Universitatea Tehnică a Moldovei

ANALIZA INSTRUMENTELOR DIGITALE UTILIZATE LA INVESTIGAREA INFRACȚIUNILOR INFORMATICE

Masterand:

Belicenco Ivan

Conducător:

lector universitar Catanoi Maxim

Chişinău 2020

Ministerul Educației, Culturii și Cercetării
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică și Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susținere
Șef departament:
dr.conf.univ. Ion Fiodorov.
„24" decembrie 2019

ANALIZA INSTRUMENTELOR DIGITALE UTILIZATE LA INVESTIGAREA INFRACȚIUNILOR INFORMATICE

Teză de master în Securitate Informațională

Masterand: (Belicenco Ivan)
Conducător (Catanoi Maxim)

Chișinău 2020

Rezumat

Prezenta lucrare cu tema:"**Analiza instrumentelor digitale ce pot fi utilizate la investigarea infracţiunilor informatice**" are menirea de a prezenta date cu privire la analiza instrumentelor digitale utilizate la investigarea infracțiunilor informatice. Prin studiul de faţă tindem să contribuim la micşorarea numărului de infracţiuni informatice şi investigarea calitativă a acestora.

Teza de master este structurată în: întroducere, trei capitole, concluzie şi referinţe biografice.

Întroducerea reprezintă o generalizare a pericolului infracţiunilor informatice, a instrumentelor digitale și a tehnicilor de utilizare a acestora, precum şi noţiuni introductive privind fenomenuzl cercetat. S-a scos în evidenţă actualitatea temei precum şi problema respectivei cercetări. La fel s-a stabilit care este obiectul de bază al cercetării şi nu în ultimul rînd s-a stabilit care este baza metodologică.

Capitolul I este întitulat **Conceptul, aspecte generale şi juridice a infracţiunilor informatice în Republica Moldova**. Este compus din două puncte: 1) Conceptul şi clasificarea infracţiunilor informatice; 2) Aspecte generale şi juridice a infracţiunilor informatice în Republica Moldova. În cadrul acestui capitol autorul abordează esenţa acestor fenomene, elementele sale conceptuale, precum şi reglementarea legală.

Capitolul II este întitulat **Clasificarea, tehnici de investigare a infracţiunilor informatice:** 1) Tehnici de investigare a infracţiunilor informatice, 2) Clasificarea şi tehnicile instrumentelor de investigare digitală a infracţiunilor informatice. 3) Probleme şi dificultăţi ce apar în cadrul utilizării instrumentelor de investigare digitală. În cadrul acestui capitol se supun tratării esenţa şi specificul tehnicilor de investigare, genul instrumentelor utilizate, dificultăţilor ce pot fi utilizate în cadrul investigaţiilor.

Capitolul III este întitulat **Teoria și practica utilizării instrumentelor de investigare digitală:** 1) Instrumente digitale utilizate la investigarea infracţiunilor informatice, 2) Teoria şi practica utilizării instrumentelor de investigare digitală FTK Imager şi Autospy. 3)Teoria şi practica utilizării instrumentului digital browsinghistoryview

Concluzia reprezintă o analiză a celor expuse în teza dată precum şi unele recomandări pentru funcţionarea şi colaborarea cît mai eficientă a organelor de drept.

Abstract

The present paper with the theme: "**Analysis of digital tools that can be used in the investigation of cybercrimes**" is intended to present data on the analysis of digital tools used in cybercrime investigation. Through this study we tend to contribute to the decrease of the number of computer crimes and their qualitative investigation.

The master's thesis is structured in: introduction, three chapters, conclusion and biographical references.

The introduction represents a generalization of the danger of cybercrimes, of digital instruments and their techniques of use, as well as introductory notions regarding the phenomenon investigated. The topicality of the topic as well as the problem of the respective research was highlighted. It was also established what is the basic object of the research and not lastly it was established what is the methodological basis.

Chapter I is entitled **The Concept, General and Legal Aspects of Computer Crimes in the Republic of Moldova**. It consists of two points: 1) The concept and classification of cybercrimes; 2) General and legal aspects of computer crimes in the Republic of Moldova. In this chapter the author addresses the essence of these phenomena, his conceptual elements, as well as the legal regulation.

Chapter II is entitled **Classification, techniques of investigation of cybercrimes**: 1) Techniques of cybercrime investigation, 2) Classification and techniques of digital cybercrime investigation tools. 3) Problems and difficulties that arise when using digital investigation tools. Within this chapter, the essence and specificity of the investigation techniques, the kind of instruments used, the difficulties that can be used in the investigations are subject to treatment.

Chapter III is entitled **Theory and practice of using digital investigation tools**: 1) Digital tools used in the investigation of cybercrimes, 2) The theory and practice of using digital investigation tools FTK Imager and Autospy. 3) Theory and practice of using the digital browsinghistoryview tool

The conclusion represents an analysis of the ones presented in the thesis as well as some recommendations for the most efficient functioning and collaboration of the law enforcement bodies.

CUPRINS

LISTA ABREVIERILOR.....8
INTRODUCERE.....10
Capitolul I. CONCEPTUL, ASPECTE GENERALE ȘI JURIDICE A INFRACȚIUNILOR INFORMATICE ÎN REPUBLICA MOLDOVA.....12
1.1.Conceptul şi clasificarea infracțiunilor informatice.....12
1.2.Aspecte generale și juridice a infracțiunilor informatice în Republica Moldova.....14
Capitolul II. CLASIFICAREA, TEHNICI DE INVESTIGARE A INFRACȚIUNILOR INFORMATICE.....19
2.1.Tehnici de investigare a infracțiunilor informatice.....19
2.2.Genul și clasificarea intrumentelor de investigare digitală a infracțiunilor informatice.....37
2.3.Probleme şi dificultăţi ce apar în cadrul utilizării instrumentelor de investigare digitală.....40
Capitolul III. TEORIA ȘI PRACTICA UTILIZĂRII INSTRUMENTELOR DE INVESTIGARE DIGITALĂ.....44
3.1.Instrumente digitale utilizate la investigarea infracțiunilor informatice.....44
3.2.Teoria şi practica utilizării instrumentelor digitale FTK Imager și Autospy.....47
3.3.Teoria şi practica utilizării instrumentului digital BrowsingHistoryView.....57
CONCLUZII.....62
BIBLIOGRAFIE.....63
ANEXE.....67

LISTA ABREVIERILOR

CP - Cod Penal

CE - Consiliul Europei

IT - Tehnologia Informațională

SUA - Statele Unite ale Americii

BSA - Business Software Alliance

CEDO - Curtea Europeană a Drepturilor Omului

SOPA - Stop Online Piracy Act (Legea Opriţi Pirateria Online)

PIPA - Protect IP Act (Legea pentru Protecţia IP-ului)

ACTA - Anti-Counterfeiting Trade Agreement (Tratatul Comercial Anti-Contrafacere)

IMSI - International Mobile Subscriber Identity

SIM - Subscriber Identification Module

RBS - Radio Base Station

IBM - International Business Machines

UPS - Uninterruptible Power Supply

CD-ROM - Compact Disc Read-Only Memory

IRC - Internet Relay Chat

ICQ - I Seek You

IP - Internet Protocol

UT - Universal Time

GMT - Greenwich Mean Time

EST - Eastern Standard Time

EDT - Eastern Daylight Time

CST - Central Standard Time

CDT - Central Daylight Time

PST - Pacific Standard Time

PDT - Pacific Daylight Time

ISP - Internet Service Provider (furnizor de servicii internet)

WLAN - Wireless Local Area Network

LAN - Local Area Network

SPSS - Statistical Package for the Social Sciences

GPS - Global Positioning System

CCTV - Closed Circuit Television

NVF - Network Dunctions Virtualizatio

NMAP - Network Mapper

HTML - HyperText Markup Language

RAM - Random Access Memory

GeoIP – Geolocation Internet Protocol

URL - Uniform Resource Locator

HEX - H exadecimal

MD5 - Message Digest 5

SHA1 - Secure Hash Algorithm

USB - Universal Serial Bus (Magistrală Serială Universală)

XML - eXtensible Markup Language

CSV - Comma-Separated Values

TSV - Tab Separated Values

TCP - Transmission Control Protocol

DNS - Domain Name System – sistem de nume de domeniu

OpenSSL - Secure Sockets Layer

RID - Relative ID

hash LM / NT - LAN Manager

CD - Compact Disc

DVD - Digital Versatile Disc

PC - Personal Computer

INTRODUCERE

Spaţiul virtual este o componentă importantă în societatea informaţională, ca parte a societăţii umane, generând o criminalitatea aparte, specifică. In mod categoric însă, serviciile oferite de lumea virtuală, de internet, ajută foarte mult cercetarea ştiinţifică şi deopotrivă relaţiile interumane precum şi afacerile.

Prin intermediul computerelor se tranzacţionează o cantitate uriaşă de informaţii, informaţii, care atât în procesul transmiterii dar şi cel al stocării lor sunt deosebit de vulnerabile, putând fi deseori compromise. Datorită vulnerabilităţii sistemelor computerizate, infracţiunile informatice pot să producă efecte dintre cele mai diverse şi mai grave. Criminalitatea informatică este un tip nou de criminalitate ce ameninţă piaţa bursieră, conturile bancare, mediul de afaceri şi chiar securitatea statelor. Criminalii specializaţi în tehnologia informaticii au posibilitatea să producă fraude enorme, să sustragă date confidenţiale prin intrarea în fişierele secrete ale oamenilor de afaceri, corporaţiilor, diferitelor instituţii şi organizaţii, etc.

Reprezentând un univers nou cu o criminalitate specifică, internetul este o armă cu ajutorul căreia se pot săvârşi cele mai diverse delicte: pornografie, hărţuire sexuală, lansare de viruşi, transferuri financiare ilegale, furturi de cărţi de credit, furturi intelectuale, achiziţii ilegale de bunuri, furturi de jocuri de la companiile producătoare, manipularea opiniei publice, piraterie aviatică, ameninţări şi atacuri teroriste, etc.

Ştiinţa şi tehnica, care a dat posibilitate de a folosi sau chiar a procura calculatoare, lap-topuri etc., simplitatea şi accesibilitatea surselor de instruirev în domeniu contribuie la faptul că numărul infracţiunilor în domeniul informaticii să fie în creştere, vizavi de faptul că infracţiunilr de acest tip să fie tot mai greu de depistat şi investigat.

Mărimea pagubei aduse societăţii este şi ea în creştere, atât ţinând seama de genul, rata, caracterul infracţiunilor în domeniul informaticii în R-Moldova ţi regiunea limitrofă şi pe plan internaţional.

Actualitatea temei: Dezvoltarea social-economică şi atingerea noii situaţii în toate sferele vieţii Republicii Moldova şi altor ţări este imposibil de efectuat fără o luptă activă cu criminalitatea, inclusiv cu cea digitală.

Investigarea infracţiunilor în domeniul informaticii ca parte integrantă a organelor de drept trebuie să corespundă cerinţelor perioadei contemporane – intercalare strânsă a ştiinţei şi practicii.

Lupta cu „infractorii digitali” va contribui la crearea statului pe care toţi îl dorim, - stat de drept. Crearea statului de drept înseamnă lichidarea încălcărilor de drept, anihilarea criminalităţii, înlăturarea tuturor cauzelor care duc la apariţia criminalităţii. În aşa stat nu trebuie să fie loc pentru încălcările de drept sau legi şi alte acte subordonate lor.

Pentru îndeplinirea scopului de înlăturare a încălcărilor de drept şi lichidarea criminalităţii în ţara noastră este necesar permanent de perfecţionat metodele de descoperire a infracţiunii şi pe cît posibil de repede de a le încadra în practica organelor de drept. Numai cu folosirea completă a datelor referitoare la cercetarea infracţiunilor în domeniul informaticii, a instrumentariului, tehnicilor inclusiv datelor celor mai recente, se va putea preîntâmpina, descoperi şi contribui la scăderea numărului de infracţiuni în acest domeniu.

Problema cercetării. Determinarea instrumentelor digitale utilizate, tehnicilor de aplicare a instrumentelor de investigare digitală.

Scopul cercetării: îl constituie studierea instrumentele digitale utilizate la cercetarea infracţiunilor în domeniul infformaticii.

Obiectul cercetării: caracteristica instrumentelor digitale şi tehnicilor utilizate la aplicarea lor, problematica existentă în acest domeniu.

Obiectivele cercetării:

- determinarea conceptului şi clasificarea infracţiunilor informatice;
- tehnicile de investigare a infracţiunilor informatice;
- instrumentele de investigare digitală a infracţiunilor informatice;
- cercetarea aprofundată a teoriei şi practicii de utilizare a unor instrumente de investigare digitală - FTK Imager, Autospy şi BrowsingHistoryView.

Baza metodologică: Apărarea valorilor sociale şi depistarea, cercetarea, preîntâmpinarea infracţiunilor ca cea mai importantă direcţie a activităţii de apărare a legalităţii trebuie să se efectueze la un nivel înalt ştiinţific, tehnic şi profesional.

La efectuarea acestei teze de master am apelat la diverse manuale, monografii a autorilor atât din Republica Moldova cît şi de peste hotare, precum şi la Codul penal al Republicii Moldova.

Metodele şi procedeele de lucru aplicate la efectuarea lucrării au fost cele mai variate. Am început cu studierea lucrărilor existente în acest domeniu, aplicând metoda analizei. Metodele comparative şi experimentale la fel au fost aplicate.

CONCLUZII

Prezenta teză fost încercarea mea de a aduce la cunoştinţa a unor metode și tehnici de investigare a infracțiunilor informatice, adică despre tendinţa de dezvoltare, prin conturarea diferitor modalităţi de investigare a infracțiunilor informatice care sunt dificil de investigat.

În urma efectuării studiul fenomenului infracțiunilor informatice, consultării părerilor şi concepţiilor diferitor specialişti în domeniu, am constatat că printre cele mai relevante semne caracteristice ale infracțiunilor informatice sunt: legătura cu alte genuri de infracțiuni, caracterul tehnologic avansat, nivelul înalt de latență, caracterul bine organizat, profesional, transfrontalier și transnațional, aceste infracțiuni fiind cele mai dinamice în evoluție, având costuri reduse pentru săvârșire și manifestând trăsături politice, extremiste și teroriste.

Infractorii digitali sunt persoane cu o flexibilitate înaltă de trecere operativă de la dimensiunea reală la cea virtuală, de la o relație mediată de un spațiu emotiv fizic la o relație mediată de un spațiu emotiv artificial, având o percepție diminuată asupra ilegalității comportamentului lor, daunei provocate, a riscurilor de a fi descoperit și sancționat.

În această lucrare de cercetare am menționat despre diferitele tipuri de instrumente criminalistice care pot fi utilizate pentru soluționarea crimelor digitale.

În unele cazuri, instrumentele sunt bazate pe software, dar uneori, hardware-ul trebuie, de asemenea, să obțină dovezi.

Unele dintre programele software sunt disponibile în mod liber și unele software-uri sunt plătite. Software-urile disponibile în mod liber sunt, de asemenea, cunoscute ca instrumente Open Source. O listă completă a acestor instrumente cu link-ul lor de descărcare, de utilizare și platforme precum Windows, UNIX, Linux, DOS și MAC etc. Instrumentele plătite sunt, de asemenea, cunoscute ca instrumente sursă închisă sau instrumente de proprietate. Aceste instrumente au mai multe caracteristici comparativ cu open source instrumente și sunt foarte scumpe. Lista de instrumente menționate este un efort de a arunca o privire asupra instrumentelor existente care poate fi utilă în domeniul criminalisticilor digitale.

BIBLIOGRAFIE

1. Legea telecomunicațiilor. Nr.520 din 07.07.1995. Abrogată prin Legea nr.241 din 15.11.2007. În: Monitorul Oficial al Republicii Moldova, 14.03.2008, nr.51-54.
2. Legea cu privire la informatică. Nr.1069 din 22.06.2000. În: Monitorul Oficial al Republicii Moldova, 05.07.2001, nr. 73-74/547.
3. Legea cu privire la informatică. Nr.1069 din 22.06.2000. În: Monitorul Oficial al Republicii Moldova, 05.07.2001, nr. 73-74/547.
4. Convenția Consiliului Europei cu privire la criminalitatea informatică, adoptată la 23.11.2001 în Budapesta. https://goo.gl/uuJpqb (vizitat 21.03.2017).
5. Legea privind prevenirea şi combaterea criminalităţii informatice. Nr.20 din 03.02.2009. În: Monitorul Oficial al Republicii Moldova, 26.01.2010, nr. 11-12/17.
6. Protocol adițional la Convenția CE privind criminalitatea informatică. 2003. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189 (vizitat 21.03.2017).
7. Moise A. C. Metodologia investigării criminalistice a infracțiunilor informatice. București: Universul Juridic, 2011
8. http://mihaelabejenari.wordpress.com/criminalitatea-fara-violenta-fraudele-informatice/ „Criminalitatea fara violenta – fraudele informatice";
9. http://itmoldova.com/2010/09/09/procuratura-generala-a-r-moldova-va-investiga-in-premiera-cazurile-decriminalitate-informatica/ „Procuratura Generală a R. Moldova va investiga în premieră cazurile de criminalitate informatică";
10. http://www.infoeuropa.md/criminalitatea-informatica/ „Criminalitatea informatică";
11. Art. 1 din Legea Nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice, publicat in Monitorul Oficial Nr. 11-12 la 26.01.2010;
12. Codul penal al Republicii Moldova din 18.04.2002 cu completările şi modificările ulterioare;
13. http://ipn.md/ro/societate/57617 " Interzicea unor siteuri pe teritoriul Republicii Moldova va duce la migraţia acestora", articol publicat la 18 octombrie 2013;
14. http://unimedia.info/stiri/procuratura-vrea-sa-oblige-providerii-de-internet-sa-blocheze-site-urile-incomode66610.html „Procuratura vrea să oblige providerii de Internet să blocheze site-urile incomode", articol publicat la 08 octombrie 2013;
15. http://unimedia.info/stiri/dovada-proiectul-de-lege-privind-cenzura-internetului-contravine-mai-multor-standardeeuropene-67004.html „Dovada! Proiectul de lege privind cenzura Internetului contravine mai multor standarde europene", articol publicat la 17 octombrie 2013;

16. Flori BOȘTINĂ, Analiza fraudelor privind licitațiile fictive, [citat 2019-09-15]. Disponibil pe Internet:http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fraudelor-privind-licitatiile-fictive/
17. Flori BOȘTINĂ, Analiza fraudelor privind mijloacele de plată electronică, [citat 2019-09-17]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fraudelor-privind-mijloacele-de-plata-electronica/
18. Flori BOȘTINĂ, Analiza fraudelor din domeniul telecomunicațiilor, [citat 2019-09-19]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fraudelor-din-domeniul-telecomunicatiilor/
19. Flori BOȘTINĂ, Analiza programelor malițioase și a virușilor informatici, [citat 2019-09-21]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-programelor-malitioase-si-a-virusilor-informatici/
20. FABRI Norbert, Analiza probelor digitale, [citat 2019-09-23]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-probelor-digitale/
21. FABRI Norbert, Prelevarea probelor digitale, [citat 2019-09-23]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/prelevarea-probelor-digitale/
22. Răzvan-Ionuţ MARIN, Analizarea mediilor de stocare indisponibilizate, [citat 2019-09-27]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analizarea-mediilor-de-stocare-indisponibilizate/
23. Răzvan-Ionuţ MARIN, Analiza fișierelor temporare, [citat 2019-09-27]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fisierelor-temporare/
24. Răzvan-Ionuţ MARIN, Analiza grupurilor de discuții (News Groups-Usenet), [citat 2019-09-29]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-grupurilor-de-discutii-news-groups-usenet/
25. Răzvan-Ionuţ MARIN, Analiza IRC (Internet Relay Chat), [citat 2019-09-27]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-irc-internet-relay-chat/
26. Răzvan-Ionuţ MARIN, Analiza paginilor de web și a fișierelor generate de activitatea pe Internet a suspectului, [citat 2019-10-09]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-paginilor-de-web-si-a-fisierelor-generate-de-activitatea-pe-internet-a-suspectului/
27. Răzvan-Ionuţ MARIN, Analiza fișierelor jurnal (log-uri), [citat 2019-10-19]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-fisierelor-jurnal-log-uri/
28. Răzvan-Ionuţ MARIN, Analiza e-mail-urilor și transformarea acestora în mijloace de probă, [citat 2019-10-22]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/analiza-e-mail-urilor-si-transformarea-acestora-in-mijloace-de-proba/

29. Răzvan-Ionuţ MARIN, Efectuarea verificărilor și percheziţiilor în mediul informatic, [citat 2019-10-26]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/efectuarea-verificarilor-si-perchezitiilor-in-mediul-informatic/
30. Răzvan-Ionuţ MARIN, Mijloace de interceptare a datelor, [citat 2019-10-29]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/mijloace-de-interceptare-a-datelor/
31. Răzvan-Ionuţ MARIN, Mijloace tehnice de localizare și identificare a subiectului investigat, [citat 2019-11-03]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/mijloace-tehnice-de-localizare-si-identificare-a-subiectului-investigat/
32. Răzvan-Ionuţ MARIN, Localizarea și identificarea subiectului investigat, [citat 2019-11-05]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/localizarea-si-identificarea-subiectului-investigat/
33. Ioan-Cosmin MIHAI, Culegerea informațiilor din mediul informatic, [citat 2019-11-8]. Disponibil pe Internet: http://www.criminalitatea-informatica.ro/tehnici-de-investigare/culegerea-informatiilor-din-mediul-informatic/
34. Ioan-Cosmin MIHAI, Procedura desfășurarii investigațiilor on-line, [citat 2019-11-11. Disponibil pe Internet:http://www.criminalitatea-informatica.ro/tehnici-de-investigare/procedura-desfasurarii-investigatiilor-on-line/
35. Golubenco Gh. Obiectul și sistemul criminalisticii: probleme actuale. În: Legea și viața, Chișinău, 2005, p. 8.
36. Doraș S. Criminalistica. Chișinău: Tipografia Centrală, 2011, p. 266.
37. Gheorghiță M. Tratat de criminalistică. Chișinău: Tipografia Centrală, 2017, p. 291.
38. Косынкин А. А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: монография. Москва: Юрлитинформ, 2013, p.13.
39. Purici S., Gheorghiță M. Măsuri tactice și strategice de depășire a obstacolelor care împiedică buna desfășurare a investigării infracțiunilor informatice. În: Studia Universitatis Moldaviae, Seria Științe Sociale, CEP USM, Chișinău, 2017, p. 146.
40. Smith S. The Concept of Security in a Globalized World. În: The Otago University Conference. Tezele conf. internaționale. Otago, 2002.
41. Осипенко А. Л. О характеристике способов совершения сетевых компьютерных преступлений. В: Вестник криминалистики, 2009, p.152
42. Шурухнов Н. Г. Криминалистика: Учебное пособие. Москва: Юристь, 2005
43. Тепуков А. В. Преодоление противодействия доказыванию по уголовным делам в отношении прокуроров, руководителей следственных органов и следователей. În: Закон и право, Юнити-Дана, 2009.

44. Бабаева Э. У. Проблемы теории и практики преодоления противодействия уголовному преследованию. Москва: Юрлитинформ, 2006.
45. Кривенко А. И. Теория и практика взаимодействия следователя с органами, осушествляющими оперативно-розыскную деятельность. М: Юрлитинформ, 2008, p. 240.
46. Ратинов А. Р. Судебная психология для следователей. Москва: Юрлитинформ, 2001.
47. Журавлёв А. Следователь как субъект процессуального руководства расследованием. В: Актуальные проблемы современного процесса РФ. Самара, 2008.
48. Старичков М. В. Тактика проведения обыска, связонного с изъятием носителей компьютерной информации. În: Криминалистика: актуальные вопросы теории и практики. Ростов-на-Дону: ФГОУ ВПО "РЮИ МВД России", 2010, p. 167.
49. Purici S. In dubio pro reo: Apărarea Cal Troian în cauzele de criminalitate informatică. În: Revista Penalmente/Relevant, Universitatea „Nicolae Titulescu”, 2016, p. 168.
50. Мерецкий Н. Е. Опыт использования тактических комбинации при расследование преступлений. În: Актуальные вопросы криминалистического обеспечения судопроизводства. Иркутск: БГУЭП, 2010, p. 295.