфиденциальной информации, используемой в своей деятельности работниками оперативных подразделений;

2) обеспечение оперативного сбора информации и изъятия доказательств из телекоммуникационных систем в отношении лиц, подозреваемых в совершении таких уголовных правонарушений, а также установления их места нахождения;

3) быстрое получение оперативной информации по фактам и обстоятельствам совершения преступления в сети Интернет;

4) обеспечение быстрого и эффективного обмена оперативной информацией в организации и осуществления мероприятий по противодействию киберпреступности.

Выводы. Таким образом, комплексное и эффективное использование правовых, технических, организационных и современных технологий, а также научно-технических средств дает возможность следователям и сотрудникам оперативных подразделений полиции эффективно и результативно осуществлять предупреждение и противодействие уголовным правонарушениям в сфере киберпреступлений, которые готовятся или совершаются лицами молодого возраста.

Список использованных источников:

1. Вехов В.Б. Компьютерные преступления. Способы совершения, методики расследования. Москва : Право и закон, 1996. 182 с.
2. ГуржійГ.С.Кіберзлочинністьтавідмиваннякоштів.URL:http://www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf.
3. Киберпреступность в Украине набирает обороты. URL: http://ua.golos.ua/social_problem/12_11_30_kiberprestupnost_v_ukraine_nabiraet_oborotyi.
4. Лук'яненко С.О. Аспекти систематизації злочинів в кредитно-фінансовій сфері. *Проблеми кодифікації законодавства України* : матеріали науково-практичної конференції (м. Київ, 14 травня 2003 року) / Інститут держави і права імені В.М. Корецького НАН України ; за заг. ред. В.П. Нагребельного, Н.М. Пархоменко. Київ, 2003. С. 214–216.

5. Малыгин С.С., Чечетин А.Е. Основы оперативно-розыскной деятельности : курс лекций. Екатеринбург : Уральский юридический институт МВД России, 2001. 306 с.
6. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма : справочное пособие. Санкт-Петербург : БХВ-Петербург, 2002. 496 с.
7. Шепетько С.А. Форми вчинення транснаціональними злочинними організаціями окремих злочинів за допомогою використання мережі Інтернет. URL: http://journal-bzozik.com.ua/menus/view/3_312013#1.
8. Шорохова Г.М. Детермінація вчинення кіберзлочинів неповнолітніми. *Сучасні напрями профілактики та актуальні проблеми розслідування злочинів, що вчиняються неповнолітніми* : матеріали науково-практичного семінару (м. Харків, 16 квітня 2010 року). Харків : Харківський національний університет внутрішніх справ, 2010. С. 127–130.
9. Юхно О.О. Діяльність транспортної міліції щодо попередження крадіжок приватного майна громадян на пасажирському залізничному транспорті : автореф. дис. … канд. юрид. наук : спец. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Харків, 2005. 20 с.

References:

1. Vexov V.B. Komp'yuterny'e prestupleniya. Sposoby' soversheniya, metodiki rasledovaniya. Moskva : Pravo i zakon, 1996. 182 s.
2. Gurzhij G.S. Kiberzlochinnist' ta vidmivannya koshtiv. URL: http://www.minfin.gov.ua/file/link/396800/ file/ tipolog2013.pdf.
3. Kiberprestupnost' v Ukraine nabiraet oboroty'. URL: http://ua.golos.ua/social_problem/12_11_30_kiberprestupnost_v_ ukraine_nabiraet_oborotyi.
4. Luk'yanenko S.O. Aspekti sistematizaczij zlochiniv v kreditno-finansovij sferi. Problemi kodifikaczij zakonodavstva Ukraïni : materiali nauk.-prakt. konf. (m. Kijv, 14 travnya 2003 roku) / In-t derzhavi i prava imeni V.M. Korecz'kogo NAN Ukrajni; za zag. red. V.P. Nagrebel'nogo, N.M. Parxomenko. Kijv, 2003. S. 214–216.
5. Maly'gin S.S., Chechetin A.E. Osnovy' operativno-rozy'sknoj deyatel'nosti : kurs lekcij. Ekaterinburg : Ural'sk. Yurid. in-t MVD Rossii, 2001. 306 s.
6. Sokolov A.V., Stepanyuk O.M. Zashhita ot komp'yuternogo terrorizma : spravochnoe posobie. SPB : BXV-Peterburg, 2002. 496 s.
7. Shepet'ko S.A. Formi vchinennya transnaczional'nimi zlochinnimi organizacziyami okremix zlochiniv za dopomogoyu vikoristannya merezhi Internet. URL: http://journal-bzozik.com.ua/menus/view/3_312013#1.
8. Shoroxova G.M. Determinacziya vchinennya kiberzlochiniv nepovnolitnimi. Suchasni napryami profilaktiki ta aktual'ni problemi rozliduvannya zlochiniv, shho vchinyayut'sya nepovnolitnimi : materiali nauk.-prakt. seminaru (m. Xarkiv, 16 kvitnya 2010 roku). Xarkiv : Xarkiv. nacz. un-t vnutr.sprav, 2010. S. 127–130.
9. Yuxno O.O. Diyal'nist' transportnoï miliczi shhodo poperedzhennya kradizhok privatnogo majna gromadyan na pasazhirs'komu zaliznichnomu transporti : avtoref. dis. … kand. yurid. nauk : specz. 12.00.08 "Kriminal'ne pravo ta kriminologiya; kriminal'no-vikonavche parvo". Xarkiv, 2005. 20 s.