# ПРОТИВОДЕЙСТВИЕ МОЛОДЕЖНОЙ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**Вадим БАБАКИН,**
кандидат юридических наук, доцент, докторант
Харьковского национального университета внутренних дел

**SUMMARY**

Article is devoted to relevant issues of combating cybercrimes committed by young persons. The essence of this negative phenomenon is considered and the ways of counteraction youth crime in the area of information technologies are also improved.

**Keywords:** operational units of law enforcement bodies, operational information, crime offence, youth, information technologies.

**РЕЗЮМЕ**

Статья посвящена актуальным вопросам противодействия киберпреступлениям, совершаемым лицами молодого возраста. Рассматривается сущность этого негативного явления, а также предложены действия по усовершенствованию противодействия молодежной преступности в сфере информационных технологий.

**Ключевые слова:** оперативные подразделения органов внутренних дел, оперативная информация, уголовное правонарушение, молодежь, информационные технологии.

**Постановка проблемы.** Современное общество характеризуется постоянным совершенствованиеминформационных 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, привело к тому, что информационное пространство стало использоваться маргинальными лицами как непосредственного инструмента совершения преступления. Теперь для совершения отдельных видов преступлений не нужна предварительная «обработка клиента» и не всегда личный контакт с потенциальной жертвой. Главным инструментом преступника становится компьютер, с помощью которого он получает доступ к информационно-коммуникационным системам, а также к системам получения денежных и иных средств, применения компьютерных вирусов, использования других противозаконных технических средств, обеспечивая себе доступ к базам данных, банковским счетам, автоматизированным системам управления [1]. 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.

**Актуальность темы.** Согласно результатам нашего научного исследования, современные тенденции развития теории и практики досудебного расследования и оперативно-розыскной деятельности в сфере использования информационных технологий опираются на использование технических средств в выявлении, раскрытии, предупреждении и предотвращении киберпреступлений, большая часть из которых совершается лицами молодого возраста до 35 лет. Многолетний анализ практической деятельности следственных и оперативных подразделений органов внутренних дел (далее – ОВД) свидетельствует о том, что на современном этапе подразделения ОВД недостаточно оснащены техническими средствами. Вышеуказанное ухудшает процессы организации и снижает эффективность проведения мероприятий по выявлению, предупреждению и пресечению уголовных правонарушений в сфере киберпреступности. Анализ статистических данных правоохранительных органов свидетельствует о том, что ежегодно около 35–40 % преступлений совершаются с использованием современных телекоммуникационных, компьютерных и иных технологий, а в будущем по криминологическим и другим прогнозам данные показатели могут резко увеличиться. По нашему мнению, одним из стратегических направлений в противодействии киберпреступности среди молодежи является совершенствование поиска, сбора, фиксации и мониторинга оперативной информации по ее сбору и анализу для планирования и реализации соответсвующих

мероприятий упредительного и пресекающего характера.

**Состояние исследования.** 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 и другие. Несмотря на вышеуказанные исследования решение проблемы противодействия киберпреступлений среди молодежи и особенно после принятия действующего УПК Украины остается не исследованным и приобретает все большую актуальность.

**Цель данной статьи** – определить пути противодействия молодежной преступности в сфере информационных технологий.

**Изложение основного материала.** Массовая компьютеризация в условиях стремительного развития информационных технологий в Украине сопровождается увеличением количества интернет-пользователей, особенно среди людей молодого возраста, что связано с доступностью подключения к глобальной сети и получения информации по любому интересующему вопросу как молодых, так и людей любого возраста. Согласно результатам исследования GfK Ukraine, количество регулярных интернет-пользователей старше 16-ти лет в Украине возросла в I квартале 2013 г. по сравнению с IV кварталом 2012 г. на 15,1 % (что на 21 % больше по сравнению с I кварталом 2012 г.) и составила 17,34 млн. человек. По итогам 2012 г. количество регулярных интернет-пользователей старше 16-ти лет в Украине составляла 15,41 млн. человек, что на 27 % больше, чем в 2011 г. [2]. Несовершеннолетние и молодежь все активнее осваивают компьютерные технологии, а некоторые из них с преступным умыслом. Мотивация этой группы правонарушителей это желание завладеть денежными средствами. Отдельные молодые преступники специализируются на уголовном посягательстве относительно денежных средств путем несанкционированного проникновения в компьютерные системы банковских учреждений, некоторые на совершение фактов мошенничества по завладению денежными средствами с использованием пластиковых документов [3].

Анкетирование, проведенное Г. М. Шороховой, показало, что возраст компьютерных правонарушителей колеблется в пределах от 14-ти до 35-ти лет, то есть людей молодого возраста. Возраст 33 % преступников на момент совершения правонарушения не превышал 20-ти лет, 54 % преступников находились в возрасте 20–40 лет и только 13 % были старше 40 лет. Таким образом 87% лиц совершивших такие виды преступлений были совершены в молодом возрасте, то есть до 35 лет. Как показало исследование правонарушений в сфере использования компьютерных технологий в пять раз чаще совершаются мужчинами. Большинство преступников имели высшее или незаконченное высшее образование (53,7 %), либо среднее профессиональное образование (19,2 %). Интересно, что в последнее время среди лиц, совершивших подобные преступления, постоянно увеличивается и доля женщин [4, с. 127].

Исследуя это направление, В. Б. Вехов указывает, что лицо молодого возраста, совершившее киберпреступление, в криминалистике рассматривается как личность со свойственными ей социальными, психологическими, психофизическими, этическими качествами. Именно личные качества молодого человека и окружающая среда во взаимодействии последовательно определяют мотивацию принятия решения об объединении с другими лицами для совместной преступной деятельности в сфере информационных технологий и выполнение принятого решения. Мотивация включает процесс возникновения и формирования мотива преступного поведения и его цель. Мотив преступного поведения, по мнению криминологов, нужно рассматривать как внутреннее побуждение к действию; желание, определенное потребностями, интересами, чувствами, которые возникают и обостряются под влиянием внешней среды, конкретной ситуации. В то же время, как считает большинство исследователей, при корыстных преступлениях личность «преобладает» над ситуацией, а мотив формирует цель. Мотив преступного поведения формируется под влиянием социального окружения, жизненного опыта личности; побуждения являются внутренней, непосредственной причиной преступной деятельности и выражают личное отношение к тому, на что направлена преступная деятельность [5, с. 66]. Указанное дает основания говорить о том, что при организации и проведении комплексных и целевых оперативно-профилактических мероприятий и противодействия уголовных правонарушений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи психологические и психофизические свойства, присущие молодежи, должны учитываться оперативными работниками ОВД. Рассматривая особенности личности злоумышленников, совершающих киберпреступления, В. Б. Вехов выделяет три группы лиц: 1) лица, особенностью которых является устойчивое сочетание профессионализма в сфере компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности; 2) лица, страдающие психическими заболеваниями (компьютерной фобией); 3) профессиональные компьютерные преступники, имеющие ярко выраженную корыстную

цель [5, с. 38–39]. Такое деление представляется целесообразным и в контексте нашего исследования, что мы поддерживаем.

Некоторые авторы, в частности А. В. Соколов и А. Н. Степанюк классифицируют правонарушителей на искателей приключений, идейных хакеров и компьютерных профессионалов. Результаты изучения материалов уголовных производств свидетельствуют о том, что чаще всего к уголовной ответственности за совершение правонарушений в сфере информационных технологий привлекалась молодежь в возрасте от 18-ти до 35-ти лет. Согласно данным исследования, за пять последних лет количество киберпреступников в возрасте 16–35 лет выросло почти в четыре раза [6].

По мнению С. С. Малыгина, решение проблем информационного обеспечения деятельности подразделений ОВД, занимающихся предупреждением, пресечением и расследованием преступлений и розыском преступников, в современных условиях непосредственно связано с их технической образованностью и оснащенностью, компьютеризацией, внедрением новых информационных технологий, а также с ростом профессионального мастерства всех сотрудников подразделений, участвующих как в сборе необходимой информации, так и в наполнении информационных систем и в результате использования этих сведений для решения задач оперативно-розыскной деятельности [7, с. 164], что мы поддерживаем. По нашему мнению, это относится и к получению оперативной информации оперативными подразделениями ОВД относительно несовершеннолетних лиц и лиц молодого возраста, которые готовятся, совершают или уже совершили уголовные правонарушения в сфере информационных технологий.

По мнению А. А. Юхно, для осуществления предупреждения преступлений, как и любой другой процедурной деятельности, необходимо несколько блоков информационных ресурсов, в частности: 1) блок основной (структурной) информации, которая отражает системные параметры; 2) блок дополнительной (функциональной) информации, которая отражает налаженные системные связи между различными компонентами; 3) блок прогнознозируемой информации, которая отражает количественно-качественные параметры равновесия системы предупреждения преступлений [8, с. 13], что мы поддерживаем и считаем дополнить блоком запланированных мероприятий для упреждения или пресечения такого вида преступлений.

В связи с тем, что в банковской сфере постоянно возрастают объемы безналичных расчетов, лица молодого возраста очень часто готовят и совершают уголовные преступления через систему интернет-банкинга. По данным Национального банка Украины, в 2011 г. количество противоправных операций по платежным картам украинских банков выросло до 7,6 тысяч по сравнению с 2,9 тысячами в 2010 году. Объем неправомерно списанных средств увеличился почти в полтора раза – с 6,3 млн. до 9,1 млн. грн [9]. Так, кражи данных платежных карт (банковских счетов) или данных доступа к системе интернет-банкинга с целью завладения денежными и иными средствами клиентов банка, кража персональных данных и коммерческой информации из частных компьютеров или серверов, умышленное нарушение работы информационных систем или средств коммуникаций с целью создания убытков компаниям это далеко не полный перечень угроз, которые несет с собой бурное развитие современных информационных технологий. При этом киберпреступность приобретает по-настоящему мировые масштабы, новейшие технологии превращают реальных преступников в анонимных, трудно доказуемых лиц, а легкость и быстрота подобного обогащения становятся соблазном для все большего количества молодых людей. Популярность сети Интернет вполне закономерна, поскольку пользователь имеет возможность круглосуточного доступа к значительному объему информации, а также может быстро обмениваться информацией с другими пользователями. Банковская система Украины является одной из сфер, где очень широко и активно используются современные возможности информационных технологий и сети Интернет. Учитывая то, что указанные технологии используются для совершения денежных переводов, указанная сфера привлекает все большее внимание молодых преступников. [10] Подготовка и совершение киберпреступления осуществляется практически не отходя от «рабочего места», то есть такое уголовное правонарушение можно совершить из какой-либо даже с удаленной точки доступа, и любого населенного пункта, а сами объекты преступных посягательств могут находиться за тысячи километров от преступника. Кроме того, достаточно сложно выявить, зафиксировать и изъять криминалистически значимую и доказательственную информацию при выполнении следственных действий [11]. На основании этого можно утверждать, что без конспиративного обеспечения оперативно-розыскной деятельности невозможно получить оперативную информацию относительно исследуемой категории правонарушителей в законном порядке и задокументировать преступную деятельность.

Согласно оценкам экспертов, преступность в сети Интернет способна нанести убытки, сравнимые с убытками от краж произведений искусства во всем мире, а по данным ООН, ущерб, который причиняет такая преступность, можно сравнить с ущербом, причиняемым противозаконным оборотом наркотиков и оружия.

Кроме того, существование данной категории преступлений выступает сдерживающим фактором развития конкурентоспособности экономики стран мира, в том числе и Украины, поскольку покупатели, предприятия и банки с опаской используют новые интернет-услуги [12]. По данным управления по борьбе с киберпреступностью МВД Украины, только в г. Киев фиксируется до двадцати случаев кражи денег через систему «клиент-банк» в месяц, а суммы похищенного составляют от 20 тысяч до 40 млн грн. Однако, подобные факты замалчиваются, сообщений в СМИ о них практически нет. Ни потерпевшим, ни банкам, ни милиции не выгоден шум вокруг происходящего. В ряде случаев такие мошеннические схемы реализуются организованными группами, в которые входят представители банков и силовых структур [13], поэтому уголовные правонарушения, совершенные в интернете, имеют латентный характер и им можна противопоставить только мероприятиями на основе использования тех же новейших достижений науки и техники.

Согласно отдельных исследований В. Б. Вехова, компьютерная преступность характеризуется огромной латентностью. Это означает, что подавляющее большинство незаконных действий в сфере информационных технологий остаются не только не раскрытыми, но и не учтенными. Для этого есть две причины. Во-первых, многие люди могут даже не заметить, что кто-то получил доступ к их конфиденциальной информации. Вторая причина латентности компьютерной преступности заключается в нежелании компаний или частных лиц признаться в том, что они стали жертвами злоумышленников. В первом случае большую роль играют страх перед потерей имиджа фирмы и боязнь, что правоохранительные органы могут выявить информацию, которую потерпевшие скрывали от них. По результатам исследований, частные лица считают, что действия хакеров не причиняют им большого ущерба. Поэтому потеря времени, связанная с обращением в правоохранительные органы, кажется им как ложно более значимой, чем убытки, нанесенные преступлением. Наверное, даже не нужно объяснять, почему эта точка зрения ошибочна. До тех пор пока мы не будем помогать правоохранительным органам, уровень компьютерной преступности в нашей стране будет расти [5, с. 103–105]. Оперативные подразделения ОВД должны заблаговременно получать информацию, чтобы адекватно реагировать на правонарушения, которые готовятся или совершаются, в том числе и относительно правонарушений совершаемых в сфере информационных технологий.

Одним из самых эффективных способов противодействия киберпреступлениям, особенно тем, которые совершаются несовершеннолетними и молодежью, является использование оперативными подразделениями ОВД различных методов и средств и методов предупредительного характера. Таким методом является информирование населения, в том числе несовершеннолетних и лиц молодого возраста о привлечении к уголовной ответственности за совершение правонарушений в сфере информационных технологий. Анализ практической деятельности оперативных подразделений свидетельствует о том, что большинство несовершеннолетних и лиц молодого возраста во время совершения киберпреступлений сохраняют иллюзию собственной безнаказанности. Особенно важно это учитывать оперативным подразделениям ОВД при организации и проведении мероприятий по предупреждению данных правонарушений.

Учитывая стремительные процессы развития информационных технологий, особенно важно, чтобы меры, принимаемые правоохранительными органами в целях противодействия киберпреступности, были своевременными и эффективными. Это зависит, прежде всего, от следующих условий: 1) от обеспечения надежного хранения информационной базы данных, которая используется сотрудниками правоохранительных органов; 2) от обеспечения сбора и изъятия доказательств по электронному документообороту у лиц, подозреваемых в совершении таких преступлений; 3) от быстрого получения оперативной информации относительно фактов и обстоятельств совершения преступления в сети интернет лицами молодого и иного возраста; 4) от установления местонахождения лиц, подозреваемых в совершении преступлений, посредством использования информационных технологий [14], что мы поддерживаем, но по нашему мнению к указанному следует добавить также эффективное использование оперативных учетов; 5) от регулярного обмена оперативно-розыскной информацией при организации и осуществлению 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 ОВД эффективно и результативно осуществлять предупреждение и противодействие уголовным правонарушениям в сфере киберпреступлений, которые готовятся или совершаются лицами молодого возраста.

Впрочем, поставленные вопросы не являются окончательно изученными и подлежат дальнейшему научному исследованию.

**Литература:**

1. Гуржій Г. С. Кіберзлочинність та відмивання коштів [Электронный ресурс] / Г. С. Гуржій. – Режим доступа: http://www.minfin.gov.ua/file/link/396800/file/tipolog2013.pdf.

2. Информационное агентство УНИАН [Электронный ресурс]. – Режим доступа: http://economics.unian.net.

3. Лук'яненко С. О. Аспекти систематизації злочинів в кредитно-фінансовій сфері / С. О. Лук'яненко // Проблеми кодифікації законодавства України : матеріали наук.-практ. конф. – К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2003. – С. 214–216.

4. Шорохова Г. М. Детермінація вчинення кіберзлочинів неповнолітніми сучасні напрями профілактики та актуальні проблеми розслідування злочинів, що вчиняються неповнолітніми : матеріали наук.-практ. семінару (м. Харків, 16 квіт. 2010 р.) / Г. М. Шорохова. – Х. : Вид-во Харк. нац. ун-ту внутр. справ, 2010. – С. 127.

5. Вехов В. Б. Компьютерные преступления. Способы совершения, методики раследования / В. Б. Вехов. – М. : Право и закон, 1996. – 182 с.

6. Соколов А. В. Защита от компьютерного терроризма : справ. пособие / А. В. Соколов, О. М. Степанюк. – СПб. : Арлит, 2002. – 496 с.

7. Малыгин С. С. Основы оперативно-розыскной деятельности : курс лекций / С. С. Малыгин, А. Е. Чечетин. – Екатеринбург : Изд-во Уральск. юрид. ин-та МВД России, 2001. – 306 с.

8. Юхно О. О. Діяльність транспортної міліції щодо попередження крадіжок приватного майна громадян на пасажирському залізничному транспорті : автореф. дис. … канд. юрид. наук : 12.00.08 / Олександр Олександрович Юхно. – Х., 2005. – 20 с.

9. Банкиры предлагают создать единую базу киберпреступлений для кибербезопасности [Электронный ресурс]. – Режим доступа: http:// http://iee.org.ua/ua/prog_info/23068/

10. Гуржій С. Г. Кіберзлочинність та відмивання коштів [Электронный ресурс]. / С. Г. Гуржій. – Режим доступа: http://cct.com.ua/2014/25.12.2013_157.htm

11. Кіберзлочинність [Электрон-ный ресурс]. – Режим доступа: http://itb.ucoz.ru/publ/kiberzlochinnist/9-1-0-208

12. Савчук Н. В. Кіберзлочинність: зміст і методи боротьби [Электронный ресурс] / Н. В. Савчук. – Режим доступа: http://tppe.econom.univ.kiev.ua/data/2009_19/zb19_48.pdf.

13. Кіберзлочинність набирає обертів [Электронный ресурс]. – Режим доступа: http://ua.golos.ua/social_problem/12_11_30_kiberprestupnost_v_ukraine_nabiraet_oborotyi

14. Шепетько С. А. Форми вчинення транснаціональними злочинними організаціями окремих злочинів за допомогою використання мережі Інтернет [Электронный ресурс] / С. А. Шепетько. – Режим доступа: http://journal-bzozik.com.ua/menus/view/1_322014#1.

# ПРОГНОЗИРОВАНИЕ, ПЛАНИРОВАНИЕ И ПРОГРАМИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ НА ОСНОВЕ ЗНАНИЙ ЕЕ РЕГИОНАЛЬНЫХ ОСОБЕННОСТЕЙ

**Андрей БАБЕНКО,**
кандидат юридических наук, доцент, профессор кафедры теории и истории государства и права
Одесского государственного университета внутренних дел, подполковник милиции

**SUMMARY**

The article investigates the problem of forecasting, planning and programming based on the knowledge of regional peculiarities crime. Systematized knowledge of the regional patterns of crime.

Allocated space and the importance of forecasting, planning and programming the system to of combating crime. Identified gaps in the current legislation to combat crime.

Proposed some ways to promoted more effective of combating crime in region based on new knowledge about the crime in the region.

**Key words:** forecasting, planning, programming, regional peculiarities crime , combating crime.

**РЕЗЮМЕ**

Статья посвящена исследованию проблем прогнозирования, планирования и програмирования на основе знаний региональных особенностей преступности. Систематизированы знания о региональных закономерностях преступности. Выделено место и значение прогнозирования, планирования и программирования в системе противодействия преступности. Выявлены пробелы в действующем законодательстве по противодействию преступности. Предложены пути повышения эффективности противодействия преступности в регионах на основе полученных новых знаний о преступности в регионах.

**Ключевые слова:** прогнозирование, планирование, програмирование, региональные особенности преступности, противодействие преступности.

**Постановка проблемы.** Следует признать, что традиционные способы изучения преступности, ее особенностей и закономерностей перестали удовлетворять потребности современного законодательства, теории и практики, о чем свидетельствует современное состояние преступности. Такой ситуации во многом способствует отставание действующего законодательства от количественно-качественных преобразований преступности. Особенно остро это находит свое проявление на региональном уровне, что в свою очередь существенно снижает контроль за происходящими социальными процессами, негативно влияет на эффективность прогнозирования, планирования и программирование последних, и как следствие, сказывается на противодействии преступности в стране и ее регионах. Представляется, что одним из перспективных направлений получения новых знаний о закономерностях преступности и повышения роли законодательного обеспечения правоохранительной деятельности является изучение преступности через призму ее региональных особенностей.

**Актуальность темы исследования** подтверждается результатами анализа статистических данных о преступности в Украине и данными криминологических исследований, которые свидетельствует о том, что доминирующей криминологической тенденцией на ближайшие годы