

CONTENTS

THE CONSTITUTIONAL BOUNDARIES OF DIGITAL EVIDENCE: INTRUSIVE MEASURES, CYBERSECURITY AND NATIONAL SECURITY IN ROMANIA (Safta, M., Stanciu, C. A. M.)	1
1. Data Retention and Structural Surveillance. Constitutional and European Standards	2
2. Technical Surveillance in Criminal Proceedings: Constitutional Limits and Safeguards	8
3. Cybersecurity and Structural Preventive Surveillance	13
AUTHENTICITY AND ADMISSIBILITY OF DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS THROUGH THE PRISM OF CRIMINAL PROCEDURE PRINCIPLES (Voloshyna V. K.)	21
1. Prerequisites for the problem of authenticity and admissibility of digital evidence	22
2. Legal nature and concept of digital evidence in criminal proceedings	26
3. Procedural principles for ensuring the admissibility of digital evidence	29
4. International standards of admissibility of digital evidence and the practice of the ECHR	32
5. Peculiarities of recording and ensuring the integrity of digital evidence in criminal proceedings	34
BASICS OF RECORDING CYBER OFFENSES THAT INFLUENCE THE MENTAL STATE OF COMPUTER OPERATORS (Gavrylenko Ye. V., Sakhanchuk A. D., Sakhanchuk T. I.)	42
1. Emergence of prerequisites and formulation of the problem	43
2. Method of cyber threats' influence on computer operators	43
3. List and scope of activities of global computer laboratories studying penetration testing	47
4. Leading research centers for the study of remote influence on the psyche of computer operators	47
5. Development and application of testers for recording optical influence on computer operators to secure digital evidence of cyber offenses	49
6. Influence of white light components on the mental state of computer operators through the subconscious mind	53
THE MAIN LAW ON INFORMATION PROTECTION (Hromyko I. O.)	57
1. Information activities of information carriers	58
2. Communicability as a unifying universal term	62
3. Classification of "communicability of information carriers"	66

FEATURES OF THE RECORDING OF DIGITAL TRACES DURING INVESTIGATIVE (SEARCH) ACTIONS (Dzyurbel A. D.)	71
1. The concept, classification and forensic characteristics of digital traces in modern forensics	72
2. Procedural procedure for obtaining and international standards for identifying and preserving electronic evidence	77
3. Техн Technical, forensic and tactical support for the extraction of digital information	83
4. Typical errors and problems of recording digital traces in judicial practice: ways of improvement	85
CYBERCRIME IN AREAS OF ARMED CONFLICT (THE CASE OF UKRAINE): VICTIMIZATION FACTORS AND PREVENTION STRATEGIES (Dumchikov M. O., Yanishevska K. D., Murach D. V.)	92
1. Ontogenesis and Pathogenesis of Cybercrime in Ukrainian National Law	93
2. War as a Factor of Cybercrime Victimization	103
3. Cybercrime Prevention Strategies in Wartime (Based on the Experience of Ukraine)	110
ON DETECTIVE (INVESTIGATIVE) ACTIVITY IN MILITARY CRIMINALISTICS (NATIONAL AND INTERNATIONAL DIMENSIONS) (Kaliuga K. V.)	128
1. General Characteristics of Detective Activity in Military Criminalistics	130
2. The System of Subjects of Detective Activity in War Crimes Investigations	131
3. Identification of the Perpetrator and Documentation of Command Responsibility	133
4. Analytical Detective Activity and Forensic Modeling	134
5. The Use of OSINT and Digital Evidence in War Crimes Investigations	136
6. Specific Features of Detective Activity in Temporarily Occupied Territories	138
7. International Cooperation in Detective Activity	140
8. Challenges and Prospects for the Development of Detective Activity	142
CRIMINAL PROCEDURAL AND FORENSIC ASPECTS OF PROVING HATE SPEECH IN THE DIGITAL ENVIRONMENT (Koval A. A., Kazarian E. H.)	149
1. Theoretical and Legal Foundations for Countering Hate Speech	150
2. Specific Features of Proving Hate Speech in the Digital Environment	156

FORENSIC TOOLS FOR OBTAINING EVIDENTIARY INFORMATION IN CRIMINAL INVESTIGATIONS IN THE DIGITAL ERA (Kurman O. V.)	166
1. Artificial intelligence in the analysis of digital traces: innovative perspectives and challenges of application	167
2. Digital traces of mobile communication devices in criminalistic practice... ..	175
MODERN CHALLENGES OF CRIMINAL LAW REGULATION OF CYBERCRIME: NATIONAL AND INTERNATIONAL DIMENSIONS (Larchenko M. O.).....	186
1. The problem’s prerequisites emergence and the problem’s formulation	186
2. Law enforcement issues regarding cyberattacks on critical infrastructure.....	188
3. Liability for the distribution of malicious software	192
4. Current cases of international cooperation in the fight against cybercrime	194
OSINT TECHNOLOGIES IN LAW ENFORCEMENT: INNOVATIONS AND AREAS OF APPLICATION DURING MARTIAL LAW AND THE COUNTRY’S POST-WAR RECOVERY (Nehrebetskyi V.V.)	201
1. Challenges of Regulating the Use of Digital Evidence Technologies During Wartime	202
2. Using Digital Technologies and Open-Source Data in Investigating War Crimes.....	206
3. Ensuring Authenticity and Admissibility of Digital Open-Source Evidence in Criminal Justice	212
ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS: CONCEPTUAL FOUNDATIONS AND PROCEDURAL REQUIREMENTS (Perunova O. M.)	220
1. The Concept of Electronic Evidence in Civil Proceedings	221
2. Requirements and the Special Significance of Electronic in Civil Proceedings.....	226
THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME AS THE BASIS FOR CRIMINAL LAW PROTECTION OF PUBLIC RELATIONS IN CYBERSPACE IN UKRAINE (Politova A. S.).....	239
1. The Concept of Electronic Evidence in Civil Proceedings	240
2. Cybercrime: concept and types of criminal offenses.....	244
3. Implementation of the provisions of the Council of Europe Convention on Cybercrime in the Criminal Code of Ukraine.....	249

COUNTERING CYBERCRIME: USING ELECTRONIC EVIDENCE IN THE INVESTIGATION PROCESS (Ryashko O. V.)	262
1. The role and place of electronic evidence in cybercrime investigations.....	263
2. Typical investigative situations and characteristics of a cybercriminal	268
INTERNATIONAL MECHANISM FOR COMBATING CYBERCRIME (Syroid T. L.)	275
1. International Legal Framework for Combating Cybercrime.....	276
2. International Institutional Framework for Combating Cybercrime	286
CONSTITUTIONAL AND LEGAL GUARANTEES OF MEDIA FREEDOM AND JOURNALISTIC ACTIVITY IN THE DIGITAL ENVIRONMENT: THE PRACTICE OF THE ECTHR IN THE CONTEXT OF CYBER OFFENCES (Slinko T. M., Slinko K. M.)	296
1. Media Freedom as a Fundamental Value of Constitutionalism in the Conditions of the Digital Society	297
2. Constitutional and Legal Foundations for Guaranteeing Freedom of Speech and Media Activity in Ukraine	303
3. Case Law of the European Court of Human Rights on Media Freedom and Journalistic Activity in the Digital Environment	313
INSTITUTIONALIZATION OF THE NATIONAL CYBERSECURITY SYSTEM: LEGAL STATUS AND POWERS OF THE SECURITY AND DEFENSE SECTOR ACTORS (Spivak M. V., Dubina O. M.)	322
1. Cybersecurity as a multifaceted phenomenon: diverse approaches to definition and protection measures	323
2. Legislative regulation of cybersecurity in Ukraine: analysis of implementation and strategic directions	326
3. Classification and mechanisms of cyber incident management: synergy of scientific approaches and state standards.....	330
4. Interaction of cybersecurity stakeholders in digital evidence collection and cyber incident neutralization: empirical analysis of law enforcement activities	334
SOME PROBLEMS OF DIGITAL INFORMATION AND THE RELIABILITY, ADMISSIBILITY OF DIGITAL EVIDENCE (Stratonov V. M., Basysta I. V., Hutnyk A.)	343
1. Information or evidence? Electronic, digital, electronic-digital?	344
2. Reliability and admissibility, how to achieve?	347
3. Verification and confirmation of the reliability of digital information	350

DIGITAL CRIMINALISTICS AS A STRATEGIC DIRECTION FOR THE DEVELOPMENT OF MODERN CRIMINALISTICS (Shevchuk V. M., Zatenatskyi D. V., Kolesnikova I. A.)	361
1. Digital transformation of criminalistics – a scientific prerequisite and methodological basis for the formation of new criminalistic knowledge	362
2. Digital criminalistics: concepts and significance in the formation of evidentiary information in the conditions of hybrid warfare.....	367
3. The role of digital criminalistics tools in the detection, recording and investigation of war crimes in Ukraine	372
DIGITAL EVIDENCE IN COUNTERING CYBERCRIME: LEGAL, TECHNICAL, AND FORENSIC ASPECTS (Homon V. O., Miroshnyk R. O., Khivrenko D. V.)	384
1. Digital evidence as an interdisciplinary legal category.....	385
2. Cybercrime and the specifics of its proof.....	386
3. Blockchain analyzers and artificial intelligence in forensic cryptocurrency investigations.....	387
4. Procedural and methodological aspects of handling digital evidence.....	389
5. Prospects for development	391