Svitlana Mazepa, Oksana Bratasyuk*

Die Gewährleistung der Informationssicherheit in der Ukraine – Verwaltungs- und strafrechtliche Maßnahmen

Abstract (dt.):
Im folgenden Aufsatz wird die nationale Gesetzgebung der Ukraine und ausländische Quellen in Bezug auf eine effektive Informationssicherheit des Staates und der Gesellschaft analysiert, und zwar es handelt sich um einzelne Mechanismen der Umsetzung der Informationspolitik in Form von administrativer und strafrechtlicher Verantwortung für Straftaten im Informationsbereich. Es wurde versucht, eine Reihe von Konzepten zu verbessern, die in dieser Forschung von zentraler Bedeutung sind: Informationssicherheit, Informationssphäre, Informationsdelikte. Es werden Vorschläge zur Reform der nationalen Rechtsvorschriften und der Strafverfolgungspraxis im Zusammenhang mit der Informationssicherheit gemacht, um sie an europäische Standards anzugleichen. Die Autoren haben die geltende Gesetzgebung bezüglich der Ordnungswidrigkeiten, des Strafgesetzbuchs der Ukraine und anderer Gesetze und Verordnungen sowie wissenschaftliche Untersuchungen umfassend untersucht, um die wichtigsten Merkmale der verwaltungs- und strafrechtlichen Verantwortung im Bereich der Informationssicherheit in der Ukraine zu ermitteln und die vorrangigen Schritte für die Gesetzreform festzulegen. Außerdem wurde auch ein Überblick der aktuellen Straftatbestände im Informationsbereich verschafft und vorgeschlagen, die Normen der administrativen Verantwortung zu vereinheitlichen und Handlungen, die im Zusammenhang mit Fake News, Propaganda, fingerten Bombenanschlägen und Cyberstalking stehen, unter Strafe zu stellen.
Keywords: Informationssicherheit in der Ukraine, Informationsbereich, administrative Verantwortung, strafrechtliche Verantwortung, Informationsdelikte, Informationskriminalität

Abstract (Engl.):
Ensuring Information Security in Ukraine – Administrative and Criminal Law Measures: This contribution analyzes the national legislation of Ukraine and foreign sources for the effective provision of information security of the state and society, na-

* *Svitlana Mazepa*, ORCID 0000-0003-1282-9089, Vice Dean of the faculty of law, Dr. Ass. professor of the Department of criminal law and procedure, West Ukrainian National University, intpolsveta@gmail.com; *Oksana Bratasyuk*, ORCID 0000-0002-5871-4386, PhD, Acting Head, Ass. Professor of the Department of Constitutional, Administrative and Financial and Law, West Ukrainian National University, e-mail: rosoliak@gmail.com. Dieser Text ist im Rahmen einer Förderung durch die VolkswagenStiftung für ukrainische Wissenschaftlerinnen und Wissenschaftler, die nach dem russischen Überfall auf ihr Land nach Deutschland geflohen sind, entstanden; in diesem Heft ist eine Übersetzung des Beitrags abgedruckt.

OER 4/2022, DOI: 10.5771/0030-6444-2022-4-421

mely, individual mechanisms for the implementation of information policy in the form of administrative and criminal liability for offenses in the information sphere. An attempt was made to improve several concepts that are key in this study: information security, information sphere, information offense. Proposals are given for reforming national legislation and law enforcement practice in the context of ensuring information security in order to bring them into line with European standards. The authors comprehensively studied the norms of the Code of Ukraine on Administrative Offenses, the Criminal Code of Ukraine and other regulatory legal acts, scientific breakthroughs, due to which the key features of administrative and criminal liability in the field of ensuring information security of Ukraine were highlighted and the corresponding priority steps were identified to reform the legislation. Also, a review of current offenses in the information sphere was carried out and it was proposed to unify the norms of administrative responsibility and criminalize acts related to fake news, propaganda, fake mining and cyberstalking.
Keywords: information security of Ukraine, information sphere, administrative responsibility, criminal liability, cybercrime, cyberspace, information offense, information crime

I. Einleitung

Unter den modernen Bedingungen sind Fragen der Gewährleistung der Informationssicherheit in der Ukraine äußerst wichtig, was in erster Linie auf die Notwendigkeit zurückzuführen ist, illegalen Eingriffen in den Informationsraum der Ukraine entgegenzuwirken, Informationsressourcen zu bewahren, die Bevölkerung vor dem negativen Informationseinfluss anderer Staaten, bestimmter politischer Kräfte und gesellschaftlicher Gruppen usw. zu schützen. Darüber hinaus hat die europäische Integration eine strategisch anerkannte Priorität für die ukrainische Außenpolitik, denn sie erfordert eine Verbesserung des rechtlichen und regulatorischen Rahmens für die Informationssicherheit der Ukraine, die nicht nur internationalen Standards, sondern vor allem den nationalen Interessen der Ukraine im Bereich der Information entspricht. Diese Bestimmungen spiegeln sich in der Informationssicherheitsstrategie der Ukraine wider, denn dadurch wird festgestellt, welchen aktuellen Herausforderungen und Bedrohungen sich die nationale Sicherheit der Ukraine im Informationsbereich ausgesetzt sieht, welche strategische Ziele zur Bekämpfung dieser Bedrohungen es gibt, wie die Menschenrechte und personenbezogene Daten geschützt werden.[1]

Die Bestimmungen dieses Dokuments legen fest, dass der Zweck der Strategie darin besteht, die Fähigkeit zur Gewährleistung der Informationssicherheit des Staates und seines Informationsraums zu stärken, die soziale und politische Stabilität durch Informationsmittel und -maßnahmen, die Landesverteidigung, den Schutz der staatlichen Souveränität, die territoriale Integrität der Ukraine, die demokratische Verfas-

1 Strategija informacionnoj bezopasnosti. Ukaz Prezidenta Ukrainy ot 28 dekabrja 2021 g. № 685/2021 [Strategie der Informationssicherheit. Erlass des Präsidenten der Ukraine vom 28 Dezember 2021, № 685/2021], https://zakon.rada.gov.ua/laws/show/685/2021#n7, 15. Januar 2022.

sungsordnung und die Gewährleistung der Rechte und Freiheiten aller Bürger zu unterstützen.[2]

Darüber hinaus werden in der Strategie die wichtigsten globalen Bedrohungen für die Informationssicherheit des Staates genannt: die zunehmende Zahl globaler Desinformationskampagnen; die Informationspolitik der Russischen Föderation, die nicht nur die Ukraine, sondern auch andere demokratische Staaten bedroht; der Einflussgrad von sozialen Netzwerken auf den Informationsraum; der Mangel an Medienkompetenz (Medienkultur) unter den Bedingungen der rasanten Entwicklung der digitalen Technologien. Trotz der externen Bedrohungen gibt es auch nationale Herausforderungen und Bedrohungen, wie z. B. die begrenzte Fähigkeit, auf Desinformationskampagnen zu reagieren; unvollständiges System der strategischen Kommunikation; Regulierungsbedarf der Beziehungen im Bereich der Informationstätigkeit und Schutz der beruflichen Tätigkeit von Journalisten; Versuche der Manipulation der ukrainischen Bürger in Bezug auf die europäische und euro-atlantische Integration der Ukraine; Zugang zu Informationen auf lokaler Ebene; unzureichendes Niveau der Informationskompetenz. Abgesehen von den in der Strategie direkt erwähnten Herausforderungen ist die Unvollkommenheit der ukrainischen Gesetzgebung im Informationsbereich und ihre Nichtübereinstimmung mit modernen Anforderungen eine weitere Herausforderung für die ukrainische Gesellschaft. Um diese Strategie umzusetzen, wurde die Regierung beauftragt, den Rechts- und Regulierungsrahmen zu verbessern, indem sie die einschlägigen Rechtsvorschriften und andere Rechts- und Regulierungsakte im Informationsbereich systematisch überprüft und ändert.

Das Ziel des Artikels ist es, die Besonderheiten und Probleme bei der Gewährleistung der Informationssicherheit zu klären, insbesondere die Besonderheiten der verwaltungs- und strafrechtlichen Verantwortung für Straftaten im Bereich der Information aufzuzeigen, die Defizite in diesem Bereich aufzudecken und Perspektiven zu zeigen.

1. Zur Frage der Definition der Begriffe Informationssicherheit, Informationsbereich und Informationsdelikt und ihrer Anpassung an die heutigen Herausforderungen der Informationssicherheit

Es gibt viele wissenschaftliche Studien, die sich mit der Gewährleistung der Informationssicherheit in der Ukraine befassen, ein großer Teil davon widmet sich Entwicklungen im Bereich des Rechts. Es ist besonders wichtig, einige Wissenschaftler zu nennen, deren Arbeiten bei der Vorbereitung dieses Artikels analysiert wurden. So beschreibt beispielsweise *Belevceva* einige Merkmale der rechtlichen Regelung von Informationsressourcen.[3] Der Autor weist auf einige Defizite im Bereich der Informati-

2 Strategija informacionnoj bezopasnosti. Ukaz Prezidenta Ukrainy ot 28 dekabrja 2021 g. № 685/2021 [Strategie der Informationssicherheit. Erlass des Präsidenten der Ukraine vom 28 Dezember 2021, № 685/2021], https://zakon.rada.gov.ua/laws/show/685/2021#n7, 15. Januar, 2022.

3 *V. V. Belevceva*, Pravovoj režim informacionnych resursov [*V. V. Belevceva*, rechtliche Regulierungsmechanismus der Informationsressourcen], http://ippi.org.ua/sites/default/files/11bvvrir.pdf,19. Januar, 2022.

onssicherheit hin, insbesondere auf die unvollständige Gestaltung des Rechtsrahmens, der die rechtliche Regelung des betreffenden Bereichs ermöglicht. *Perun* zeigt in seiner Arbeit die Besonderheiten des administrativen und rechtlichen Mechanismus zur Gewährleistung der Informationssicherheit in der Ukraine auf.[4] Im Rahmen der Untersuchung von Merkmalen und Problemen der rechtlichen Regelung im Bereich der Informationssicherheit in der Ukraine war eine Überprüfung der offengelegten Fragen ziemlich sinnvoll. *Turčak* betrachtet umfassend die Mechanismen der Informationssicherheit der Ukraine als Bestandteil der Staatssicherheit der Ukraine. Es ist klar, dass Informationssicherheit nicht nur den Schutz von Informationen vor unbefugtem Zugriff beinhaltet, sondern vor allem die Verhinderung des unbefugten Zugriffs, der Nutzung, Offenlegung, Änderung, Überprüfung, Aufzeichnung oder Vernichtung von Informationen. Die Informationssicherheit umfasst also sehr viele Anwendungsbereiche wie Kryptographie, Computer, Cyberforensik, soziale Online-Medien usw.[5]

Borisov stellt fest, dass das nationale Gesetzgebungssystem weder die Ziele und aktuellen Aufgaben der Informationssicherheit der Ukraine noch die Zuständigkeiten in diesem Bereich und die Mittel der rechtlichen Regelung klar festlegt, die einen angemessenen und ausgewogenen rechtlichen Einfluss auf die einschlägigen Rechtsbeziehungen ermöglichen würden. Gleichzeitig verweist der Autor auf die Bedeutung und Notwendigkeit einer angemessenen legislativen Unterstützung bei der Gestaltung des Rechtssystems und der Gewährleistung des Funktionierens des Mechanismus der rechtlichen Regelung der Informationssicherheit. Dementsprechend stellt der Autor fest, dass die Schaffung eines angemessenen Rechtsrahmens für die Informationssicherheit in der Ukraine eine wichtige Voraussetzung und ein vorrangiger Schritt für die Umsetzung einer wirksamen rechtlichen Regelung zur Gewährleistung der Informationssicherheit in der Ukraine ist.[6]

In der Alltagskommunikation und in den Medien treten häufig folgende Begriffe auf wie Informationsraum, Informationsinfrastruktur, Informationssphäre, Informationsaktivität, Informationspotential, Informationsrealität, Informationswirklichkeit, Bereich von Informatisierung, Infosphäre und sogar Cyberspace, Cybersphäre und ähnliche, die für den Durchschnittsbürger tatsächlich synonym sind und soziale Prozesse im Zusammenhang mit dem Informationsaustausch und mit der Informatisierung widerspiegeln.

Es wäre logisch, mit der Analyse einer Kategorie zu beginnen, die auf die eine oder andere Weise geeignet ist, die im Informationsrecht weit verbreiteten Begriffe zu

4 *T.S. Perun*, Administrativnaja otvetstvennost' v sisteme mer obespečenija informacionnoj bezopasnosti // IT pravo: problemy i perspektivy razvitija v Ukraine (vtoraja Meždunarodnaja ježegodnaja konferencija) [*T.S. Perun*, Administrative Verantwortung im System der Informationssicherheitsmaßnahmen // IT-Recht: Probleme und Entwicklungsperspektiven in der Ukraine (Zweite Internationale Jahreskonferenz)], http://aphd.ua/publication-358/, 19. Januar, 2022.

5 What is Information Security?, https://www.geeksforgeeks.org/what-is-information-security/, 19. Januar, 2022.

6 *O. Borisov*, Osobennosti pravovogo režima obespečenija informacionnoj bezopasnosti Ukrainy, obuslovlennyje Konstitucijej Ukrainy [*O. Borisov*, Besonderheiten des rechtlichen Regulierungsmechanismus der Informationssicherheit in der Ukraine, die durch die Verfassung der Ukraine bestimmt sind], http://ippi.org.ua/sites/default/files/20_8.pdf, S. 160, 10. Januar, 2022.

vereinen und das Wesen des Gegenstands der rechtlichen Regelung der Informationsbeziehungen zu erfassen, wobei die theoretischen und methodischen Voraussetzungen für die Definition des Begriffs "Informationssphäre" berücksichtigt werden sollten. Die Definition der Informationssphäre ist sowohl im allgemeinen Sprachgebrauch als auch in der Medienansprache, in der wissenschaftlichen Terminologie, in Gesetzestexten usw. weit verbreitet. Es ist jedoch darauf hinzuweisen, dass es bisher keine eindeutige Auslegung dieses Begriffs gibt.

Es ist allgemein anerkannt, dass die Öffentlichkeitsarbeit im Zusammenhang mit Informationen und Informationsprozessen durch die Normen des Informationsrechts geregelt wird. Es liegt daher nahe, dass eine systematische und eingehende Untersuchung der theoretischen und methodischen Grundlagen des Informationsrechts, seiner wissenschaftlichen Probleme in verschiedenen Richtungen und der Angemessenheit der Informationsgesetzgebung an die modernen gesellschaftlichen Anforderungen eine der wichtigsten Voraussetzungen für die erfolgreiche Gestaltung des Informationsbereichs und die rechtliche Unterstützung dieses Prozesses ist.

Um diverse Konzepte zu beschreiben, die den Bereich der Information darstellen, werden in der wissenschaftlichen Literatur bei Forschungen in verschiedenen Wissens- und Tätigkeitsbereichen in der Regel folgende Begriffe verwendet: Informationsraum, Informationsfeld, Informationsbereich, Informationssphäre. Gegenwärtig gibt es jedoch trotz der breiten Verwendung des Begriffs Informationsraum weitere Definitionen des Konzepts des Informationsraums. „Die Informationssphäre ist eine Sphäre des Informationsaustausches (Produktion – Verteilung – Konsum), bei dem die Subjekte ihre Bedürfnisse und Möglichkeiten in Bezug auf die Information umsetzen“ – diese Definition wurde von den bekannten Forschern auf dem Gebiet des Informationsrechts *Bačilo*, *Lopatin* und *Fedotov* vorgeschlagen.[7] Und wenn die Definition selbst ziemlich allgemein ist, wird sie durch die nachfolgenden Erläuterungen der Autoren präzisiert. Zu den Hauptobjekten der Informationssphäre gehören also: Informationen, einschließlich der auf entsprechenden Informationsträgern gespeicherten Informationsressourcen, sowie die Informationsinfrastruktur, die mehrere Informationssysteme umfasst: Organisationsstrukturen, Informations- und Telekommunikationsstrukturen, Informations-, Computer- und Telekommunikationstechnologien und Mediensysteme.

Es ist klar, dass die von den Autoren aufgeführte Liste der Elemente der Informationsinfrastruktur bei weitem nicht vollständig ist. Ein wesentlicher Bestandteil dieses Regelwerks ist das Informationsrecht. Der größte Nachteil dieser Definition besteht jedoch darin, dass sie durch einen anderen Begriff – „Sphäre“ – ersetzt wird, dessen Definition nicht angegeben ist. Man sollte der Definition von *Aristova* zustimmen, die in ihrer Auslegung die Besonderheit der Informationssphäre als die Sphäre, in der die Informationstätigkeit ausgeübt wird (Sammlung, Produktion, Speicherung, Nutzung, Verbreitung von Informationen), und die entsprechenden Aktivitäten, die die Informa-

7 *I.L. Bačilo,* Informacionnoje pravo: pod red. akademika B.N. Topornina. Sankt-Peterburg: Izdatel'stvo R. Aslanova "Juridičeskij centr Press [*I.L. Bačilo,* Informationsrecht: *B.N. Topornin* (Hrsg.)]. Sankt Petersburg, Verlag von R. Aslanov „Juridičeskij centr Press“, 2005, S. 156, 10. Januar, 2022.

tionstätigkeit gewährleisten, betont.[8] Eine ähnliche wissenschaftliche Auffassung vertritt *Beljakov*, der argumentiert, dass die Informationsumgebung als Gesamtheit der Informationsressourcen in Einheit mit den Mitteln, Methoden und Bedingungen, die ihre Aktivierung und aktive Nutzung ermöglichen, definiert werden kann.[9] Wesentlich praktischer ist jedoch die Definition von *Strelcov*: Die Informationssphäre besteht aus der Gesamtheit der Information und Informationsinfrastruktur der Gesellschaft sowie aus den sozialen Beziehungen, deren Gegenstand die Information und die Informationsinfrastruktur sind.[10] Diese Definition wurde von *Kašapov* präzisiert, der die Informationsumgebung als Gesamtheit folgender Elemente versteht: 1) Subjekte der Informationsinteraktion oder -beeinflussung; 2) die eigentliche Information, die für die Nutzung durch die Subjekte der Informationssphäre bestimmt ist; 3) die Informationsinfrastruktur, die den Informationsaustausch zwischen den Subjekten ermöglicht; 4) die sozialen Beziehungen, die im Zusammenhang mit der Bildung, Übertragung, Verteilung und Bewahrung von Informationen entstehen.[11]

Und in jedem Fall werden in den Definitionen entweder die Informationsinfrastruktur oder die Informationsressourcen aus dem Modell der Informationssphäre ausgeklammert, oder es werden nicht einmal alle Phasen des Informationsaustausches abgedeckt, oder es wird die Frage der Regulierung der Öffentlichkeitsarbeit nicht berücksichtigt. Ganz besonders ist die Begriffsdeutung zu beachten, die in der gemeinsamen Monographie „Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: eine Monographie“ formuliert wird: „Die Informationssphäre ist eine Sammlung von Informations- und Informationsressourcen, der Informationsinfrastruktur, der Subjekte, die den Informationsaustausch durchführen, d. h. ihre Schaffung, Verteilung (Übertragung), Speicherung, Nutzung und Zerstörung, und diesen Austausch sicherstellen, der daraus entstehenden sozialen Beziehungen, des Systems der rechtlichen Unterstützung sowie des institutionellen Systems der staatlichen Verwaltung dieser Umgebung“.[12] Gleichzeitig kann

8 *I.V. Aristova*, *V.D. Černadčuk*, Koncepcija informacionnych pravootnošenij: suščnost' i osobennosti ispol'zovanija v sfere bankovskoj dejatel'nosti/Informacija i pravo. [*I.V. Aristova*, *V.D. Černadčuk*, Das Konzept der Informationsrechtsbeziehungen: das Wesen und die Besonderheiten der Anwendung im Bankenumfeld], 2012, №3, S. 47-57, 19. Januar, 2022.

9 *K.I. Beljakov*, Informatizacija v Ukraine: problemy organizacionnogo pravovogo i nauchnogo obespečenija: monografiya. Kiyev: KVITS, 2008. 576 S. [*K.I. Beljakov,* Informatisierung in der Ukraine: Probleme der organisatorischen, rechtlichen und wissenschaftlichen Unterstützung: eine Monographie], 19. Januar, 2022.

10 *A.A. Strel'cov,* Obespečenije informacionnoj sochrannosti Rossii. Teoretičeskije i metodologičeskije bazy / Pod red. V.A. Sadovničego i V.P. Šerstjuka. Moskva: MTSNMO, 2002. 296 S. [*A.A. Strel'cov,* Gewährleistung der Informationssicherheit in Russland. Theoretische und methodologische Grundlagen / Herausgegeben von V.A. Sadovničij und V.P. Šerstjuk], http://labs.rulezz.ru/files/241/str.pdf, 19. Januar, 2022.

11 *M. Kašapov,* Teorija i praktika razrešenija konfliktnych situacij. Kratkiy slovar'. Moskva Jaroslavl': Remder, 2003, 779 S., [*M. Kašapov*, Theorie und Praxis der Konfliktlösung. Ein kurzes Wörterbuch.], 15. Januar, 2022.

12 Juridičeskaja otvetstvennost' za pravonarušenija v informacionnoj sfere i osnovy informacionnoj deliktologii: monografija / I. V. Aristova, A. A. Baranov, O. P. Dzoban' i dr.; pod obšč. red. prof. Beljakova. Kijev: KVITS, 2019, S. 23 [Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: Monographie / *I.V. Aristova, A.A. Baranov, O.P. Dzoban'* u.a.; Hrsg. von *Prof. Beljakov*], 19. Januar, 2022.

die Ansicht von A. Selezneva unterstützt werden, dass die Informationssphäre eng mit anderen Sphären der öffentlichen Tätigkeit verbunden ist, aber zugleich durch eine sektorale Zugehörigkeit gekennzeichnet ist, die ihre Autonomie gegenüber anderen Sphären bestimmt.[13]

Die Komplexität des Informationsrechts und der branchenübergreifende Inhalt der bestehenden Informationsgesetzgebung erfordert eine eingehende Untersuchung der Analyse des Instituts der rechtlichen Verantwortlichkeit für Straftaten im Informationsbereich mit dem Ziel, die Informationssicherheit des Einzelnen, des Staates und der Gesellschaft zu gewährleisten, indem der Mechanismus zur Regelung der sozialen Beziehungen, die bei Informationstätigkeiten entstehen (Informationsbeziehungen), verbessert wird, was für die Entwicklung des Informationsrechts von zentraler Bedeutung ist.

2. Merkmale von Straftaten im Informationsbereich: Begriffe, Arten, Besonderheiten.

Bei der Betrachtung von Straftaten im Zusammenhang mit Informationen, die als Grund für die strafrechtliche Verantwortlichkeit gelten, ist zu beachten, dass alle rechtswidrigen Handlungen in irgendeiner Weise mit Informationen zusammenhängen: Informationen, Computerstraftaten, Computerinformationsdelikte, IT-Delikte, Informationssicherheitsdelikte, Cyberstraftaten usw. Dies zeigt, dass daran ein großes wissenschaftliches Interesse besteht und dass das Problem der Bekämpfung solcher Straftaten äußerst dringlich ist. Die Vielfalt der Straftaten im Bereich der Information ist jedoch so groß, dass weder die Wissenschaft noch die nationalen Rechtssysteme oder das internationale Recht ein gemeinsames Verständnis davon entwickelt haben. Es fehlt nach wie vor an einer einheitlichen Terminologie und an einem System allgemein akzeptierter theoretischer Konzepte, die die gesamte Bandbreite rechtswidriger Handlungen und der sich daraus ergebenden Folgen im Bereich der Information, der Informationsauswirkungen, der Technologien, der Computer und ihrer Systeme, der lokalen und globalen Informations- und Telekommunikationsnetze usw. vollständig widerspiegeln könnten.

Bei der Untersuchung dieser Art von Straftaten sind wir auf verschiedene Definitionen von Informationsdelikten gestoßen, nämlich „Computerkriminalität", „Cyberkriminalität", „Informationskriminalität", „Informationsdelikte", „Informationstechnologiedelikte", „IT-Delikte", „E-Kriminalität" und „High-Tech-Kriminalität".[14]

13 *O. M. Selezneva*, Teoretiko-metodologičeskaja traktovka otdel'nych osnovnych kategorij informacionnogo prava [*O. M. Selezneva*, Theoretische und methodologische Auslegung bestimmter Hauptkategorien des Informationsrechts], http://aphd.ua/publication-164/, 19. Januar, 2022.

14 Organizacionno-pravovyje i taktičeskije osnovy protivodejstvija prestupnosti v sfere vysokich informatsionnych technologij: učebnoje posobije / Pod red. B.V. Romanjuka; Je.D. Skulyša. Kijev: KIT, 2011. 404 s. [Organisationsrechtliche und taktische Grundlagen zur Kriminalitätsbekämpfung im Hightech-Umfeld: Lehrbuch / *B.V. Romanjuk; Je.D. Skulyša* (Hrsg.)], 10. Januar, 2022.

Es ist zu bedenken, dass die kognitiven Prozesse der Bildung von Informationskriminalität als wissenschaftlicher Rechtskategorie inhärent widersprüchlich und fragmentiert sind, was durch die Aktualisierung ihrer Einzelaspekte bedingt ist, vor allem derjenigen, die heute gewohnheitsmäßig als „Cybercrime" bezeichnet werden. In der jüngeren Vergangenheit wurde im postsowjetischen Wissenschaftsraum der Begriff „Computerkriminalität" viel häufiger verwendet, wodurch de facto der wissenschaftliche Diskurs über Cyberkriminalität im Inland begann.[15]

Bei der Untersuchung der Korrelation von Computer- und Informationsdelikten kommt *Pravdjuk* zu dem Schluss, dass „Computerdelikte nur ein Teil von Informationsdelikten sind, das heißt, sie beziehen sich als Teil und Gemeinsamkeit aufeinander".[16] So bezieht sich *Butuzov* bei der Analyse dieses Problems auf Computerkriminalität im Bereich der Nutzung von elektronischen Computern, Systemen und Computernetzen sowie Telekommunikationsnetzen und definiert sie als „Angriff auf die Beziehungen im Bereich der computergestützten Verarbeitung von Informationen, auf das Eigentumsrecht natürlicher und juristischer Personen auf Informationen und den Zugang zu ihnen".[17] Es liegt auf der Hand, dass diese Auslegung des Begriffs der Computerkriminalität inhaltlich weiter gefasst ist und verschiedene Erscheinungsformen von Straftaten umfasst, sowohl solche, die sich direkt gegen die Ordnung der computergestützten Verarbeitung von Informationen richten, als auch solche, die die Informationsrechte von Personen verletzen, die durch die Nutzung von Computersystemen verwirklicht werden. Ähnliche Ansätze lassen sich in den Arbeiten vieler einheimischer Wissenschaftler finden, unabhängig davon, wie sie den Begriff „Computerkriminalität" oder „Cyberkriminalität" deuten. Wenn man den Begriff „Cyberkriminalität" analysiert, sollte man zunächst das allgemein anerkannte Konzept der „Kybernetik" für sich klären (abgeleitet vom griechischen κυβερνητική – „die Kunst der Kontrolle") – „die Wissenschaft von den allgemeinen Gesetzmäßigkeiten der Verwaltungsprozesse und Informationsübertragung in verschiedenen Systemen, seien es Maschinen, lebende Organismen oder die Gesellschaft".[18]

Die weite Auslegung des Begriffs „Cyberkriminalität" steht auch weitgehend im Einklang mit dem Standpunkt internationaler Experten, der im Jahr 2000 auf dem Zehnten Kongress der Vereinten Nationen zur Verbrechensverhütung und Behandlung von Straftätern verkündet wurde. Der Begriff „Cyberkriminalität" umfasst alle Straftaten, die mit der Absicht begangen werden, ein Computersystem oder -netz zu stö-

15 Juridičeskaja otvetstvennost' za pravonarušenija v informacionnoj sfere i osnovy informacionnoj deliktologii: monografija / I. V. Aristova, A. A. Baranov, O. P. Dzoban' i dr.; pod obšč. red. prof. Beljakova. Kijev: KVITS, 2019, S. 23 [Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: Monographie / *I.V. Aristova, A.A. Baranov, O.P. Dzoban'* u.a.; Hrsg. von *Prof. Beljakov*], 19. Januar, 2022.

16 *S.A. Pravdjuk*, Komp'juternyje prestuplenija i informacionnyje prestuplenija: aspekty sootnošenija. Naučnyj vestnik Nacional'nogo universiteta bioresursov i prirodopol'zovanija Ukrainy, 2013, Vyp. 182., Č. 3, S. 216-223, S. 222 [*S.A. Pravdjuk*, Computerkriminalität und Informationskriminalität: Korrelationsaspekte], 18. Januar, 2022.

17 *V.M. Butuzov,* Protivodejstvije komp'juternoj prestupnosti v Ukraine (sistemno-strukturnyj analiz): monografija. Kijev: KIT, 2010, S. 94 [*V.M. Butuzov,* Bekämpfung der Computerkriminalität in der Ukraine (Eine System- und Strukturanalyse): Monographie], 19. Januar, 2022.

18 Prestuplenija v sfere informacionnych technologij ili kiberprestupnost' [Computerkriminalität oder Cyberkriminalität] http://ru.wikipedia.org/wiki, 19. Januar, 2022.

ren. Im Prinzip gilt er für alle Straftaten, die im „elektronischen Bereich“ begangen werden können.[19]

Heute sollte unbedingt beachtet werden, dass es äußerst wichtig ist, eine Kategorie von Informationsdelikten zu verstehen, die über die Zuständigkeitsgrenzen der nationalen Rechtssysteme hinausgeht und eine weltweite Bedrohung darstellt – die „internationale Informationskriminalität“. Sie kann als Aktivitäten von Akteuren der internationalen Politik zur eklatanten Verzerrung des Informationsraums durch starke Informationsausweitung, systematische Desinformation, Informationsisolierung bestimmter Regionen und die Schaffung von Hindernissen für internationale Beobachter zur Bildung einer illusorischen öffentlichen Meinung interpretiert werden, die für die Durchführung der staatlichen internationalen Politik notwendig ist, was nicht den humanistischen und rechtlichen Idealen der modernen Gesellschaft entspricht und die Weltordnung bedroht. Die Wirksamkeit der Gegenmaßnahmen gegen internationale Informationsdelikte hängt mit einer bestimmten Art von rechtlicher Verantwortung zusammen – der internationalen Verantwortung – und dementsprechend auch mit allen Problemen ihrer Umsetzung.

So liefert das Autorenkollektiv in seiner Arbeit eine Definition, die den modernen Anforderungen und Herausforderungen weitgehend gerecht wird: „Ein Informationsdelikt ist eine Gesamtheit rechtswidriger, sozial gefährlicher Handlungen (Handlungen oder Unterlassungen) von Delinquenten der Informationsbeziehungen, die von der geltenden Gesetzgebung vorgesehen sind und die die Interessen der Gesellschaft, des Staates und des Einzelnen im Bereich der Information schädigen – dies betrifft die Verletzung des Rechts auf Schutz vor unbefugter Verbreitung und Nutzung von Informationen, negative Folgen der Beeinflussung von Informationen oder der Funktionsweise von Informationstechnologien sowie andere sozial gefährliche Handlungen im Zusammenhang mit der Verletzung des Eigentumsrechts an Informationen und Informationstechnologien, des Rechts der Eigentümer oder Nutzer der Informationstechnologien, rechtzeitig zuverlässige und vollständige Informationen zu erhalten oder zu verbreiten, für deren Umsetzung der Staat die Anwendung von rechtlichen Maßnahmen zur gesetzlichen Haftung gegenüber dem Täter vorsieht“.[20]

Was die Merkmale und Eigenschaften einer Straftat im Bereich der Information betrifft, so ist das rechtliche Kriterium für die Unterscheidung der Informationsdelikte von allen anderen Delikten das Vorhandensein von Informationskomponenten (Informationseigenschaften) in ihrer Zusammensetzung, wie zum Beispiel: 1) der Gegenstand einer Straftat – wenn sich die unrechtmäßige Handlung gegen die Informationsbeziehungen oder den Gegenstand der Straftat richtet, d.h. gegen die Information und ihre Träger, die Informationsmittel und -systeme; 2) das Element der objektiven Seite

19 Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000. Crimes related to computer networks /A/ CONF. 187/10. P. 4, 19. Januar, 2022.

20 Juridičeskaja otvetstvennost' za pravonarušenija v informacionnoj sfere i osnovy informacionnoj deliktologii: monografija / I. V. Aristova, A. A. Baranov, O. P. Dzoban' i dr.; pod obšč. red. prof. Beljakova. Kijev: KVITS, 2019, S. 23 [Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: Monographie / *I.V. Aristova, A.A. Baranov, O.P. Dzoban'* u.a.; Hrsg. von *Prof. Beljakov*], 19. Januar, 2022.

der Straftat, das die Art und Weise der Begehung der unrechtmäßigen Handlung angibt – wenn sie unter Verwendung von Informationstechnologien begangen wird.

Eigenständige Rechtsnatur haben dabei nur Delikte, die unmittelbar in die Informationsbeziehungen eingreifen, sich in der Verletzung von Informationsrechten und der Nichterfüllung oder missbräuchlichen Erfüllung von Informationspflichten (Informationsdelikte im engeren Sinne) äußern.

Gerade dieser Teil der Straftatbestände gibt den Anlass, Informationsdelikte als eigenständige Straftaten zu definieren. Alle anderen rechtlichen Merkmale entsprechen der traditionellen rechtstheoretischen Konstruktion eines Delikts. Obwohl der Begriff "Informationsdelikt" in erster Linie ein wissenschaftlicher Begriff ist, finden sich seine wesentlichen Merkmale in zahlreichen rechtswidrigen Handlungen wieder, die gesetzlich vorgeschrieben sind und insbesondere in der Praxis zum Ausdruck kommen:

- rechtswidrige Sammlung, Speicherung, Verarbeitung, Vernichtung, Vervielfältigung und Verbreitung von Informationen;
- Vorenthaltung, Nichtmeldung von Informationen;
- die nicht rechtzeitige Bereitstellung von Informationen;
- Verzerrung, Bereitstellung oder Verbreitung von wissentlich unzuverlässigen (parteiischen) Informationen;
- Verbreitung von Informationen mit sozial schädlichem Inhalt;
- Unerlaubter Zugang zu Informationen;
- Offenlegung von vertraulichen Informationen;
- Ausübung eines negativen informationellen Einflusses auf das Bewusstsein einer Person (Personengruppe, Gesellschaft);
- Erstellung, Verwendung und Verbreitung von bösartiger Software und Hardware;
- unrechtmäßiger Zugang zu und Nutzung von Informationsverarbeitungs-, -speicherungs- und -übertragungssystemen;
- unbefugte Eingriffe in und Behinderung des Betriebs von automatisierten Systemen sowie von Informations- und Telekommunikationssystemen und deren Komponenten.

In der Vielfalt der rechtswidrigen Handlungen im Zusammenhang mit Informationen lassen sich ganz klar bestimmte Gruppen von Handlungen unterscheiden, die einen gemeinsamen Inhalt (eine gemeinsame Richtung) haben und die man als die Hauptgruppen von Straftaten im Bereich der Information betrachten kann: 1) Straftaten gegen Informationsressourcen, die sich auf die Rechtsbeziehungen im Bereich der Information auswirken, die die ordnungsgemäßen qualitativen Merkmale der Information (Vertraulichkeit, Integrität, Verfügbarkeit usw.) gewährleisten; 2) Straftaten gegen den Informationsraum, die sich auf die Rechtsbeziehungen im Bereich der Information auswirken, die mit der ordnungsgemäßen Bereitstellung relevanter Informationen, der Verhinderung der Verbreitung gefährlicher (schädlicher) Informationen und der Verwendung von Technologien mit negativen informationspsychologischen Auswirkungen verbunden sind; 3) Straftaten im Bereich der Informationsinfrastruktur, die sich auf Informationsrechtsverhältnisse auswirken, die sich aus der Nutzung von Objekten der Informationsinfrastruktur ergeben (automatisierte und Informations- und Telekommunikationssysteme, Computer, Server, deren Software usw.); 4) andere Informationsdelikte, die durch die Nutzung von Informationsressourcen, des Informations-

raums und der Informationsinfrastruktur zur Begehung rechtswidriger Handlungen gekennzeichnet sind, die sich auf andere Rechtsverhältnisse auswirken (Dies betrifft Eigentum, öffentliche und staatliche Sicherheit, Wirtschaftstätigkeit usw.).[21]

Es liegt offensichtlich, dass diese Klassifizierung hauptsächlich allgemeiner theoretischer Natur ist. Informationsdelikte als ein bestimmter begrifflicher Typus können nach vielen anderen Merkmalen klassifiziert werden, die für die Typologie von Delikten üblich sind, insbesondere: nach den Sphären der sozialen Beziehungen (im wirtschaftlichen, politischen, ökologischen, kulturellen, wissenschaftlichen, pädagogischen Bereich); je nach dem Gegenstand, der geschädigt wird (Informationsdelikte gegen die Person; Informationsdelikte gegen die Gesellschaft; Informationsdelikte gegen den Staat); nach Wirtschaftszweigen (Industrie, Handel, Landwirtschaft, Verkehr); nach der Art der Informationstätigkeit (im Bereich der Erstellung, Sammlung, Entgegennahme, Speicherung, Nutzung, Verbreitung, des Schutzes von Informationen); nach dem Grad der öffentlichen Gefährdung/Schädigung (Informationsdelikte und -verstöße); nach der Form der Handlung (rechtswidrige Handlung oder Unterlassung); nach der Form des Verschuldens (Vorsatz; Fahrlässigkeit); nach der Anzahl der Personen, die ein Informationsdelikt begehen (Einzelperson; Gruppe); nach der Art der rechtlichen Verantwortung (Informationsdelikte, für die eine strafrechtliche, verwaltungsrechtliche, zivilrechtliche, disziplinarische und sonstige Verantwortung festgelegt ist) usw.[22]

3. Administrative Verantwortung als Instrument zur Gewährleistung der Informationssicherheit: Konzept, Merkmale, Wirksamkeit der Anwendung

Unter den rechtlichen Instrumenten zur Gewährleistung der Informationssicherheit und zur Bekämpfung von Informationsdelikten nimmt die verwaltungsrechtliche Verantwortung einen zentralen Platz im System der Maßnahmen zum Schutz der sozialen Beziehungen im Informationsbereich ein, da die Normen der verwaltungsrechtlichen Verantwortung darauf abzielen, rechtswidrige Eingriffe in rechtlich geschützte Informationsbeziehungen zu verhindern und zu unterbinden.

Gleichzeitig, wie *Perun* zu Recht feststellte, hält die Gesetzgebung zur administrativen Verantwortung „nicht Schritt" mit den rasanten Entwicklungsprozessen der Informationsgesellschaft, was sich negativ auf den Zustand von Recht und Ordnung in der Gesellschaft auswirkt und eine weitere wissenschaftliche Entwicklung erfordert. Der oben genannte Autor hat alle im Gesetzbuch der Ukraine über Ordnungswidrigkeiten (im Folgenden OWiG) enthaltenen Ordnungswidrigkeiten im Bereich der Informationssicherheit analysiert und sie in drei Gruppen unterteilt, und zwar: 1) Sicherstellung des Zugangs natürlicher und juristischer Personen zu öffentlichen Informationen, die für die Ausübung ihrer Rechte, Freiheiten und legitimen Interessen

21 *A. A. Tichomirov*, Informacionnyje pravonarušenija: teoretiko-pravovaja koncepcija. Informacionnaja sochrannost' čeloveka, obščestva, strany, 2015, №1(17), S. 38-47 [*A. A. Tichomirov,* Informationsdelikte: ein theoretisches und rechtliches Konzept], 10. Januar, 2022.

22 *S. A. Pravdjuk*, Klassifikacija informatsionnych pravonarušenij. Sravnitel'no-analitičeskoje pravo, 2013, №4, S. 209–211, [*S. A. Pravdjuk*, Klassifizierung von Informationsdelikten] http://pap-journal.in.ua/wp-content/uploads/2020/07/4_2013.pdf, 19. Januar, 2022.

erforderlich sind; 2) Sicherstellung der Beschränkung des Zugangs zu bestimmten Informationen, deren Verbreitung negative Auswirkungen auf die Rechte und Freiheiten der Bürger, die legitimen Tätigkeiten juristischer Personen oder die nationale Sicherheit haben kann; 3) Gewährleistung der Sicherheit im Bereich der Medieninformation.[23] Der Autor stellt auch fest, dass die regulatorische und rechtliche Unterstützung der administrativen Verantwortung im Bereich der Informationssicherheit unzureichend ist, um die Gesamtheit der sozialen Beziehungen in der Informationssphäre abzudecken, insbesondere regeln die Normen des OWiG über Ordnungswidrigkeiten nicht die Festlegung der Verantwortung für den Inhalt und die Qualität der Medieninhalte von Fernseh- und Rundfunkorganisationen.

Die Wissenschaftlerin *Volkova* ist bei der Analyse der Gesetzgebung, die administrative Verantwortung für Straftaten im Informationsbereich festlegt, und der Materialien der Praxis von Verfahren zu dieser Art von Ordnungswidrigkeiten zu dem Schluss gekommen, dass es bestimmte Lücken in der administrativen und rechtlichen Regelung der Beziehungen im Bereich der Gewährleistung der Informationsrechte und -freiheiten gibt, die Hindernisse bei der Strafverfolgung sowie bei der Aufdeckung und Prävention dieser Art von Straftaten schaffen.[24] Man kann die Auffassung des Verfassers teilen, dass die Rechtsvorschriften über Ordnungswidrigkeiten bisher keine vollständige Liste der Gesetze enthalten, die eine verwaltungsrechtliche Haftung für Straftaten im Bereich der Information vorsehen. Das Gesetzbuch der Ukraine über Ordnungswidrigkeiten (OWiG) ist so aufgebaut, dass die meisten Elemente von Informationsdelikten in verschiedenen Kapiteln des Gesetzbuchs zu finden sind, was den Schutz der rechtlichen Beziehungen im Bereich der Information erheblich erschwert.[25] Gemäß den oben genannten Vorschlägen halten kann man es für sinnvoll halten, ein separates Kapitel zur Bekämpfung der Geldwäsche in das Gesetzbuch einzuführen, in dem alle Ordnungswidrigkeiten im Bereich der Information geregelt werden. Wir schlagen beispielsweise vor, eine Reihe von Straftaten im Informationsbereich in einem einzigen Kapitel 15-B mit dem Titel „Ordnungswidrigkeiten im Informationsbereich" zusammenzufassen, das solche Straftaten enthalten kann:

- Versäumnis, Informationen für Tarifverhandlungen bereitzustellen und die Umsetzung von Tarifverträgen zu überwachen (Art. 41-3);

23 *T.S. Perun*, Administrativnaja otvetstvennost' v sisteme mer obespečenija informacionnoj bezopasnosti // IT pravo: problemy i perspektivy razvitija v Ukraine (vtoraja Meždunarodnaja ježegodnaja konferencija) [*T.S. Perun*, Administrative Verantwortung im System der Informationssicherheitsmaßnahmen // IT-Recht: Probleme und Entwicklungsperspektiven in der Ukraine (Zweite Internationale Jahreskonferenz)], http://aphd.ua/publication-358/, 19. Januar, 2022.

24 *A. Volkova*, Osobennosti juridičeskoj otvetstvennosti za pravonarušenija v informacionnoj sfere [*A. Volkova*, Merkmale der gesetzlichen Haftung für Straftaten im Informationsumfeld], http://ippi.org.ua/volkova-ao-osoblivosti-yuridichnoi-vidpovidalnisti-za-pravoporushennya-v-informatsiinii-sferi, 19. Januar, 2022.

25 Code of Ukraine on Administrative Offenses: Law of Ukraine of December 18, 1984. Document 8073-X, on the basis – 1965-IX https://zakon.rada.gov.ua/laws/show/80731-10?lang=en#Text, 14. Januar, 2022.

- Nutzung von Kommunikationseinrichtungen für Zwecke, die den Interessen des Staates zuwiderlaufen, die öffentliche Ordnung stören und die Ehre und Würde der Bürger verletzen (Art. 148-3);
- Verschweigen von Informationen über die Tätigkeit des Emittenten (Art. 163-5);
- illegale Nutzung von Insiderinformationen (Artikel 163-9);
- Verstoß gegen das Verfahren zur Änderung des Systems der Wertpapierverwahrungsunterlagen (Art. 163-10);
- Verstoß gegen das Verfahren zur Offenlegung von Informationen an der Börse (Art. 163-11);
- unlauterer Wettbewerb (Artikel 164-3);
- Verbreitung von falschen Gerüchten (Art. 173-1);
- Weitergabe von Informationen über die Sicherheitsmaßnahmen der unter Schutz gestellten Person (Art. 185-11);
- Nichteinhaltung der rechtmäßigen Aufforderungen von Beamten des Staatlichen Dienstes für Sonderkommunikation und Informationsschutz der Ukraine (Art. 188-31);
- Verletzung der Gesetzgebung im Bereich des Schutzes persönlicher Daten (Art. 188-39)
- Nichteinhaltung der gesetzlichen Anforderungen von Beamten eines besonders ermächtigten zentralen Exekutivorgans zum Schutz personenbezogener Daten (Art. 188-40)
- Verstoß gegen das Gesetz über Staatsgeheimnisse (Art. 212-2)
- Verletzung des Rechts auf Information (Art. 212-3);
- Verstoß gegen das Verfahren zur Aufzeichnung, Speicherung und Verwendung von Dokumenten und anderen Datenträgern mit vertraulichen Informationen, die Eigentum des Staates sind (Art. 212-5);
- Illegaler Zugang zu Informationen in (automatisierten) Informationssystemen, illegale Herstellung oder Verbreitung von Kopien von Datenbanken von (automatisierten) Informationssystemen (Art. 212-6) und eine Reihe anderer Straftaten im Informationsbereich.

Ein weiteres Problem im Bereich der menschlichen Informationssicherheit ist der unzureichende Schutz personenbezogener Daten und die Ineffizienz des mit der Kontrolle des Schutzes personenbezogener Daten beauftragten Organs. Besonders besorgniserregend ist die Situation in Bezug auf die Bestimmungen der ukrainischen Gesetzgebung, die die Haftung für Verstöße gegen die Normen zum Schutz personenbezogener Daten regeln. Derzeit sind in der ukrainischen Gesetzgebung das Konzept des „Schutzes personenbezogener Daten" sowie die Kriterien, die ein solcher Schutz erfüllen muss, und die Anforderungen an den Eigentümer und Verwalter zur Bestimmung des Schutzniveaus nicht vollständig definiert; die tatsächlichen Haftungsgründe für Verstöße bei der Verarbeitung personenbezogener Daten sind vage. Es sollte ebenso darauf hingewiesen werden, dass die ausschließlich verwaltungsrechtlichen Sanktionen als Mittel zur Bestrafung von Verstößen gegen die Normen zum Schutz personenbezogener Daten unzureichend sind; das institutionelle System zur Verfolgung von Verstößen gegen die Rechtsvorschriften zum Schutz personenbezogener Daten, das derzeit vom Sekretariat des Menschenrechtsbeauftragten des „Obersten Rat" (der

Werchowna Rada) der Ukraine durchgeführt wird, ineffizient ist. Wir schlagen jedoch vor, ein eigenes Organ oder einen eigenen Beamten für den Schutz personenbezogener Daten einzuführen: einen Informations- oder Datenschutzbeauftragten.

Zusammenfassend ist festzustellen, dass das Institut der administrativen Verantwortung für Straftaten im Informationsbereich kein geeignetes Instrument zur Gewährleistung der Informationssicherheit in der Ukraine ist und sich noch in der Aufbauphase befindet. Wir halten es auch für notwendig, die Begriffe „Informationsbereich" und „Straftaten im Informationsbereich" gesetzlich zu regeln und zur Straffung der rechtlichen Regelung der Verwaltungszuständigkeit alle Straftaten im Informationsbereich in einem eigenen Abschnitt des Gesetzes über Ordnungswidrigkeiten im OWiG zusammenzufassen.

4. Strafrechtliche Maßnahmen zur Gewährleistung der Informationssicherheit und Begründung der Notwendigkeit, bestimmte sozial gefährliche Handlungen in der Informationssphäre unter Strafe zu stellen

Die Welt hat sich verändert, das moderne Leben hat sich in einen Informationsraum verwandelt. Die Gefahr besteht darin, dass der Durchschnittsbürger nur unzureichend über Fernarbeit und Online-Lernen Bescheid weiß. Die Informationswelt birgt viele Gefahren und Risiken. Einerseits entwickelt sich die Technik rasant und erleichtert den Menschen das Leben in vielen Bereichen, andererseits entstehen neue Formen der Kriminalität, auf die Gesetzgeber und Strafverfolgungsbehörden nur langsam reagieren. Cyberkriminalität ist heute nicht nur eine Bedrohung für die Informationssicherheit, sondern auch für die nationale Sicherheit insgesamt. Auf dem Gipfeltreffen 2016 erklärten die Staats- und Regierungschefs des Nordatlantikbündnisses den Cyberspace zu einem neuen Bereich der operativen Verantwortung. Die NATO konzentriert sich auf Cybersicherheit.[26] Die Folgen der Cyberkriminalität haben negative Auswirkungen auf die Wirtschaft des Landes (Petya-Virus), die Politik (Fake News, russische Bots und Propaganda), die finanzielle Situation (verschiedene Arten von Internetbetrug) und die psychische und physische Gesundheit der Menschen. Daher sollte die Frage der Informationssicherheit Teil der öffentlichen Politik des Staates werden.[27]

Einige Delikte im Informationsbereich werden als kriminell eingestuft. In diesem Artikel wurde bereits erwähnt, dass Angriffe auf die Informationssicherheit eine breitere Bedeutung haben als die der Cybersicherheit. Es lohnt sich, die Unterschiede an einem einfachen Beispiel zu verdeutlichen. Wenn man eine Antiviren-Software auf dem Computer installiert und ein Angreifer versucht, einen Virus auf dem Computer zu installieren, um Daten zu sammeln oder seine Nutzung zu blockieren (Ransom-

26 How is NATO Meeting the Challenge of Cyberspace By Jamie Shea PRISM Volume 7, No 2, https://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/, 20. Dezember, 2021.

27 Shypovskyi, Volodymyr & Cherneha, Volodymyr & Marchenkov, Serhiy. (2020). Analysis of the ways of improvement of Ukraine – NATO cooperation on cybersecurity issues. Journal of Scientific Papers Social development & Security. 10. 11-15. 10.33445/sds.2020.10.2.2. https://www.researchgate.net/publication/341098345_Analysis_of_the_ways_of_improvement_of_Ukraine_-_NATO_cooperation_on_cybersecurity_issues, 20. Dezember, 2021.

ware), ist das ein Angriff auf die Cybersicherheit. Aber die Informationen zu Benutzernamen und Kennwort auf einem Stick, der auf den Bildschirm geklebt wird und in die Hände des unbefugten Täters gelangt, stellen einen Verstoß gegen die Informationssicherheit dar.

Das ukrainische Strafgesetzbuch enthält den Abschnitt XVI „Straftaten im Zusammenhang mit der Nutzung von Computern, Computersystemen, Computernetzen und Telekommunikationsnetzen", der sechs Straftatbestände enthält[28] (Artikel 361 „Unbefugter Eingriff in Computer, automatisierte Systeme, Computernetze oder Telekommunikationsnetze"); Art. 361-1 „Herstellung mit dem Ziel der Nutzung, der Verbreitung oder des Verkaufs von bösartiger Software oder technischen Mitteln sowie deren Verbreitung oder Verkauf"; Art. 361-2 „Unerlaubter Verkauf oder Verbreitung von Informationen mit beschränktem Zugang, die in elektronischen Datenverarbeitungsanlagen (Computern), automatisierten Systemen, Computernetzwerken oder auf Datenträgern mit solchen Informationen gespeichert sind"; Art. 362 „Unerlaubte Handlungen mit Informationen, die auf elektronischen Datenverarbeitungsanlagen (Computern), automatisierten Systemen, Computernetzen verarbeitet oder auf Trägern solcher Informationen gespeichert sind, begangen von einer zugriffsberechtigten Person"; Artikel 363 „Verletzung der Vorschriften für den Betrieb von elektronischen Datenverarbeitungsanlagen (Computern), automatisierten Systemen, Computernetzen oder Telekommunikationsnetzen oder des Verfahrens oder der Vorschriften zum Schutz der darin verarbeiteten Informationen"; Art. 363-1 „Verhinderung des Betriebs von elektronischen Datenverarbeitungsmaschinen (Computern), automatisierten Systemen, Computernetzwerken oder Telekommunikationsnetzwerken durch massenhafte Verbreitung von Telekommunikationsnachrichten". Der Entwurf des neuen Strafgesetzbuches[29] wird Abschnitt 5.8 enthalten: „Vergehen und Verbrechen gegen die Informationssicherheit". In Abschnitt 5.9 des Entwurfs wird versucht, Straftaten und Ordnungswidrigkeiten in Bezug auf die Zuverlässigkeit von Informationen auf materiellen Datenträgern (ausgenommen elektronische Datenträger) zusammenzufassen. Diese Unterteilung basiert auf Straftaten, die auf nicht-digitale, papierbasierte Informationen und Informationen auf elektronischen Medien abzielen.

In diesem Artikel wurde versucht, die Besonderheiten aktueller sozial gefährlicher Handlungen im Informationsbereich und die strafrechtliche Verantwortlichkeit für diese Handlungen aufzuzeigen. Es muss auch darauf hingewiesen werden, dass jeder Abschnitt des Strafgesetzbuchs eine Reihe von Artikeln enthält, die eine strafrechtliche Verantwortlichkeit für Handlungen im Informationsbereich vorsehen. Diese reichen von Abschnitt I des Besonderen Teils des ukrainischen Strafgesetzbuchs „Straftaten gegen die Grundlagen der nationalen Sicherheit" (z. B. Artikel 109 „Handlungen, die auf eine gewaltsame Änderung oder einen Umsturz der verfassungsmäßigen Ordnung oder die Ergreifung der Staatsgewalt abzielen", bei denen öffentlich zu einer gewaltsamen Änderung oder einem Umsturz der verfassungsmäßigen Ordnung oder der Ergreifung der Staatsgewalt aufgerufen wird, sowie die Verbreitung von Materia-

28 Das ukrainische Strafgesetzbuch, https://zakon.rada.gov.ua/laws/show/2341-14#Text, 22. Dezember, 2021.

29 Entwurf für ein neues Strafgesetzbuch der Ukraine, https://newcriminalcode.org.ua/upload/media/2022/01/18/kontrolnyj-proekt-kk-18-01-2022.pdf, 22. Dezember, 2021.

lien, in denen zu solchen Handlungen aufgerufen wird, über soziale Netzwerke und andere Internetressourcen) bis zu Abschnitt XX des Besonderen Teils des Strafgesetzbuches „Verbrechen gegen den Frieden, die Sicherheit der Menschheit und das Völkerrecht", „Kriegspropaganda" (Artikel 436 Strafgesetzbuch); Herstellung und Verbreitung von kommunistischen oder nationalsozialistischen Symbolen und Propaganda für kommunistische und nationalsozialistische (nationalsozialistische) totalitäre Regime (Artikel 436-1GB). Ein weiteres spezielles Kriterium, das die strafrechtliche Sicht auf die Möglichkeit der Begehung eines Informationsdelikts grundlegend verändert, ist die Begehung von Handlungen mittels Fernkommunikation. Die Kommunikation zwischen weit voneinander entfernten Personen unter Einsatz von IT sollte als Fernkommunikation betrachtet werden. Die Technologie, die einen sofortigen Informationsaustausch aus der Ferne ermöglicht, ist ein Merkmal der Beziehungen in der Informationsgesellschaft, des Fortschritts des einundzwanzigsten Jahrhunderts, der sicherlich zur Wirksamkeit der Globalisierungsprozesse beiträgt.[30]

Im Zusammenhang mit der Notwendigkeit, bestimmte sozial gefährliche Handlungen, die im Informationsbereich begangen werden, unter Strafe zu stellen, ist auf einige Lücken im ukrainischen Strafrecht hinzuweisen. Die erste hängt möglicherweise mit der fehlenden strafrechtlichen Verantwortung für die Erstellung und Verbreitung von Fake News zusammen, da Manipulationen und „Angriffe" auf das Bewusstsein der Menschen nicht weniger gefährlich sind als Cyberangriffe. Obwohl dem Obersten Rat der Ukraine eine Reihe von Gesetzesentwürfen vorgelegt wurden, die eine Haftung für Fake News[31] vorsehen, wurde die Gesetzgebung bisher nicht geändert. Der Entwurf des neuen Strafgesetzbuches enthält die Bestimmung 5.8.10 „Verbreitung wissentlich falscher Nachrichten", die besagt, dass „... die für die Veröffentlichung von Nachrichten verantwortliche Person zugelassen hat, dass wissentlich falsche Informationen von öffentlichem Interesse verbreitet, in Umlauf gebracht oder redaktionell in einem sozialen Netzwerk gemeldet wurden".[32] Wann das neue Strafgesetzbuch verabschiedet wird, ist jedoch noch offen. Die Verbreitung von Fake News wird in einem Artikel von *Mazepa*[33] ausführlicher beschrieben. Die Fälschungen betreffen hauptsächlich zwei globale Probleme in der Ukraine: die militärische Aggression der Russischen Föderation und die Covid-19-Pandemie. Informationskriege werden durch eine Vielzahl von Desinformationen, Fake News und Propagandamethoden geführt. Die hohe gesellschaftliche Gefahr der genannten Taten liegt darin, dass die

30 Juridična vidpovidal'nost' za pravonarušenija v informacijnij sferi ta osnovy informacijnoi deliktologii: monografija / I. V. Aristova, A. A. Baranov, O. P. Dzoban' ta in.; red. prof. Beljakova. Kijev: KVITS, 2019, 344 S., S. 205-226 [Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: Monographie / *I.V. Aristova, A.A. Baranov, O.P. Dzoban'* u.a.; Hrsg. von *Prof. Beljakov*].

31 Gesetzentwurf zur Bekämpfung von Desinformationen, https://mkip.gov.ua/files/InformPolityka.pdf, 20. Dezember, 2021.

32 Entwurf eines neuen Strafgesetzbuches, https://newcriminalcode.org.ua/upload/media/2022/01/18/kontrolnyj-proekt-kk-18-01-2022.pdf, 20. Dezember, 2021, https://newcriminalcode.org.ua/upload/media/2022/01/18/kontrolnyj-proekt-kk-18-01-2022.pdf, 2. Dezember, 2021.

33 *S. Mazepa* et al. An Ontological Approach to Detecting Fake News in Online Media //2021 11th International Conference on Advanced Computer Information Technologies (ACIT). – IEEE, 2021. – C. 531-535.

Zahl der Opfer nicht ermittelt werden kann. Das Phänomen der Propaganda,[34] das leider in negativer Weise verwendet wird, sollte gesondert hervorgehoben werden. Es wurde vorgeschlagen, das ukrainische Strafgesetzbuch um Artikel 161-1 zu ergänzen, der laut Gesetzentwurf Nr. 3316[35] „öffentliche Aufrufe zur Feindseligkeit, gewalttätige Handlungen, die Verfolgung oder Erniedrigung der Würde von Personen oder Personengruppen oder die Beschädigung oder Zerstörung ihres Eigentums aufgrund der sexuellen Orientierung oder Geschlechtsidentität" unter Strafe stellen würde, und gemäß Artikel 3316-1[36] „öffentliche Aufrufe und/oder Propaganda der Kinderverweigerung, die Zerstörung der Institution Familie, außereheliche und unnatürliche sexuelle Beziehungen und Ausschweifungen" unter Strafe gestellt würden.

Das nächste Thema betrifft fingierte Bombenanschläge. In letzter Zeit häufen sich in der Ukraine die Fälle von Falschmeldungen über Bombenanschläge auf sensible Einrichtungen,[37] was zu einer erheblichen Destabilisierung in Bezirken, Städten und im ganzen Land führt. Die Informationen werden per E-Mail an staatliche Behörden und Unternehmen sowie über Messenger verschickt. Allein seit Anfang 2022 wurden innerhalb von drei Wochen 339 Bombendrohungen gemeldet, davon 306 per E-Mail, 27 per Telefon und 6 persönlich oder per Post. Und das ist die Hälfte aller für das Jahr 2021[38] eingegangenen Meldungen. Das Verfahren zur Reaktion auf solche Vorfälle erfordert eine Reihe von speziellen Diensten, Personal- und Zeitressourcen. Da derartige Fragen nicht nur durch strafrechtliche Instrumente geregelt werden sollten, ist es angemessen, eine strafrechtliche Haftung für die oben genannte Handlung in Betracht zu ziehen, da sie eine erhebliche Gefahr für die Öffentlichkeit darstellt.

Darüber hinaus erschwert das Fehlen von Schlüsselbegriffen und Definitionen in den Rechtsvorschriften die strafrechtliche Verfolgung der Täter von Informationsdelikten. So ist beispielsweise der Begriff „Kryptowährung" in der ukrainischen Gesetzgebung noch nicht enthalten. Obwohl Kryptowährungen als Zahlungsmittel für jedermann zugänglich sind, haben sie ihre Abnehmer auf dem modernen ukrainischen Markt gefunden. So meldeten ukrainische Beamte in ihren Erklärungen für 2020

34 *S. V. Ševčenko*, Strafrechtliche Verantwortung für Propaganda in der Ukraine: ein Blick durch das Prisma des Grundsatzes der Verhältnismäßigkeit. Zeitschrift der Ukrainischen Vereinigung für Strafrecht 2020, № 2(14), S. 260-272, http://vakp.nlu.edu.ua/article/view/218815/219451, 20. Januar, 2022.

35 Gesetzentwurf zur Änderung des Strafgesetzbuches der Ukraine zur Bekämpfung von Hassverbrechen aufgrund der sexuellen Orientierung und der Geschlechtsidentität vom 9. April 2020 № 3316, http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68552, 25. Dezember, 2021.

36 Gesetzentwurf zur Änderung des ukrainischen Strafgesetzbuchs (Kriminalisierung des öffentlichen Aufrufs und/oder Propaganda der Kinderverweigerung, der Zerstörung der Institution der Familie, außerehelicher und widernatürlicher sexueller Beziehungen und der Ausschweifung № 3316-1 vom 24.4.2020, http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68664, 20. Dezember 2021.

37 https://www.pravda.com.ua/rus/news/2022/01/21/7321214/, 22. Dezember, 2021.

38 Offizielle Website der ukrainischen Cyberpolizei, https://cyberpolice.gov.ua/news/informaciya-shhodo-seriyi-nedostovirnyx-minuvan-obyektiv-infrastruktury-ukrayiny-1110/, 20. Januar, 2022.

46.351 Bitcoins, deren Marktwert im April 2021 fast 75 Milliarden Griwna betrug.[39] Bislang sind die Rechtsverhältnisse im Bereich der Kryptowährungen jedoch noch nicht gesetzlich geregelt. In der Tat fanden die bereits 2016-2018 vorgestellten Gesetzesentwürfe (Gesetzentwurf Nr. 7183 vom 6.10.2017 „Über den Umlauf von Kryptowährungen in der Ukraine"; Gesetzentwurf Nr. 7183 1 vom 10.10.2017 „Über die Stimulierung des Marktes für Kryptowährungen und deren Derivate in der Ukraine") im Parlament Unterstützung. Im Gegenzug wurde erst am 2.12.2020 der Gesetzesentwurf über virtuelle Vermögenswerte Nr. 3637 (der kritisiert wird, da er im Hinblick auf die Angleichung an die EU-Richtlinien einer grundlegenden Überarbeitung bedarf) in erster Lesung angenommen, was sicherlich ein richtiger, aber kein ausreichender Schritt zur Konsolidierung seines Rechtsstatus war. Ab heute definiert die Anmerkung 1 zu Artikel 368-5 des Strafgesetzbuches der Ukraine, dass Kryptowährungen zusammen mit Bargeld, anderen Vermögenswerten, Eigentumsrechten und immateriellen Vermögenswerten zur Gruppe der Vermögenswerte gehören.[40]

Die weltweite Praxis zeigt, dass Straftaten im Zusammenhang mit Kryptowährungen unterteilt werden sollten in Straftaten im Zusammenhang mit Diebstahl, Erpressung mit Kryptowährungen, Legalisierung (Geldwäsche) von mit kriminellen Mitteln erworbenem Eigentum und illegalem Verkauf von verbotenen Waren, Dienstleistungen und Inhalten (Drogen, psychotrope Drogen, Waffen usw.).[41]

Ein großes Problem stellt auch die umstrittene Anpassung des ukrainischen Strafrechts an das europäische Recht im Rahmen der Istanbul-Konvention dar (Council of Europe Convention on preventing and combating violence against women and domestic violence; Istanbul Convention).[42] Am ukrainischen Strafgesetzbuch wurde eine Reihe von Änderungen vorgenommen, ohne die historischen und kulturellen Traditionen des Landes zu berücksichtigen. So wurde beispielsweise die Strafbarkeit von Zwangsheiraten eingeführt, obwohl solche Handlungen für slawische Völker nicht besonders typisch sind. Das Konzept des Stalkings und die strafrechtliche Verantwortlichkeit dafür fehlen hingegen noch. Es ist zu betonen, dass es keine Haftung für Cyberstalking gibt, das eine große soziale Gefahr darstellt, da der Täter das Opfer jederzeit aus der Ferne beeinflussen und in Angst halten kann.

39 Informationen von der offiziellen OpenDataBot-Website „46.351 Bitcoins von Beamten gemeldet", https://opendatabot.ua/analytics/bitcoin-2021, 10. Januar, 2022.

40 Strafgesetzbuch der Ukraine, https://zakon.rada.gov.ua/laws/show/2341-14#Text, 20. Januar, 2022.

41 *S. V. Ivancov, E. L. Sidorenko, B. A. Spasennikov*, Prestuolenija, svjazannye s ispol'zovaniem kriptovaljuty: onovnye kriminologičeskie tendencii. // Vserossijskij kriminologičeskij žurnal [Straftaten im Zusammenhang mit Kryptowährungen: Wichtige kriminologische Trends. // Russische Zeitschrift für Kriminologie]- № 1, 2019, S. 85–93.

42 Council of Europe Convention on preventing and combating violence against women and domestic violence; Istanbul Convention https://www.coe.int/en/web/istanbul-convention/home? 15. Januar, 2022.

5. Überblick über die gefährlichsten Bedrohungen der Informationssicherheit in der Ukraine

In diesem Zusammenhang muss auch die Frage der Bedrohungen für die Informationsgesellschaft und der Möglichkeiten, sie zu bewältigen, angesprochen werden. An erster Stelle sind hier Cyberangriffe zu nennen, wobei der neueste groß angelegte Angriff am 13. und 14. Januar 2022 stattfand. Die Viper-Software WhisperGate wurde nach Microsofts Einstufung zur Datenvernichtung eingesetzt. Der Austausch von Informationen (Dephasierung) auf den Websites der angegriffenen Regierungsbehörden und die Zerstörung von Daten mithilfe einer Viper sind Bestandteile des Cyberangriffs.[43] Insgesamt wurden mehr als 70 Regierungswebsites angegriffen, von denen 10 unbefugten Eingriffen ausgesetzt waren. Die Hacker nutzten eine Sicherheitslücke im Content-Management-System aus. Fachleute stellten fest, dass der Angriff über die supply chain attack erfolgte. Die Angreifer drangen in die Infrastruktur eines kommerziellen Unternehmens ein, das mit Administrationsrechten Zugang zu den von dem Angriff betroffenen Webressourcen hatte. Wegen unbefugter Eingriffe in die Arbeit von Websites staatlicher Einrichtungen leitete die Ermittlungsabteilung der Kiewer Polizei ein Strafverfahren nach Teil 2 Artikel 361 (unbefugte Eingriffe in die Arbeit von elektronischen Computern, automatisierten Systemen, Computernetzen oder Telekommunikationsnetzen) des Strafgesetzbuches der Ukraine ein. Die Ermittlungen dauern an.[44] Nicht zu vergessen ist der größte Cyberangriff *Petya*, der als der zerstörerischste in der Geschichte gilt, und Black Energy, der erste erfolgreiche Cyberangriff auf ein Energiesystem, bei dem Umspannwerke in der Region Iwano-Frankiwsk lahmgelegt wurden. Auch verschiedene Arten von Betrug, Erpressung und Phishing stellen nach wie vor die am weitesten verbreitete Internetkriminalität dar. Eine besonders gefährliche Form der Internetkriminalität ist laut dem Jahresbericht des IOCTA[45] in Bezug auf Kinder in letzter Zeit das Online-Grooming. Dabei handelt es sich um illegale Aktivitäten, die darauf abzielen, erotische oder pornografische Kinderfotos zu beschaffen, oder um Kriminelle, die für die Verbreitung dieser Fotos Lösegeld verlangen.[46] Der Diebstahl von virtuellem Zubehör in Computerspielen wird immer beliebter, da das "Aufmotzen" eines virtuellen Abbilds mit Kosten und Zeitaufwand verbunden ist.

Für eine erfolgreiche Cybersicherheit lohnt es sich, internationale Erfahrungen zu analysieren und Ansätze beispielsweise aus Deutschland zu übernehmen, das einen Rahmen für seine Cybersicherheitspolitik in drei wichtigen Bereichen entwickelt hat: präventive Maßnahmen, die sich auf technische Lösungen und Technologien konzentrieren; Maßnahmen zum Schutz personenbezogener Daten, die auf eine hohe Ach-

43 BBC News Website, https://www.bbc.com/ukrainian/news-60050149, 15. Januar, 2022.

44 Die offizielle Website der ukrainischen Cyberpolizei, https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/, 15. Januar, 2022.

45 Internet Organised Crime Threat Assessment (IOCTA) 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf, 1. Dezember 2021.

46 Andrew Murray Information Technology Law: The Law and Society (4th edn) Oxford University Press https://doi.org/10.1093/he/9780198804727.001.0001.

tung der Privatsphäre durch rechtliche, technische und organisatorische Maßnahmen abzielen, und – ebenso wichtig – Strategien zur Ausweitung von Straftatbeständen und zur Stärkung der Sicherheitsbehörden sowie zur Ausweitung der Ermittlungsbefugnisse im Bereich der Computerkriminalität. Diese drei Schwerpunkte haben eines gemeinsam: Sie sind in erster Linie präventiv und zivil. Sie beruhen auf der Vorstellung, dass Cybersicherheit durch die richtige Strukturierung informationstechnischer Systeme, den rechtlichen Schutz von Personen vor Missbrauch des Systems und die konsequente Verfolgung von Rechtsverstößen geschaffen werden kann. Deutschland ist mit diesem Ansatz sehr erfolgreich gewesen.[47]

Besondere Aufmerksamkeit sollte der Kriminalisierung von Handlungen im Zusammenhang mit der Unterzeichnung des Übereinkommens der Europäischen Union über Computerkriminalität[48] im Jahr 2001 und seiner Ratifizierung durch die Ukraine im Jahr 2005 gewidmet werden.[49] Der Begriff „Cyberkriminalität" umfasst eine Reihe von gesellschaftlich gefährlichen Handlungen,[50] die nicht nur gegen Informationen, Medien und Computersysteme gerichtet sind, sondern im gesamten Cyberspace begangen werden. Bei der Einstufung des Stadiums der Begehung von Straftaten muss die Fernkommunikation in der Informationsgesellschaft berücksichtigt werden. Solche Handlungen können als Vorbereitung zur Begehung einer Straftat gewertet werden. Die Suche nach einem Komplizen in einem anderen Land oder auf einem anderen Kontinent, die mit Hilfe des Internets und der Telekommunikation durchaus möglich ist, erhöht in gewisser Weise die soziale Gefährlichkeit einer Tat, da eine Person mit Erfahrung in ähnlichen Handlungen, die bereits erfolgreich ähnliche Straftaten begangen hat, in ein bestimmtes Verbrechen verwickelt sein kann; Handlungen zur Begehung von Straftaten auf Distanz haben den Charakter eines kriminellen Handels. Außerdem erhöht sich durch die Fernsuche nach Komplizen die Zahl der „Experten" beträchtlich, was die Chancen erhöht, dass die Täter ihre Absichten verwirklichen können. Die meisten Hacker, die eine Aktion gegen ein bestimmtes Computersystem planen, wissen überhaupt nichts übereinander, abgesehen von den gegenseitigen Nicknames und bestenfalls den IP-Adressen ihrer Partner. In solchen Fällen ist das Darknet weit verbreitet.[51] Der Nachweis der Mittäterschaft ist äußerst schwierig. Sie erfordert besondere Kenntnisse und die Sammlung besonderer Beweise, was ihren Nachweis in der Praxis sehr schwierig macht. Das moderne Strafgesetzbuch enthält weder eine gesonderte Bestimmung, die den Begriff der "Verschwörung" beschreibt, noch eine Analyse des Tatbestands der Verschwörung oder einen wissenschaftlichen

47 Schallbruch, Martin & Skierka, Isabel. (2018). The German View on Cybersecurity. 10.1007/978-3-319-90014-8_2.

48 Übereinkommen über Computerkriminalität vom 23. November 2001, № 994_575 // Staatsanzeiger der Ukraine vom 10.9.2007, № 65, S. 107, Art. 2535. http://zakon.rada.gov.ua/laws/show/994_575.

49 Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art vom 28. Januar 2003, № 994_687 // Staatsanzeiger der Ukraine, 2010, № 56 Art. 2202, http://zakon.rada.gov.ua/laws/show/994_687.

50 Advances in Cyber Security Third International Conference, ACeS 2021 Penang, Malaysia, August 24–25, 2021 Revised Selected Papers.

51 Mirea, M., Wang, V. & Jung, J. The not so dark side of the darknet: a qualitative study. Secur J 32, 102–118 (2019). https://doi.org/10.1057/s41284-018-0150-5.

und praktischen Kommentar zum Strafgesetzbuch. In der Praxis ist es unmöglich, ohne eine besondere praktische oder wissenschaftliche Grundlage eine geheime Absprache zwischen zwei entfremdeten Personen nachzuweisen, da es unmöglich wäre, die Tatsache ihres Kontakts miteinander und ihre Diskussion über die Bedingungen und Verfahren zur Erreichung eines gemeinsamen kriminellen Ziels zu beweisen, wenn Aussagen von entfremdeten Mittätern gemacht werden.[52]

Hinzu kommt, dass die gesellschaftliche Gefahr der Computerkriminalität gerade wegen der „beschleunigten Entwicklung von Wissenschaft und Technik im Bereich der Computerisierung sowie der stetigen und raschen Ausweitung des Einsatzes der Computertechnologie" ständig zunimmt.[53] Es ist zu bedenken, dass die Gefahr besteht, ein Verbrechen in großem Umfang zu begehen. Das Fehlen von Grenzen (transnationale Kriminalität) und die Umwandlung der Cyberkriminalität in organisierte Kriminalität sind ebenfalls charakteristische Merkmale.

II. Fazit

In diesem Artikel wurde versucht, die neuen Herausforderungen für die Informationssicherheit der Ukraine im Zusammenhang mit der militärischen Aggression der Russischen Föderation und der Covid-19-Pandemie zu analysieren, die für die Gewährleistung der nationalen Sicherheit im Allgemeinen erschwerende Faktoren darstellen.

Es wurde auf Lücken in der ukrainischen Gesetzgebung hinsichtlich der Haftung für Straftaten im Informationsbereich hingewiesen. Bei der Analyse der Verwaltungsvorschriften sind wir zu dem Schluss gekommen, dass das Institut der verwaltungsrechtlichen Verantwortlichkeit für Straftaten im Informationsbereich kein geeignetes Instrument zur Gewährleistung der Informationssicherheit in der Ukraine ist und sich noch in einem Entwicklungsstadium befindet. Es besteht die Notwendigkeit, das Konzept der „Informationssphäre" und der „Straftaten in der Informationssphäre" gesetzlich zu regeln; und um die gesetzliche Regelung der administrativen Verantwortung zu straffen, sollten alle Straftaten in der Informationssphäre in einem separaten Abschnitt des GBdU über Ordnungswidrigkeiten zusammengefasst werden. Es wurde auch vorgeschlagen, eine gesonderte Stelle oder einen Beamten für den Schutz der Informationsrechte und der personenbezogenen Daten einzuführen – den Informationsbeauftragten, dessen Aufgabe es wäre, den Schutz der Menschenrechte im Informationsbereich zu überwachen und zu kontrollieren.

---

52 Juridična vidpovidal'nost' za pravonarušenija v informacijnij sferi ta osnovy informacijnoi deliktologii: monografija / I. V. Aristova, A. A. Baranov, O. P. Dzoban' ta in.; red. prof. Beljakova. Kijev: KVITS, 2019, 344 S., S. 205-226 [Rechtliche Verantwortung für Straftaten in der Informationssphäre und Grundlagen der Informationsdeliktologie: Monographie / *I.V. Aristova, A.A. Baranov, O.P. Dzoban'* u.a.; Hrsg. von *Prof. Beljakov*].

53 *M. V. Karčevs'kij*, Dosliđennja praktiki vikoristannja nacional'nymy sudamy norm pro kryminal'nu vidpovidal'nost' za zločyny v sferi vikoristannja komp'uternoij techniky ta merež elektrozv'jazku / Zločyny v sferi vikoristannja IT [*M. V. Karčevs'kij,* Studie über die Anwendung des Straftatbestands der Computer- und Telekommunikationsnetzstraftaten / Internetstraftaten durch die nationalen Gerichte], http://it-crime.at.ua/index/zagalna_kharakteristika/0-32.

In Bezug auf die strafrechtliche Haftung wurde von den Autoren eine Reihe von Fragen gestellt, die einer strafrechtlichen Regelung bedürfen. Dazu gehören die Notwendigkeit, die Erstellung und Verbreitung von Fake News, Propaganda, Fake Mining und Cyberstalking unter Strafe zu stellen, sowie die Frage, ob die rechtzeitige Einführung neuer Schutzmaßnahmen in die geltenden Rechtsvorschriften sinnvoll ist. Zusammenfassend lässt sich sagen, dass der Schwerpunkt nicht auf der Einführung der Verantwortung für neue Straftaten liegen sollte, auch wenn dies der Fall ist, sondern auf der Analyse von Straftaten und Verbrechen, dem Studium internationaler Erfahrungen und der Ausarbeitung eines nationalen Berichts über die Informationskriminalität sowie einer offiziellen Übersetzung des Berichts für die Bürger (IOCTA), damit diese verstehen, wie sie sich schützen können. Daher sind die Cyberhygiene und die Empfehlungen von Europol wichtige Elemente bei der Prävention von Internetkriminalität, und die rechtzeitige Einführung wissenschaftlich fundierter Konzepte und Definitionen, wie z. B. Kryptowährungen, wird es ermöglichen, Einzelpersonen für die Begehung von Straftaten, die sie nutzen, strafrechtlich zu verfolgen. Die Analyse der am häufigsten vorkommenden Straftaten setzt in der Regel voraus, dass man ihre Gemeinsamkeiten erkennt, ihre charakteristischen Merkmale versteht und sich die entsprechenden technischen und analytischen Mittel zu ihrer Verhinderung aneignet. Der Artikel zielt jedoch nicht darauf ab, den Gesetzgeber zu kritisieren, sondern vielmehr wichtige Fragen aufzuwerfen, die eine wissenschaftliche Diskussion erfordern.