Розділ II. ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ ЗАСТОСУВАННЯ ЗАКОНОДАВСТВА

УДК 343.346.8:004

Н.В. Карчевский

ПРЕСТУПЛЕНИЕ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ: ОПРЕДЕЛЕНИЕ ПОНЯТИЯ

Робиться спроба визначити поняття "злочин в сфері інформаційних технологій", розглядати його в контексті запропонованих в науці кримінального права понять "комп'ютерний злочин", "кіберзлочин".

Ключові слова: *інформатизація, злочин в сфері використання інформаційних технологій, комп'ютерний злочин, кіберзлочин.*

Предпринимается попытка определить понятие "преступление в сфере использования информационных технологий", рассмотреть его в контексте предложенных в науке уголовного права понятий "компьютерное преступление", "киберпреступление".

Ключевые слова: *информатизация, преступление в сфере использования информационных технологий, компьютерное преступление, киберпреступление.*

Attempts to define the concept of "crime in sphere of use of information technology", to consider it in the context of the proposed science of criminal law concepts of "computer crime", "cybercrime".

Key words: *informatization, crime in sphere of use of information technology, computer crime, cybercrime.*

Расширение сферы применения компьютерной техники представляет собой закономерный результат роста информационной социальной потребности. Процессы информатизации и компьютеризации обеспечивают сегодня существенное увеличение возможностей человека, значительную интенсификацию деятельности предприятий учреждений и организаций. Вместе с тем, подчиняясь диалектическому закону, эти процессы не являются однозначными. Кроме положительных социальных трансформаций широкое распространение информационных технологий привело к появлению и развитию целого комплекса негативных последствий. Одним из них является так называемая киберпреступность.

Количественный и качественный рост киберпреступности прямо пропорционален успехам компьютерных технологий и расширению сферы их применения. Первые упоминания о компьютерной технике в

контексте нарушений уголовного законодательства относятся к 60-м годам прошлого столетия [8, С. 18]. В то время количество ЭВМ в мире исчислялось десятками тысяч (первая ЭВМ была построена в 1946 году). Преимущественно речь шла о физическом повреждении чрезвычайно дорогостоящих в то время электронно-вычислительных машин[5], а также совершении работниками крупных компаний (только такие могли позволить себе использование ЭВМ) хищений с помощью компьютеров[1, С. 10]. На территории бывшего СССР компьютерное преступление было впервые зарегистрировано в 1979 году в Вильнюсе. Оператор почтовой связи путем мошенничества с использованием автоматизированного программно-технического комплекса в течение двух лет совершала хищения денежных средств, направляемых соответствующими государственными органами гражданам в качестве пенсий и пособий по старости. Несовершенство программного обеспечения и наличие двойной бухгалтерии, ведущейся на различных (по форме представления информации) материальных носителях, позволили преступнице длительное время создавать излишки подотчетных денежных средств, изымать их из кассы и присваивать, а также уходить от ответственности[21]. Качественное изменение компьютерной преступности связано с развитием сетевых компьютерных технологий. К 1990 году большинство профессиональных пользователей компьютеров в США имели доступ к интернету, количество компьютеров, включённых в сеть, начало стремительно возрастать [2, С. 267]. Сегодня доступ к интернету имеет 34,3 % населения планеты [9], суммарные продажи персональных компьютеров и смартфонов в год оцениваются более чем в 2 миллиарда штук[3]. В таких условиях компьютерная преступность уже обосновано рассматривается как существенная угроза не только национального, но и международного уровня[11]. По мнению экспертов Организации по Безопасности и Сотрудничеству в Европе (ОБСЕ), преступность, связанная с использованием компьютерных систем и сетей, способна создать не меньший хаос, чем экономический кризис. Если в 2008 году вред, который ежегодно причиняет киберпреступность в мире, оценивался примерно в 100 млрд. долларов США[19], то по оценкам 2013 года этот показатель приблизился к одному триллиону[7].

Сказанное свидетельствует об актуальности проблем уголовно-правового регулирования в сфере информатизации. Одним ключевых вопросов здесь является определение понятий "преступление в сфере использования информационных технологий", "компьютерное преступление", "киберпреступление" и т.д. Попытка ответить на данный вопрос и является целью данной статьи.

Прежде всего уточним содержание понятия "преступление в сфере использования информационных технологий". Как отмечалось ранее,

обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин "информационная безопасность", ее структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. При этом социальная значимость отношений информационной безопасности, а следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность [18]. В свою очередь, информационная технология представляет собой организованную совокупность информационных процессов с использованием средств вычислительной техники, которые обеспечивают высокую скорость обработки данных, быстрый поиск информации, передачу данных, доступ к источникам информации независимо от места их расположения [18]. Таким образом, преступления в сфере использования информационных технологий, являясь одним из видов преступлений в сфере информационной безопасности, представляют собой *предусмотренные законодательством об уголовной ответственности, общественно опасные, виновные, совершенные субъектом преступления деяния, причиняющие вред обеспеченным средствами вычислительной техники отношениям в сфере реализации информационной потребности.* Анализ действующего УК позволяет прийти к выводу, что к таким преступлениям следует относить посягательства, предусмотренные *ч. ч. 11, 12 в. 158, ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 УК.*

Наряду с предлагаемым понятием ("преступление в сфере использования информационных технологий") в уголовно-правовом дискурсе достаточно активно используются следующие: "компьютерное преступление", "киберпреступление", "интернет-преступление" и т.д. Объем данных понятий определяется по-разному. Тем не менее, наиболее распространенным является отнесение к компьютерным преступлениям всех общественно опасных посягательств, при совершении которых компьютеры используются как технические средства[12, с. 11; 17, с. 14; 22, с. 243; 15, с. 35-40; 10, с. 72; 13, с. 65; 20, с. 87; 27, с. 55-57].

Появление термина "киберпреступление" связывают с расширением технической базы информатизации. В частности отмечается, что вследствие широкого распространения так называемых "коммуникаторов" и "смартфонов", сочетающих в себе свойства мобильных телефонов и компьютеров, термин "компьютерное" преступление в буквальном понимании, перестал охватывать весь спектр общественно опасных деяний в сфере применения информационных технологий. Это, по мнению неко-

торых исследователей, свидетельствует о необходимости введения в научный оборот термина "киберпреступление"[28, с. 32-33] В частности, Т.Л. Тропина предлагает определять киберпреступление как "виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству" [28, С. 38]. Здесь следует обратить внимание на то, что нормативные определения определения вычислительной машины и электронно-вычислительной машины не позволяют толковать понятие "компьютер" настолько ограничительно [26; 25]. Понятием ЭВМ полностью охватываются как современные устройства мобильной связи так и любые другие устройства, представляющие собой "совокупность технических средств, создающую возможность проведения обработки информации и получение результата в необходимой форме, основные функциональные устройства которой выполнены на электронных компонентах" [26]. Таким образом, понятия "компьютерное преступление" и "киберпреступление"[1] можно рассматривать как тождественные.

Данный вывод подтверждается и анализом зарубежных источников. Так, на Десятом конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (Вена, апрель 2000 года) киберпреступления рассматривались как любые преступления, которые могут совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. При этом отмечалось, что существуют две категории киберпреступлений:

a) киберпреступление в узком смысле ("компьютерное преступление"): любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

b) киберпреступление в широком смысле ("преступление, связанное с использованием компьютеров"): любое противоправное деяние, совер-

[1] Необходимо отметить, что в науке также высказывались предложения понимать под киберпреступлениями преступления, совершаемых в так называемом "киберпространстве". Следует отметить, что применение категории "киберпространство" в уголовно-правовом контексте, тем более на уровне определений, нам представляется нецелесообразным. Очевидно, что определяемая им информационная среда не может рассматриваться как вид некоего пространства, территории в классическом юридическом смысле. Поэтому, попытка описывать при помощи данного термина новый вид преступлений или особенности юрисдикции скорее всего не будет результативной, создаст путаницу, лишние терминологические и концептуальные сложности.

шаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети [23].

Изложенный подход используется и на уровне научных исследований [6]. Yvonne Jewkes определяет киберпреступления (cybercrimes) как противоправные деяния совершенные с использованием или посредством компьютеров, компьютерных сетей, Интернет, сетевых информационных или коммуникационных технологий [4]. Susann W. Brenner рассматривает три категории киберпреступлений: преступления, в которых компьютер является целью преступления, преступления в которых компьютер используется в качестве средства совершения преступления, а также преступления, в которых компьютер играет незначительную роль в совершении преступления (crimes in which a computer plays an incidental role in the commission of the offense). В качестве примера преступлений третей группы автор приводит преступление, совершенное Melanie McGuire. В 2007 году последняя была осуждена за убийство мужа. По данным прокуратуры, обвиняемая использовала сильнодействующее снотворное чтобы усыпить потерпевшего, несколько раз выстрелила в него, расчленила труп и скрыла останки в водоеме. После обнаружения останков, работники полиции обнаружили в компьютере обвиняемой следы, свидетельствующие об осуществлении поиска в интернет по темам "совершение убийства", "незаконное приобретение оружия", "яды". Также была обнаружена электронная переписка ("romantic e-mails") обвиняемой и ее начальника. В ходе судебного рассмотрения дела прокуроры использовали "компьютерные доказательства" для обоснования того, что у обвиняемой был мотив для убийства мужа, и ею исследовались методы совершения убийства, в том числе методы, использованные при совершении преступления [1].

В целом, приведенное определение киберпреступлений является практически общепризнанным в зарубежной научной литературе, а также достаточно широко представлено в отечественной. Тут необходимо отметить, что зарубежный опыт несомненно должен изучаться и быть использованным. В тоже время, безоглядный перенос западных стандартов регулирования политических, экономических и социальных процессов без учета исторических и национальных особенностей далеко не всегда приводит к положительным результатам. Представляется, что в случае с определением компьютерных преступлений и использованием данного понятия в отечественном уголовно-правовом дискурсе имеет место как раз такая ситуация.

При описанном понимании, любое преступление, совершенное с использованием компьютерной техники (мошенничество, шпионаж, незаконное распространение наркотических средств и т.д.), должно счи-

таться компьютерным. Хотя абсолютно очевидно, что вышеперечисленные общественно опасные деяния не являются преступлениями нового вида. Такие действия, несмотря на использование для их совершения компьютерной техники, остаются государственной изменой, шпионажем, кражей, мошенничеством, незаконным сбором сведений, которые составляют коммерческую тайну и т.д. Средство не меняет сути преступления. Недостатком данного подхода является его несоответствие основному принципу структурирования национального законодательства об уголовной ответственности – систематизации уголовных законов на основе классификации посягательств по объекту. Определение новой группы преступлений всегда должно производиться на основе признаков, характеризующих объект посягательства. Именно поэтому в пределах национального уголовно-правового дискурса необоснованным следует считать определение группы преступлений на основе признаков, характеризующих способ, орудие или средство посягательства. Об этом достаточно красноречиво свидетельствует приведенный ранее пример отнесения к числу киберперступлений конкретного умышленного убийства на том основании, что получение доказательств осуществлялось путем исследования компьютера обвиняемой.

Уместным будет и следующий пример. Как известно, изготовление поддельных денежных купюр с помощью современных печатающих устройств, несмотря на повышение общественной опасности, не изменило квалификации этих действий: виновные привлекались и продолжают привлекаться к уголовной ответственности по статьям о фальшивомонетничестве, так же как и те, кто использовал для подделки фототехнику или обычные карандаши, краски и лезвие бритвы. Компьютерная техника позволяет до совершенства довести процесс изготовления поддельных документов: перенесенные с оригинала печати, подписи, другие реквизиты практически идентичны. Для установления подделки будет необходимо проведение высококвалифицированной криминалистической экспертизы, но это не означает, что такого рода подделки документов требуют особой, отличной от существующей квалификации. Вывод может быть только один: модификация орудий и средств совершения преступления, использование с этой целью достижений научно-технического прогресса не меняет тех отношений, на которые оно посягает, не свидетельствует о появлении преступлений нового вида.

Сказанное вовсе не означает, что расширение сферы применения компьютерных технологий не привело к появлению преступлений нового вида, как, например, считает Ю. Батурин. По его мнению, компьютерных преступлений как особой группы преступлений в юридическом смысле не существует. Несомненная модификация традиционных преступлений позволяет говорить лишь о компьютерных аспектах преступлений, не

выделяя их в обособленную группу [12]. С такой позицией трудно согласиться, далеко не всегда общественно опасное посягательство, совершенное с использованием компьютерной техники, можно рассматривать как традиционное преступление, усложненное применением новых средств. Как быть, например, с квалификацией распределенной атаки отказа от обслуживания, совершенной с использованием бот-сети? В терминах какого из традиционных преступлений можно описать незаконные множественные рассылки электронных сообщений (спам)?

Вместе с тем, следует признать, что определение компьютерных преступлений как группы посягательств, характеризующейся общими признаками способа, орудия или средства, может быть востребовано. Речь идет об установлении особенностей методики раскрытия или расследования преступлений, специфики фиксации следов и т.д. Можно частично согласиться с В.В. Веховым, который предлагает давать различные определения компьютерных преступлений с точки зрения уголовно-правовой охраны и с точки зрения криминалистической. Очевидно, что именно последнюю группу можно определять как деяния, в которых компьютер является предметом, орудием или средством совершения преступления. Такая группа безусловно имеет значение для криминалистики. Однако применять такой же термин, но с другим определением в уголовном праве представляется ошибочным. Использование термина, имеющего скорее криминалистическое значение, в пределах уголовно-правового дискурса приведет к путанице и неопределенности. Данный подход обусловит сложности в четком определении предметов соответствующих научных исследований.

Кроме того, одной из очевидных тенденций современной преступности является рост числа традиционных преступлений, совершаемых с использованием компьютерной техники. Так, например, исследование, проведенное в Великобритании, показало, что четыре из пяти ограблений совершаются при помощи Twitter и Facebook [29]. В таких условиях, использование критикуемого подхода приведет к искажению и утрате информативности данных официальной статистики. Группа "компьютерные преступления" будет разрастаться, складываться из самых разнообразных посягательств (от блокирования сайтов организаций до торговли оружием и наркотиками). В конце концов, подобные статистические данные потеряют актуальность для решения задач противодействия преступности.

Таким образом, уместное в пределах зарубежного уголовно-правового дискурса определение компьютерных преступлений имеет весьма ограниченную ценность для национальной науки уголовного права. Как известно, в зарубежной уголовно-правовой доктрине материально-правовые проблемы рассматриваются в неразрывной связи с процессуальны-

ми. В таких условиях критикуемый подход к определению компьютерных преступлений имеет смысл и несомненно оправдан. В свою очередь, попытка исследования проблем национального уголовно-правового отражения тенденций информатизации на основе такого же подхода, как представляется, не имеет перспективы.

Понятия "компьютерное преступление" и "киберпреступление", в общепризнанном понимании, могут быть эффективно использованы при проведении криминологических, уголовно-процессуальных, криминалистических[1] исследований. Что же касается национального уголовно-правового дискурса, то здесь их применение следует ограничить, и использовать предложенное понятие "преступление в сфере использования информационных технологий".

Использованная литература:

1. Brenner S. Cybercrime : criminal threats from cyberspace / Susan W. Brenner. – Praeger, 2006. – 281 p.

2. Campbell-Kelly M., Aspray W. Computer: A History Of The Information Machine [Second Edition] / Martin Campbell-Kelly, William Aspray. - Westview Press : 2004. – 325 p.

3. Gartner: Планшеты и смартфоны продолжают вытеснять настольные компьютеры [Электронный ресурс] // Новости сайта "Открытые системы". - 25.06.2013. – Режим доступа : http://www.osp.ru/news/2013/0625/13019543/

4. Jewkes Y. Cybercrimes / Yvonne Jewkes // The Sage Dictionary of Criminology. Compiled and edited by Eugene McLaughlin, John Muncie. Third Edition. - Sage Publications, 2013. – 536 p.

5. Kabay M. E. A Brief History of Computer Crime: An Introduction for Students [Electronic resourse] / M. E. Kabay // Personal Site of M. E. Kabay, PhD – Mode of access: www.mekabay.com/overviews/history.pdf

6. Leukfeldt R., Veenstra S., Stol W. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands [Electronic resource]/ Rutger Leukfeldt, Sander Veenstra, Wouter Stol // International Journal of Cyber Criminology. Vol. 7 Issue 1 January - June 2013. – Mode of access: http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf

[1] Примечательно, что в отчественной юридической науке термин "компьютерные преступления" первоначально применялся именно в криминалистическом контексте. В марте 1993 года в НИИ проблем укрепления законности и правопорядка при Генеральной прокуратуре РФ на заседании межведомственного семинара на тему "Криминалистика и компьютерная преступность" было отмечено, что термин компьютерная преступность, уже воспринятый как отечественной, так и зарубежной литературой, имеет право на существование. Компьютерными преступлениями предлагалось именовать те предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства [24, с.37; приводится по: 14, с. 167].

7. Lewis A., Baker S. The Economic Impact of Cybercrime and Cyber Espionage. Report, July 2013 [Electronic resourse] / James Andrew Lewis, Stewart Baker // Center for Strategic and International Studies (CSIS). – Mode of access: http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage

8. Sieber U. Legal Aspects of Computer-Related Crime in the Information Society / Ulrich Sieber. - Brussels, Belgium : European Commission, 1998. – 239 p.

9. World Internet Users and Population Stats [Electronic resource] // Internet World Stats. – Mode of access : http://www.internetworldstats.com/stats.htm

10. Азаров Д. С. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. С. Азаров // Право України. – 2000. – № 12. – С. 69–73.

11. Антонов С. Компьютерные преступления в банковской сфере / С. Антонов // Юридическая практика. – 1997. – № 8. – С. 7.

12. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юридическая литература, 1991. – 157 с.

13. Біленчук П. Д. Комп'ютерна злочинність : навчальний посібник / Петро Дмитрович Біленчук, Володимир Васильович Бут, Владислав Данилович Гавловський, Михайло Васильович Гуцалюк, Руслан Леонідович Колпак. – К. : Атіка, 2002. – 240 с.

14. Геллер А.В. Уголовно-правлвые и криминологические аспекты обеспечения защиты электронной информации и Интернета : Дис. ... канд. юрид. наук : 12.00.08. Москва, 2006. – 219 с.

15. Голубєв В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.

16. Закон України "Про національну програму інформатизації" від 04.02.1998 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua-/cgi-bin/laws/main.cgi?nreg=74%2F98-%E2%F0.

17. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... доктора юрид. наук: 12.00.02 / Ростислав Андрійович Калюжний. – К., 1992. – 47 с.

18. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

19. Киберпреступность страшнее финансового кризиса [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 03.12.2008. – Режим доступа : http://www.crime-research.ru/news/03.12.2008/5056/.

20. Лісовий В. "Комп'ютерні" злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.

21. Манифест и история [Электронный ресурс] // Отдел "К" при ГУВД Воронежской области. – Режим доступа : http://k-vrn.ru/pages/about

22. Правовая информатика и кибернетика : учебник / Г.А. Атанесян, О.А. Гаврилов, П. Дёри, А. Г. Каблуков, А. К. Караханьян, И. Ковачич, К. Ко-

вачичне, В. В. Крылов, А. Малиновский, М. Г. Мальковский, Г. О. Матюшкин, Я. Петцель, Н. С. Полевой, Л. Д. Самыгин, Д. Д. Хан-Магомедов, И. Ханец, С.И. Цветков, Н. П. Яблоков ; [под ред. Н. С. Полевого]. – М. : Юридическая литература, 1993. – 528 с.

23. Преступления, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума. Десятый конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Вена, 10-17 апреля 2000 года [Электронный ресурс] // United Nations Crime and Justice Information Network. – Режим доступа: http://www.uncjin.org/Documents/congr10/10r.pdf

24. Селиванов Н. Проблемы борьбы с комньютерной нреступностью // Законность. – 1993. – N° 8. – С.37.

25. Системи оброблення інформації. Основні положення. Терміни та визначення : ДСТУ 2938-94. – [Чинний від 1996-01-01].– К. : Держспоживстандарт України, 1996. – 20 с.

26. Системы обработки информации. Термины и определения. – ГОСТ 15971-90. – Дата введения 01.01.92

27. Супруненко А.М. Кіберзлочинність як особливий вид протиправної діяльності / А.М. Супруненко, М.С. Гожий // Боротьба з інтернет-злочинністю : матеріали міжнародної науково-практичної конференції (м. Донецьк, 12-13 червня 2013 р.). – Донецьк : ДЮІ МВС України, 2013. – С. 55–57.

28. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : Дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2005. – 235 с.

29. Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // NB: Национальная безопасность. – 2013. – № 2. – С.160-181. DOI: 10.7256/2306-0417.2013.2.608. URL: http://e-notabene.ru/nb/article_608.html.

УДК 343.982.33

В.В. Бірюков

ВИЗНАЧЕННЯ ДИСТАНЦІЇ ПОСТРІЛУ І МІСЦЯ, ЗВІДКИ ЙОГО БУЛО ЗДІЙСНЕНО, ЗА СЛІДАМИ НА МІСЦІ ПОДІЇ

В статті розглянуто питання пошуку слідів застосування вогнепальної зброї, встановлення дистанції пострілу, та напрямку і місця звідки його було здійснено. Виділено три зони близького пострілу, розглянуто характер слідоутворення, в залежності від куту зустрічі кулі з перешкодою, а також ефект Виноградова при пострілі з далекої відстані.

Ключові слова: *огляд місця події, вогнепальна зброя, дистанція пострілу, сліди пострілу, візування, ефект Виноградова, рановий канал.*

В статье рассмотрены вопросы поиска следов применения огнестрельного оружия, установления дистанции выстрела, направления и места откуда он